

### Terms and Conditions of Use of Digitised Theses from Trinity College Library Dublin

### **Copyright statement**

All material supplied by Trinity College Library is protected by copyright (under the Copyright and Related Rights Act, 2000 as amended) and other relevant Intellectual Property Rights. By accessing and using a Digitised Thesis from Trinity College Library you acknowledge that all Intellectual Property Rights in any Works supplied are the sole and exclusive property of the copyright and/or other IPR holder. Specific copyright holders may not be explicitly identified. Use of materials from other sources within a thesis should not be construed as a claim over them.

A non-exclusive, non-transferable licence is hereby granted to those using or reproducing, in whole or in part, the material for valid purposes, providing the copyright owners are acknowledged using the normal conventions. Where specific permission to use material is required, this is identified and such permission must be sought from the copyright holder or agency cited.

### Liability statement

By using a Digitised Thesis, I accept that Trinity College Dublin bears no legal responsibility for the accuracy, legality or comprehensiveness of materials contained within the thesis, and that Trinity College Dublin accepts no liability for indirect, consequential, or incidental, damages or losses arising from use of the thesis for whatever reason. Information located in a thesis may be subject to specific use constraints, details of which may not be explicitly described. It is the responsibility of potential and actual users to be aware of such constraints and to abide by them. By making use of material from a digitised thesis, you accept these copyright and disclaimer provisions. Where it is brought to the attention of Trinity College Library that there may be a breach of copyright or other restraint, it is the policy to withdraw or take down access to a thesis while the issue is being resolved.

#### Access Agreement

By using a Digitised Thesis from Trinity College Library you are bound by the following Terms & Conditions. Please read them carefully.

I have read and I understand the following statement: All material supplied via a Digitised Thesis from Trinity College Library is protected by copyright and other intellectual property rights, and duplication or sale of all or part of any of a thesis is not permitted, except that material may be duplicated by you for your research use or for educational purposes in electronic or print form providing the copyright owners are acknowledged using the normal conventions. You must obtain permission for any other use. Electronic or print copies may not be offered, whether for sale or otherwise to anyone. This copy has been supplied on the understanding that it is copyright material and that no quotation from the thesis may be published without proper acknowledgement.

## **Geographical Information and Privacy**

An Examination of the Relationship between Privacy, Data Protection and Digitally-Stored Personal Geographical Information in Ireland in the 1990s

16 MAY 2000

Submitted as fulfilment of the Requirements for the Degree of Ph.D. by Research to Trinity College, Dublin.

Aodán Edmonds October 1999



### DECLARATION

I declare that this thesis is entirely my own work, and has not been submitted for examination at any other university.

From activity of the limit particularly thank Dr. Margaret O'Flanagan of DCU for her halp in the second second to whom I spoke during the course of this study was both encourse of this study was both encourse of this study was both in the second of the content of the terminal of whom were very generous with their time and knowly the

i also tryif there is the staff and presignation of students of the Tripics' both the posting up with and for an long and the t particularit haust there the many people who have passed they be yongs, all these Pat and Tale deserve special praise for the out and blocking final copies

Aodán Edmonds

The copyright for this work resides with the author. Any reference to material contained in this work should be appropriately acknowledged.

#### ACKNOWLEDGEMENTS

To begin with I would like to thank my supervisor, Dr. Krysia Rybaczuk. When Dr. Rybaczuk first came to Trinity I was one of the young Junior Sophister students who signed up for the new-fangled GIS course under her tutelage. And so to Dr. Rybaczuk I owe my interest in GIS, and my interest in its privacy implications, both of which were sparked during that lecture course. More pertinently Dr. Rybaczuk has been a patient supervisor over the last number of years, who dealt with my tendency to run off on tangents remarkably well and who always managed to bring me back to earth successfully. Her ideas, help, support, and sane criticism have been vital.

From outside Trinity I must particularly thank Dr. Margaret O'Flanagan of DCU for her help in the design of my questionnaire. The helpfulness of the many people in various organisations around Ireland to whom I spoke during the course of this study was both encouraging and vital. In particular I would like to thank the many individuals interviewed in the course of my questionnaire survey all of whom were very generous with their time and knowledge.

I also owe thanks to the staff and postgraduate students of the Department of Geography in Trinity, both for putting up with me for so long and for their ideas and support. In particular I must thank the many people who have passed through the GIS Laboratory over the years. Of these Pat and Tale deserve special praise for their help in matter of printing out and binding final copies.

Thanks also to all of those at conferences and elsewhere who showed an interest in my research and offered advice. It not only gave me ideas but often helped to prop up my flagging enthusiasm.

Finally I would like to thank my family and friends. My parents in particular have been very supportive, and mercifully slow to ask when I will get a 'proper job'. Stephen, Mike, Ian, Helen, Matthew and others helped me to clarify my thoughts and often challenged them. And finally Annette, who helped me to see the light at the end of the tunnel.

#### Aodán Edmonds

# SUMMARY

Geographical Information (GI) has traditionally been an instrument of power used particularly by governments and other organisations with the large resources needed to utilise such an expensive resource. Recent developments mean that digitally-stored personal information of all kinds can now effectively be treated as GI and analysed geographically. Since digital storage means that information from different sources can be merged easily it is now practical to create large databases of personal information on an individual basis.

In effect this means that digital information is now a serious threat to privacy on an individual basis. Personal GI is particularly prone to have an impact on privacy due to its integrative power and focus on spatial analysis. In effect it is now potentially possible to track individuals in space, and to link private information from diverse sources to this tracking process, allowing the monitoring of all human activity and destroying real privacy, although the illusion of privacy may sometimes persist. The aim of this study was to examine the impacts and potential impacts on Ireland of such developments.

One of the primary purposes of privacy in modern democratic society is seen as the freeing of the individual from observation so that he/she can develop an individual personality, including views potentially divergent from the social norm. One of the characteristics of societies where such a strong individual privacy does not exist is strong social conformity enforced by social pressure and maintained by observation. Such a system of control is operated through individual observation and monitoring, according to Foucault, in modern disciplinary institutions such as the prison. Clearly the constant monitoring of individuals in the entire population, now possible through the use of GI technology, can potentially have the same effect.

Although privacy is clearly vital to the protection of individual democratic freedom and the right to dissent it is a poorly defined right, in large part due to it s relationship to human intimacy, and the range of activities and spaces on which it impacts. Its nature and extent are poorly defined and considerable disagreement exists both legally and philosophically concerning privacy and its protection. The result is that legal protection of privacy tends to be weak and fragmented. Such is the case in Ireland.

In relation to digital information the clear impact it can have on privacy has led to the introduction of legislation in many jurisdictions, including Ireland, to protect the integrity of private information stored in a digital medium. Such statutes do not, however, directly protect privacy since they allow the collection, storage and processing of information for a variety of legal purposes, both public and private. In general it is also the case that such legislation is not motivated by concern for privacy, but rather to enable commercial and government activities to continue unhindered. The Irish Data Protection Act (1988) is such a statute, developed under pressure from Europe for the benefit of business.

In the study it became clear that although there was a high degree of compliance with the data protection principles as defined by the Act such compliance was largely based on either serendipity or organisational imperatives of data collectors and processors. Thus there is substantial effort devoted to data security and to limitation of access, while data sharing is also restricted, though often for technical reasons such as the age of systems. However, such protection is being diminished through the modernisation and integration of systems, the increased power of analysis particularly due to changes in the nature of what can legitimately be considered digital GI and changing organisational needs which

dictate increased data sharing to increase efficiency. The dangers of deliberate or inadvertent misuse of private information are thus increased at a time when more and more such information is being collected and used.

Although in the current situation the law is being upheld the meaning of privacy has been diminished to that of data protection, enforced by an under-funded Commissioner at a time when the amount of information and the techniques for its manipulation are always increasing. The result is increasingly the creation of a society where individuals are observed either directly or indirectly and where the social pressure of observation can be used to enforce certain behaviours.

LIST OF MAPS LIST OF FIGURES LIST OF TABLES LIST OF APPENDICES ABBREVIATIONS AND ACCRONYMS

#### CHAPTER 1 INTRODUCTION

1 INTRODUCTION

- 1 3 REAKONS FOR THE STUDY
- 1.4 AND AND OR PCTIVES OF THE STUDY
- 1 S CHAPTER OUTLINE

CHAPTER 2

### TEORMATION SYSTEMS (C) D

CROCRAPHINE OF SECONDALION
 DERITAL OF SCIENCE
 DERITAL OF SCIENCE

<sup>2.6</sup> CONCLUSIONS

### TABLE OF CONTENTS

TITLE Publicat Tennions in the Information Age	I
DECLARATION	II
ACKNOWLEDGEMENTS	III
SUMMARY	IV
TABLE OF CONTENTS	VI
LIST OF MAPS	IX
LIST OF FIGURES	X
LIST OF TABLES	XI
LIST OF APPENDICES	XII
ABBREVIATIONS AND ACCRONYMS	XIII

### CHAPTER 1 INTRODUCTION

1.1 INTRODUCTION	1
1.2 INTRODUCTION TO GEOGRAPHICAL INFORMATION	3
1.3 REASONS FOR THIS STUDY	4
1.4 AIMS AND OBJECTIVES OF THE STUDY	6
1.5 CHAPTER OUTLINE	7

### CHAPTER 2 GEOGRAPHICAL INFORMATION, GEOGRAPHIC INFORMATION SYSTEMS AND THE ISSUE OF POWER

2.2 GEOGRAPHICAL INFORMATION	9
	13
2.3 DIGITAL GI AND GIS	. 13
2.3.1 Problems with Digital GI.	. 13
2.3.2 GIS: Geographic Information Systems	. 16
2.3.3 GI in Information Systems: GIS and IS	. 20
2.3.4 The Demise of GIS	. 21
2.4 PRE-DIGITAL GI AND POWER	. 24
2.4.1 GI and World Views: The Creation of Place	. 25
2.4.2 GI, Land Ownership and Taxation	. 29
2.4.3 GI and Colonialism	.30
2.4.4 GI and Military/Political Power	.32
2.5 DIGITAL GI AND POWER	.35
2.5.1 Digital GI and Privacy: Issues and Examples	.36
2.6 CONCLUSIONS	.42

### CHAPTER 3 ETHICAL ISSUES AND PRIVACY

3.1 INTRODUCTION	
3.2 ETHICAL DIMENSIONS OF IT AND THE ISSUE OF PRIVACY	
3.2.1 Fundamentals of Modern Ethics	
3.2.2 Ethical Tensions in the Information Age	
3.2.3 Privacy as an Issue in the Information Society	
3.3 PRIVACY	
3.3.1 Defining Privacy	
3.3.2 Arguments against Privacy	
3.3.3 Historical and Cultural Dimensions of Privacy	
3.3.4 Privacy as a Universal Value	
3.3.5 The Importance of Privacy	60
3.3.6 International Legal Protection of Privacy	
3.5 CONCLUSIONS	63

### CHAPTER 4 THEORETICAL ISSUES OF INFORMATION AND POWER

4.1 INTRODUCTION	
4.2 SCHILLER AND MARXIAN THEORY	
4.2.1 Marxian Theory and the Information Society	
4.2.2 Surveillance.	
4.2.3 Marxian Theory and IT in summary	
4.3 GIDDENS AND THE NATION-STATE.	74
4.3.1 Violence and Surveillance	
4.3.2 Organisation/Administration and Surveillance	77
4.3.3 The Nation-State and Surveillance in summary	
4.4 FOUCAULT, POWER-KNOWLEDGE, AND THE PANOPTICON	
4.4.1 The Panopticon	
4.4.2 The Confessional	
4.4.3 The Panoptic Mechanism.	
4.4.4 The Mechanism outside the Institution	
4.5 CONCLUSIONS	

### CHAPTER 5 LEGAL PROTECTION OF PRIVACY IN IRELAND

5.1 INTRODUCTION	92
5.2 THE RIGHT OF PRIVACY IN IRISH LAW	92
5.2.1 Defining Privacy in the Irish Legal Context	93
5.2.2 Ireland's Obligations under International Human Rights Law	94
5.2.3 Privacy and The Constitution and Common Law	96
5.2.4 Legislative Protection of Privacy	
5.3 INFORMATION PRIVACY AND THE LAW IN IRELAND	98
5.3.1 Criminal Damage Act, 1991	99
5.3.2 Official Secrets Act, 1963 and Freedom of Information Act, 1997	101
5.3.3 Data Protection Act, 1988	105
5.3.4 Irish Implementation of EU Directive 95/46/EC	118
5.4 CONCLUSIONS	123

### CHAPTER 6 METHODOLOGICAL ISSUES

6.1 INTRODUCTION	
6.2 METHODOLOGY OF QUESTIONNAIRE SURVEY	
6.2.1 Aims	
6.2.2 Questionnaire Design	
6.2.3 The Final Questionnaire	
6.2.5 Selection of the Study Sample	
6.3 CONCLUSIONS	

### CHAPTER 7 QUESTIONNAIRE RESULTS

7.1 THE GI INDUSTRY IN IRELAND	
7.2 DATA COLLECTION	
7.3 DATA INPUT AND UPDATE	
Same Person	
7.4 NATURE OF DATA STORAGE AND ANALYSIS MEDIUM	
7.5 DATA ACCESS AND SECURITY ISSUES	
7.5.1 General Access Issues	
7.5.2 Internal Access	
7.5.3 External Access	
7.6 DATA PROTECTION.	
7.7 CONCLUSION	

### CHAPTER 8 DISCUSSION OF RESULTS

8.1 INTRODUCTION	
8.2 PRIVACY OF GI IN IRELAND.	
8.3 IMPLEMENTATION OF THE DATA PROTECTION PRINCIPLES IN IRELAND	
8.3.1 Data Protection and Survey Results	
8.4 THE IRISH LEGISLATIVE CONTEXT	
8.5 A COMPARISON OF DATA PROTECTION FOR GI IN IRELAND AND THE US	
8.6 PRIVACY AND POWER.	
8.6.1 Power and the Privacy of GI	
8.7 CONCLUSIONS	197

### CHAPTER 9 CONCLUSIONS AND RECOMMENDATIONS

9.1 BACKGROUND	
9.2 SUMMARY OF FINDINGS	
9.3 CONCLUSIONS	
9.4 RECOMMENDATIONS AND FURTHER RESEARCH	
9.4.1 Recommendations	
9.4.2 Recommendations for Further Research	

BIBLIOGRAPHY	210
APENDICES	254

### LIST OF MAPS

Map 2.1. Yurock Indian Religious World View	26
Figure 2.2: Digital GL- Component Parts	20
Map 2.2: T in O Map	27
Map 2.3: Ethnocentric Mapping	28
Map 2.4: Mackinder's Map	34

### **LIST OF FIGURES**

Figure 2.1: The Data to Wisdom Continuum	10
Figure 2.2: Digital GI – Component Parts	15
Figure 2.3: The Layer Structure of GIS	18
Figure 3.1: Spinello's Categorisation of Ethical Dimensions of IT	49
Figure 6.1: Diagram of Interrelationships of Data Protection Issues	127

on's Six Ethical Issues in the Digital

able 5.2. Date Protection Principles in Ireland

Table 5.3: Registration under the DPA from 1989-199

ale 5.5: Complaints made to Commissioner dodor terms

### LIST OF TABLES

Table 2.1: Location and Attribute Data	12
Table 2.2: Simple Geocoding of Address and Postcode	14
Table 2.3: Examples of Multiple Non-Standard Addresses	16
Table 2.4: Raster and Vector Systems	19
Table 2.5: Attributes in a Raster Systems	19
Table 3.1: Mason's Six Ethical Issues in the Digital Age	48
Table 5.1: Exemptions from the Freedom of Information Act	103
Table 5.2: Data Protection Principles in Ireland	107
Table 5.3: Registration under the DPA from 1989-1996	109
Table 5.4: Breakdown of Registration Based on Sensitive Information in 1996	111
Table 5.5: Complaints made to Commissioner under terms of DPA (1988)	112
Table 6.1: Factors of Importance to Data Protection and Privacy	126
Table 6.2: Final Interviewees	137

### LIST OF APPENDICES

Appendix	One: Data Protection Registration	254
Appendix	Two: Questionnaire	258
Appendix	Three: Initial List of Potential Interviewees	271
Appendix	Four: Template of Letter to Interviewees	273

 RGH
 European Geographic Information Infrastructure

 RSRI
 Environmental Systems Research Institute (makers of ARC/INFO)

 EUROGF
 European Umbrelia Organisation for Geographic Information

 FOLA
 Preedom of Information Act, 1998 (Ireland)

 GI
 Geographic(al) Information

 GIS
 Geographic(al) Information Systems

 GSDI
 Global Spatial Data Infrastructure

 ICCPR
 International Convention on Civil and Polytopi Rights, 1996

 IDMA
 Hish Direct Marketing Association

 IRLOGI
 Information Systems

 IS
 Information Systems

 ISDI
 National Conter by Geogra

### **ABBREVIATIONS AND ACRONYMS**

AGI	Association for Geographic Information (UK equiv. of IRLOGI)
CAD	Computer Aided Design
CDA	Criminal Damage Act, 1991 (Ireland)
CSO	Central Statistics Office
DG	A Directorate General (of the EU Commission)
DPA	Data Protection Act, 1988 (Ireland)
DPC	Data Protection Commissioner (Ireland)
DPR	Data Protection Registrar (United Kingdom)
EC	European Community
ECHR	European Convention on Human Rights, 1950
EGII	European Geographic Information Infrastructure
ESRI	Environmental Systems Research Institute (makers of ARC/INFO)
EUROGI	European Umbrella Organisation for Geographic Information
FOIA	Freedom of Information Act, 1998 (Ireland)
GI	Geographical Information
GIS	Geographic(al) Information Systems
GSDI	Global Spatial Data Infrastructure
ICCPR	International Convention on Civil and Political Rights, 1966
IDMA	Irish Direct Marketing Association
IRLOGI	Irish Organisation for Geographic Information
IS	Information Systems
IT	Information Technology
LRC	Law Reform Commission (Ireland)
NCGIA	National Center for Geographic Information and Analysis (USA)
NSDI	National Spatial Data Infrastructure
OECD	Organisation for Economic Cooperation and Development
OSA	Official Secrets Act, 1963 (Ireland)
OS/OSI	Ordnance Survey (Ireland)
PPS No.	Personal Public Service Number (formerly RSI number)
RDBMS	Relational Database Management System
RSI No.	Revenue and Social Insurance Number (see PPS)
UDHR	Universal Declaration of Human Rights, 1949
UNHCHR	United Nations High Commissioner for Human Rights
Y2K	Year 2000 Bug/Problem
WWW	World Wide Web

Chapter One Introduction

### 1.1 Introduction

The twentieth century and particularly its latter half have been characterised as the Information Age. A rapid succession of new technologies and techniques of information manipulation have followed late nineteenth century developments such as telegraphy. Recent decades have seen the rise of the computer and associated technologies enabling the storage, transfer, manipulation and analysis of information predominantly held in digital form. Such developments have caused changes in everything from government and private sector organisation to the lifestyle of individuals. This is reflected in what are now everyday terms such as Information or Digital Revolution, Information Society, Information Technology, Internet, computer virus and the Millennium Bug (Y2K).

These technologies, originally military in origin, were for a long time the preserve of the only organisations that could afford the huge outlays necessary to purchase and maintain them, such as large government and private sector bodies. The late 1980s and early 1990s have seen a number of developments including the personal computer and user-friendly software, reduced software and hardware costs, and the development of the World Wide Web. These and other developments have made computers a common household item and the Internet a part of everyday language. One indication of these changes is that Bill Gates, the Head of Microsoft, is now the second most powerful man in the UK (despite being non-resident), exceeded in influence only by the Prime Minister (The Sunday Times, 1999).

In a society where such information technologies have become so important and ubiquitous a number of issues of ethical concern have come to light including the question of fair allocation

of information resources, ownership of information, quality of information, and the issue of privacy of personal information. Privacy as an issue in regard to Information Technology was already a concern in the early 1970s, when computer databases were still the preserve of large organisations and particularly of government (Rowe, 1972; Warner and Stone, 1970; Sieghart, 1976). The US Privacy Act of 1974 reflects this since, although it is aimed at databases of personal information it only applies to federal government organisations (Onsrud, 1994). By the 1980s concern had become significant enough to inspire the issuing of Council of Europe Convention on Data Protection that applies to both public and private sector data (Council of Europe, 1981).

Privacy is a concept important to the autonomy of the individual, though notoriously difficult to define. While the notion of privacy has many meanings and a number of distinct focuses, it is generally held to be a right of individuals and is included as such in international human rights conventions. In regard to Information Technology, privacy is most specifically concerned with the treatment of information held on computer concerning an individual (who has access to such private information, how it is used, and so on). While such information has always been collected by some organisations such as government bodies there are two new developments. The first is an increasing amount of collection of such information and the second is the digital recording of what would formerly have been held in paper files. This digital storage means that the manipulation of information is substantially easier as the techniques of information processing and recombination can easily be utilised since both are in the same medium. The potential for the inappropriate use of information provided for specific purposes is therefore vastly expanded. In such a situation the balance of power is not in the individual's favour, as to prevent such misuse would necessitate the refusal to give information and thus would mean opting out of society as such information is now collected as a matter of course.

Such concerns, coupled with the commodification of information that can potentially lead to its being sold to third parties, has led both to concerns about privacy in relation to information, and to legal initiatives such as the introduction of data protection legislation.

### 1.2 Introduction to Geographical Information

One aspect of the digital revolution has been the development of various technologies and techniques for handling Geographical Information (GI) for various purposes. Various initiatives in a variety of disciplines led to what is now known as Geographical Information Systems (GIS) and other GI-related technologies such as Global Positioning Systems (GPS) and satellite remote sensing. Until recently these technologies tended to be separate from mainstream IT products because of the incompatibility of the spatial component of GI with the architecture of information systems that were not GIS. Any item of GI is composed of two types of attribute: its location, and any other characteristics. In general only the latter have been used in non-GI specific software. The former component, however, makes it possible to perform a whole suite of operations on GI that are distinct from other information. At the simplest it is possible to display GI graphically as a map or more complex spatial image (such as a three dimensional surface such as an elevation model). In addition it is possible to perform various spatial analyses of varying complexity where it is precisely the spatial component which is the key to the analysis. If the spatial unit that forms the basis of this analysis is the individual address the potential threat to privacy is substantial, though even analysis of area-based data, if undertaken in a sophisticated fashion has the potential to uncover much personal information.

In the past the complexity of spatial data and the difficulty of representing and analysing it in a computer system meant that GIS packages tended to be large, complex, specialist programs. In the last decade, however, the gap between such Geographical Information Systems and other databases has begun to be broken down with the development of various spatial tools that can be used in normal databases. In addition, recent developments at the data end of the GI industry have led towards the production of geocoded address databases, one of which was launched for Irish addresses in February 1999 by the OSI and An Post (IRLOGI, 1999a). Another trend in recent years has been towards the development of metadatabases: databases that contain details pertaining to GI held by many organisations in order to make the sharing or purchase of data easier and avoid the duplication of effort. One such dataset developed

specifically for Ireland is Geo-ID (Geospatial Information Directory), which was launched on the Internet in October 1999<sup>1</sup>.

The recent trend towards the development of spatial tools for 'ordinary' databases means that data held by organisations with an address component can now practically be treated as GI. Thus, personal data in organisations that have previously not used GIS will be potentially open to manipulation based on its spatial component as well as its non-spatial characteristics, without the organisation necessarily needing to invest in a GIS as such. Coupled with this are the other recent trends in GI: developments in geocoding of individual addresses, the production of metadatabases to enable broader data sharing, and the growing availability of both spatial tools and spatial data over the internet. All of these increase the amount of data that can be treated as GI and the availability of tools to manipulate it, as well as making it possible to conduct such analysis at the level of individual addresses. In addition much of the data that is now potentially capable of being treated as GI are personal data collected for use in standard databases. The potential impacts of the analysis of GI under such circumstances are far greater than ever before.

### 1.3 Reasons for this Study

As has been alluded to above, the past decade has seen many developments that have the potential to enable a vastly increased amount of information to be easily integrated into the realm of digital GI that is useful in practice for spatial analysis. Other developments mean that such information can now be analysed without using expensive specialist GIS packages. Significantly much of the information that can now be considered useful GI includes personal information collected on an address basis. While such information was always GI, the amount of spatial analysis that could previously have been conducted on it was relatively limited in the absence of geocoding.

In Ireland the widespread adoption of GIS technology came relatively late. The Irish Organisation for Geographic Information (IRLOGI) was only formed in the 1990s. For a long time the greatest interest in GIS technology was in the public sector and environmental

<sup>1</sup> http://www.tcd.ie/Geography/GIS/Geoid/index.html

organisations. In more recent years, the most rapid growth of interest has been in the field of marketing and geodemographics (Ovington, 1999). This fact is reflected in the changing membership profile of IRLOGI and the changing focus of the GIS Ireland Conferences which for the first time in 1998 specifically aimed to interest members of the private sector by including a number of presentations on the role of GI in marketing.

Two other developments in 1999 in regard to GI were alluded to in Section 1.2. These are the launch of the An Post/OSI GeoDirectory product and the IRLOGI-funded Geo-ID metadatabase of Irish GI. The former is a database of standardised addresses, each of which is geocoded, developed over a number of years by the OSI in co-ordination with An Post who were responsible for testing its accuracy 'on the ground' (IRLOGI, 1999a). Although IRIS (Irish Regional Information Systems Ltd.), a private sector organisation, has created at least one other geocoded address directory it only covers major towns and cities in order to be cost effective (Appleby, 1998). The OSI/An Post product by contrast aims at complete coverage of the country. At its launch in February the GeoDirectory contained "more than 250,000 validated business and residential addresses in the Dublin numbered postal districts", but will achieve complete coverage of the country by "December 1999" (IRLOGI, 1999a: 6). The chief problems in geocoding Irish addresses are encountered in rural areas due to a problem of non-uniqueness of address formats. However, the combination of the two geocode products means that effectively addresses in urban areas where the vast majority of the population reside can now be accurately placed for GI analysis. In rural areas there is greater difficulty but it is to be anticipated that the completion of the GeoDirectory product will have a major impact.

The production of the Geo-ID product by IRLOGI and the GIS Laboratory in Trinity College Dublin is another important development in this regard. The absence of metadata in regard to GI in Ireland has resulted in a relatively fragmented approach in the past. As organisations were often unaware of the data possessed by others it was often easier to generate new data than try to seek out data already in existence. The Geo-ID product potentially changes this by enabling users to find out not only what data are held where, but also levels of accuracy, formats and other important details such as price and availability. Since this product was only launched in October 1999 it is as yet difficult to assess its impact in regard to personal information. As of October 1999 only a very limited number of datasets appeared in the directory under the two personal data classifications of 'demography' and 'health'. It remains to be seen how successful the database is and whether it is adequately kept up to date. If it is, and if it attracts further submissions from those anxious to share personal information it could prove a very powerful enabling tool. One of its potential impacts would be to ease the greater combination of personal GI from diverse sources, making the protection of privacy in relation to personal GI more difficult.

It is against this background of rising awareness of the uses of socio-economic and demographic GI and of the development of geocoded address lists and a metadatabase that this study was undertaken. It seeks to examine two aspects of the interaction between personal GI and privacy, namely the legal situation in regard to privacy and data protection in Ireland, and the current practices of large organisations holding personal data, whether address-linked or directly georeferenced.

### 1.4 Aims and Objectives of the Study

The aim of the study was to assess and analyse the current situation in regard to the legal and practical protection of privacy with regard to digitally stored personal geographical information. As such the study had two main objectives:

- An examination of the legal status of the right of privacy in Ireland with a particular emphasis on its application to digitally held information
- An examination of the practical methods used to prevent misuse of personal GI and to ensure compliance with privacy and data protection law by organisations holding largescale databases of such information.

To realise the aims of the study, thus, two separate courses of action were undertaken. The former was a study of the literature pertaining to privacy and data protection law in Ireland and of the most important legislation, namely the Data Protection Act (DPA) of 1988, Criminal Damage Act (CDA) of 1991 and the Freedom of Information Act (FOIA) of 1997.

The second part of the study involved selecting organisations that held large databases of personal information. Representatives of such organisations were then interviewed to

determine the protection they provided for the personal GI they held, and to a lesser extent to determine the uses made of it in terms of spatial analysis.

It was expected that the results would show that there is a relatively high level of protection of such information in Ireland, with the Data Protection Act playing a particularly strong role. It was also expected that of the organisations questioned, the majority would have GI that was not being used as such inside a GIS, but rather that such information would typically include address data and generally be stored in non-spatial information systems.

### 1.5 Chapter Outline

Chapter One introduces the subject of the thesis by describing the rise of information technology and its impacts on the use of GI. It also explains the reasons for this study by reference to the privacy-related fears raised by IT in general and GI in particular, and the recent developments in Ireland that have the potential to enable almost any personal information to be used as GI. Finally the aims of the study and its expected outcomes are detailed.

Chapter Two introduces Geographical Information in more detail. The nature of GI and its pre-digital use to exercise power are described. The impact of the digital revolution on GI, first through the use of GIS, and later through its integration into mainstream IT, is described. The final section of the chapter discusses the impacts of these changes on the power of GI and in particular on its potential to be used in ways invasive of individual privacy.

Chapter Three concerns the ethical issues raised by IT and the issue of privacy in particular. The chapter describes the nature of the interlinked ethical questions raised in regard to the use of IT, of which privacy is regarded as one of the most important. It then goes on to describe the legal and philosophical debate about the nature and importance of privacy, and to describe the distinction between privacy and data protection.

Arising out of the discussion of privacy it becomes clear that one of the important attributes of privacy is that it enables a person to develop independent thoughts and modes of action free

from public pressure. This important attribute of privacy is developed in Chapter Four, which discusses the role of information in the exercise of power over people from three main theoretical perspectives. These concentrate respectively on the importance of information to: the power of the state, the power of capital, and the creation of a disciplinary society in which power is exercised over individuals through their own actions in response to observation.

Chapter Five concerns the first of the objectives of the study: the protection of privacy in Irish law. It first examines the general protection of privacy under the Irish constitution, legislation and case law. It then goes on to examine the implications of legislation implemented in response to the so-called 'Information Revolution', namely the Data Protection Act (1988), the Freedom of Information Act (1997), and the Criminal Damage Act (1991). A final section discusses the changes to Data Protection law necessitated by EU Directive 95/46/EC that has yet to be implemented at time of writing.

The succeeding two chapters are concerned with the second objective of the study: the practical situation in regard to personal GI in large Irish organisations. Chapter Six outlines the methodology used to undertake the study. Chapter Seven details the results of this questionnaire survey under the five broad headings: Data Collection, Data Input and Update, Characteristics of the Database System, Access to Information on the System, and Data Protection Compliance.

Chapter Eight discusses the results of the questionnaire survey and the Irish legal situation in the context of the issues discussed in the earlier chapters. It details the current state of practical implementation of the data protection principles in Ireland. A comparison is also made between the US and Ireland in regard to the potential for the use of GI to infringe privacy. Finally the implications of the current use of personal GI for the exercise of power in Ireland are assessed.

Finally, Chapter Nine summarises the background to the concern about the impact of GI on privacy, and the results of the study. It then goes on to draw conclusions regarding the current state of GI use and legislation in Ireland and to suggest useful areas for further research.

### **Chapter Two**

# Geographical Information, Geographic Information Systems and the Issue of Power

"Without maps there are no roads, no signposts, no safe travel, no law, no lawful government and trade of only the most primitive and localised variety. Without maps, travellers get lost and eaten. Here be dragons. An uncharted land can expect governance only by raiding parties exacting tribute; it cannot expect the delivery of measured and daily authority and an assured and lasting peace." (Myers, 1998)

### 2.1 Introduction

This chapter will focus on Geographic Information (GI) and Geographical Information Systems (GIS) and their effect on power relations. This will entail definitions of the central terms such as GI, an examination of the relationship of GI to power historically and in the present digital age, and the implication of the Information Age in vastly expanding the power associated with spatial information. It will be seen that the Digital Revolution has had a dramatic effect on the power potential of GI by vastly expanding the capacity to store, combine and analyse such information, a factor that poses major new ethical and legal problems. While historically GI, though undeniably powerful, did not seriously impact on personal privacy modern information technology in combination with GI creates a slew of new power conflicts and ethical problems one of which is that of privacy.

### 2.2 Geographical Information

Before defining what is meant by Geographical Information it is perhaps a good idea to address briefly the question of the distinction between information and data. In the context of information systems data are what is input, and if manipulated appropriately, information is output. Data and Information are, according to Haywood (1995), part of a continuum which ranges from data to wisdom through information and knowledge (see Fig. 2.1). This continuum is characterised by the addition of value through contextualisation at each stage from data to wisdom, though only the first two steps of the range concern us here. Data are the most basic aspect of this chain and are symbols of one kind or another. Without context they are meaningless. A list of numbers input to a computer comprise data. Out of context these numbers are meaningless, or at the very least may be perceived to have some meaning that is unclear. They require both the exercise of some analysis and a context to make them meaningful.



Figure 2.1: The Data to Wisdom Continuum

To convert such data items into information requires "a process of reception, recognition and conversion, made possible by our cognitive history and our ability to decipher symbols" in the case of human interpretation (Haywood, 1995: 3). In an information systems context, the list of numbers may have been recorded as a set of numbers in a 'field' entitled 'rainfall'. This title converts meaningless numbers into a limited form of information. However, the strength of IT is the ability it gives to link such a field of information with others to provide more useful information. For example, this information if linked to a geographical co-ordinate tells us that this is rainfall at a particular place, and, if linked with other such information for other places may enable the creation of a map of rainfall and the generation of other related information.

The steps from information to knowledge and from knowledge to wisdom are not relevant in an information systems context as only data and information can be involved without the agency of a human to add wider context, despite the attempts to create 'knowledge-based' or intelligent systems. Thus data are what is input into an information system, whether in the form in which a human operator types them in, or in the machine code through which they are stored. The power of an 'information system' lies in its ability to usefully create information from data by linking the data together. Within the Geographical Information community the terms Geographical Information and Geographical (or more often Spatial) Data are often used interchangeably. Thus some of the literature may define spatial data while another author may refer to geographical information though clearly both refer to the same concept. By virtue simply of being given a spatial context it is arguable that much spatial data is already information (though perhaps of a very limited use).

Geographical information is information that is related in some way to some location in space (in three dimensions), and more specifically to a location on earth (including its atmosphere and its interior). Martin (1996: 1) says that GI "in its simplest form...[is] information which relates to specific locations". A more comprehensive definition is given by Haywood (1998: 13) "spatial data are characterised by information about position, connections with other features and details of non-spatial characteristics".

The most familiar example of GI is the map; "a set of symbols recorded in spatial relationship to each other, so that the position of the symbols acted as an integral part of the message" (Chrisman, 1997: 4). Other traditional forms of GI also existed alongside the map and include written records and descriptions, tables and statistical information (Chrisman, 1997; Rhind, 1997). The important factor linking all the diverse forms of GI is the factor of location.

Geographical Information can be subdivided, however, into two basic types hinted at by Haywood's definition. These are the specifically spatial information such as a grid reference, and the non-geographic data, sometimes referred to as attribute or thematic data. The former locates an object in space (and may also implicitly or explicitly describe its relationship to other objects in space), while the latter describe the non-spatial aspect of the object (Fischer, 1996; Haywood, 1998; Huxhold, 1995). Burrough thus characterises GI as describing "objects from the real world in terms of (a) their position with respect to a known co-ordinate system, (b) their attributes that are unrelated to position (such as colour, cost, pH, incidence of disease, etc.)" (1986: 7). Table 2.1 shows a number of examples of location and attribute information types.

11

### Table 2.1: Location and Attribute Data

Location	Attribute Attribute Attribute Attribute		
Georeferenced:	Soil Type		
Latitude, Longitude	Geology		
National Grid Co-ordinates	Elevation		
Geocoded Address Location	Land Value		
	Ownership		
Non-Georeferenced:	Demographic Characteristics		
Postcode or Zipcode	Сгор Туре		
Individual Address	Pollution Levels		
Census Enumeration Area (District	Crime Statistics		
Electoral Division)	Individual Financial Details		
Property Parcel	Insurance Information		

Another way of approaching the issue draws a distinction between 'geographic information', 'geo-referenced information' and 'non-geographic information'. This is merely a different way of drawing the same distinction:

- 'Geographic information' relates specifically to space;
- 'Geo-referenced information' by contrast does not need to be a representation of geography at all, but is merely a "bag of bits with a geographic footprint" (Goodchild, 1997 unpublished);
- 'Non-geographic information' has no spatial link and in consequence includes all other information, provided it is not given a geo-reference.

This leads the author on to create a new term,' Information with a Geographically Determined Interest' or 'IGDI' that includes any information with any geographical component. <sup>1</sup>Effectively this IGDI is the same as what is meant by GI in the context of this study.

<sup>&</sup>lt;sup>1</sup> This type of information includes both geographic information and geo-referenced information, and is designed for a world of Internet exploration of such IGDIs, held on local servers, given that such information is of greatest information closest to the footprint. (Goodchild, 1997).

Geographical Information is thus a twofold matter: locational information and attribute information. In traditional GI this distinction is generally of minor concern as the two aspects of the information are jointly expressed. Thus in a map the location of the object on the map surface reflects its location in real space, and the method used to depict the object gives its attribute information, when read in combination with the map key. In regard to written information a simple example such as the electoral register contains both an address and an associated name or names. The address gives the location, and the name gives the identity of the voter or voters domiciled there. Digital GI is more complex, however, as will be discussed in Section 2.3.

# 2.3 Digital GI and GIS

#### 2.3.1 Problems with Digital GI

Table 2.2: Simple Geocoding of Address and Postcode

Digital GI can be defined in precisely the same terms as non-digital GI, as information referring to a location on earth consisting of two components, a spatial reference and attributes found at this location. A further distinction within GI needs to be drawn in the context of the use of GI in digital operations, however. Though GI typically consists of these two aspects, the specifically spatial and the non-spatial, not all GI is spatially linked in the same way. Thus, GI can be linked to space by a geo-reference or by a less specific geographic locator. A georeference is the method of locating features 'in a model of space' (Huxhold, 1995) and is typically a set of Cartesian co-ordinates in relation to a model such as the Irish National Grid. This ties the information to place defined in mathematically unique way. Other methods can also be used to locate something in space, however. Perhaps the most widely used in everyday life are addresses, and postal codes, though other administrative divisions such as census area codes (or names) also fall into this category. While these are also often very specific they cannot be directly used (for spatial purposes) by machine since they are not mathematically specific.

An address, for example, can clearly be denoted with mathematical precision, either as a point location, or an area location on maps. To a human with appropriate contextual knowledge (a postman for example) an address will convey this place: it is specific. The same is true for many other spatial locators such as postcodes, county names or codes, or census area codes. While these are unique (aside from address which will be discussed below) and have a definite location, they do not convey spatial location in a mathematical sense. For example, the postcode LE2 6BF is unique and refers to a well-defined place, in this case a small area of Leicester in the UK. However, nothing about the postcode itself gives this information about location. A postman will know where it is from knowledge of the postcode system and many others may be able to guess at its location. A computer will not. For this it is necessary to geocode the information, in other words to attach a georeference to the information (Huxhold, 1995). This can be accomplished in a number of ways, the simplest of which is to create a file containing the correspondences between locational descriptors of address such as the postcode and the appropriate georeference as shown in Table 2.2 for both a postcode and an address.

<b>Table 2.2:</b> S	Simple	Geocoding	of Add	ress and	Postcode
---------------------	--------	-----------	--------	----------	----------

Postcode	Centroid Location
LE2 6BF	128054, 723842
of an eddress, and a lutter beating any c	of these variations will reach the recipient
Address	Point Location
6 Hume St, Dublin 2.	250356, 645783

Figure 2.2 shows the constitution of fully georeferenced GI, comprising attribute and spatial data, and shows how a process of geocoding is used to convert non-georeferenced data into georeferenced data.



### Figure 2.2: Digital GI – Component Parts

A second problem arises in relation to Irish GI. This is the fact that as yet Irish addresses are not standardised. Table 2.3 shows four of an even greater number of potential combinations of an address, and a letter bearing any of these variations will reach the recipient. The problem is twofold, that there is no single way that addresses are written, and that in rural areas the absence of street names and numbers also makes addresses non-unique. This lack of standardisation of address means that geographical analysis is complicated in the Irish context both due to the difficulty in matching different instances of the same address, and due to the difficulty of geocoding such non-standard addresses. Additionally alternative spellings of the same placenames may add further difficulty, as may the legal option of using the Irish version of the address.

analysis. Other commentators tend to base their definition on these core attributes of GUS and then stress other additional factors. Thus Husbold (1995: 3) states that a GIS is a "collocore of information technology, data, and procedures" and that it is capable of "analysis" as well to the other operations mentioned above. This spatial analysis function is regarded as toportant by authors such as Huxbold (1991), and Egenhofer and Golledge (1998: 3) who stress that the

#### Table 2.3: Examples of Multiple Non-Standard Addresses

Aodán Edmonds	Aodán Edmonds	Aodán Edmonds	Aodán Edmonds
Farrihy	disparate sources (DoE	, 1987; Rhind, 1988; I	ionham-Carter, 1994), a
Broadford	Broadford	Broadford	Béal an Átha
Via Charleville	Rathluirc	thaps one of the most	Ráthluirc
Co. Limerick	Co. Cork	Co. Limerick	Contae Luimní

#### 2.3.2 GIS: Geographic Information Systems

GIS technology is a relatively recent development that has come about due to the ongoing amalgamation of innovations and ideas from a variety of disciplines (DeMers, 1997; Huxhold, 1995). This, coupled with the desire of many to profit from the use of the term by renaming their unchanged product a GIS (Maguire, 1991), has led to the production of a multitude of different definitions (Haywood, 1998; Huxhold, 1995; Burrough, 1986). Each of these stresses particular aspects of GIS depending on the interests and background of the person defining the term (Haywood, 1998). There is, in consequence, no single universally or even widely accepted definition of GIS (DeMers, 1997).

A relatively simple definition of GIS given by Maguire (1989: 171) is that a GIS is a collection of "integrated systems for the collection, storage, manipulation and presentation of geographical data". Many definitions stress these and similar aspects of GIS, namely the fact that they are systems (though not necessarily computer systems) that collect, store and manipulate spatial data and present some form of output (Burrough, 1986; Obermeyer and Pinto, 1994; Burrough and McDonnell, 1998). According to Haywood (1998) three components make up a GIS: a computer system, geographical data and manipulation and analysis. Other commentators tend to base their definition on these core attributes of GIS, and then stress other additional factors. Thus Huxhold (1995: 3) states that a GIS is a "collection of information technology, data, and procedures" and that it is capable of "analysis" as well as the other operations mentioned above. This spatial analysis function is regarded as important by authors such as Huxhold (1991), and Egenhofer and Golledge (1998: 3) who stress that the

ability to render the results of "detailed analysis" in visual form is "one of the greatest strengths" of GIS. Worboys (1995: 1) stresses that GIS is "computer-based" and to 'analysis' also adds "retrieval" and "modelling". Other attributes that are stressed are: integration of data from potentially disparate sources (DoE, 1987; Rhind, 1988; Bonham-Carter, 1994); and the fact that it is the interaction of human and computer systems with the geographical data which constitute the GIS (ESRI, 1993). Perhaps one of the most widely used definitions of GIS is that from the Chorley Report "a system for capturing, storing, checking, integrating, manipulating, analysing and displaying data which are spatially referenced to the Earth" (Department of Environment, 1987: 132).

The Chorley definition is quite a comprehensive one that is widely quoted. It, and many of the definitions above fall into the category of what Burrough and McDonnell (1998: 11) describe as "toolbox definitions" that concentrate on the tools available within a system. Burrough and McDonnell (1998) also identify two other major trends in definition, those that emphasise the difference between a GIS database needing to deal with spatial phenomena, and those that emphasise the organisational structure within which the tools are used. Bonham-Carter (1994: 1) belongs to the former category, describing GIS as "computer tools for manipulating maps, digital images and tables of geocoded (geographically located) data items...designed to bring together spatial data from diverse sources into a unified database...all of which are in a spatial register, meaning they overlap correctly at all locations". This definition, unlike the others stresses the importance of database structures to deal with specifically spatial aspects of data, a factor that will be discussed later. From an organisational viewpoint the ESRI (1993: 1-2) definition stresses that a GIS is "an organised collection of computer hardware, software, geographic data, and personnel" as well as describing the tools used.

There is, however, an aspect of the nature of GIS that these definitions all largely ignore, namely the reason for this manipulation of spatial data. Burrough (1986: 6; Burrough and McDonnell, 1998: 11) states that the various operations on the data are conducted "for a particular set of purposes". The importance of this is that all of the integration, manipulation and analysis, in whatever database and organisational setting, is expected to produce not only output, but useful output. DeMers (1997) ignores the traditional list of operations to be performed on data to concentrate on the purpose of GIS manipulation. Thus GIS are "tools that allow for the processing of spatial data into information, generally information tied

17

explicitly to, and used to make decisions about, some portion of the earth" (DeMers, 1997: 7). The importance of this definition is that it clearly distinguishes one a key characteristic of GIS, namely that from spatial data it produces spatial information that can be used to support decision making.

There are two main types of traditional GIS system architecture: raster and vector. Three dimensional data are also sometimes stored as Triangulated Irregular Networks (Martin, 1996) and in more recent times interest has also developed in Object-Oriented Systems which store each individual spatial object with all of its associated information discretely (Goodchild, 1995). Both of the traditional architectures, which constitute the majority of widely used packages, store data as a series of layers of individual attributes (see Fig. 2.3). Some of the differences between the two system-types are substantial as can be seen from Table 2.4 that highlights major differences between raster and vector.



Figure 2.3: The Layer Structure of GIS

Source: Huxhold (1995)

Table 2.4: Raster and Vector Systems

Raster contraction and and and and and	Vector any of the leading GLS packages had any
Grid of Cells	Points, Lines (vectors) and Areas
Topology Implicit	Explicit Storage of Topology
Each Cell Coded	Each Individual Feature Coded

What they have in common, however, is that locational and attribute information is stored in distinctly different ways. This returns us to the nature of GI, and to the database definitions of GIS. The twofold nature of GI creates problems in database architecture because as well as the traditional concern of databases with "entity and attributes", GIS must also deal with the location and topology of these entities (with attributes) (Burrough and McDonnell, 1998).

Thus in a typical vector system such as  $ARC/INFO^2$  details of points, lines and areas are stored along with their topological interrelationships. Each of these geographic features also has an identifier which is used to link these spatial characteristics with attributes stored elsewhere using the same identifier. In raster systems such as Idrisi<sup>3</sup> the spatial data is stored as a grid of cells of defined dimension with a definite origin. Each has a value, which in turn links an individual cell with the attributes associated. Thus all grid cells with a value of '1' might be water bodies, while all cells of value '2' are arable land (See Table 2.5).

Cell Value	Associated Attribute
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Water
definition of GIS can be taken	Arable Landuse
3 a there would not regard as	Pastoral Landuse
4	Residential Landuse
5 been a problem of all GI	Industrial Landuse
6	Recreational Landuse

Table 2.5: Attributes in a Raster System

<sup>&</sup>lt;sup>2</sup> Produced by the Environmental Systems Research Institute, Inc., Redlands, California.

<sup>&</sup>lt;sup>3</sup> Produced by Clark Labs for Cartographic Technology and Geographic Analysis, Clark University, Worcester, MA.

According to Van Oosterom (1993) the difficulties of dealing with spatial data because of the differences between spatial and attribute have led to many of the leading GIS packages having a dual architecture. In such cases attribute data is stored in a relational database, while spatial data is stored in a separate subsystem. This is the case with ARC/INFO, for example, which was originally written as two separate components ARC for spatial data, and INFO for attribute data. INFO was written as a relational database system. Thus a large component of this leading GIS package is actually very similar to relational database systems in use in the mainstream IT industry.

### 2.3.3 GI in Information Systems: GIS and IS

The fact that leading GIS packages traditionally use non-spatial database technology for a large portion of their operations prompts questions about whether GIS is really very different from other information technology. In effect the differences are more of emphasis than anything else. According to Obermeyer and Pinto (1994) it is the reliance on space as an organising framework and the ability to do geographical analysis that separates GIS from other information systems. As we have seen the unusual characteristics of GI have necessitated unusual adaptations in data storage and manipulation. Most authors appear to agree that the use of spatial information and the performance of spatial tasks are the defining characteristics of GIS.

There has, however, always been substantial uncertainty regarding the precise boundaries of GIS. This is in part due to the difficulty of defining the term. Thus Burrough's (1986) definition of GIS can be taken to include systems with low or no analytical capability which others would not regard as 'true' GIS such as Computer Aided Design packages, and automated mapping packages. Indeed, according to Rogerson and Fotheringham (1994) this has been a problem of all GIS: that for a long time the design emphasis was on storage, retrieval and display resulting in poor analytical capability. Thus not only is there a problem of definition of GIS but the spatial analysis capability that many feel is the core of GIS has often been weak. In addition, large components of many GIS packages are actually mainstream (non-GIS) database packages or are modelled on them. In effect the only

remaining uniqueness of GIS is the use of spatial data, since spatial analysis is not always considered necessary, and is often weak.

In addition, GIS is no longer a small isolated technology used by a small community but has become a "mainstream" part of the telecommunications revolution (Curry, 1998: 1). According to Rhind *et al.* (1997) a potentially understated estimate of the value of the GI market in 1996 was \$2000 million, with an annual growth rate of between 10 and 20%. The result is a situation where "geographical technologies – geographical information systems, global positioning systems, remote surveillance systems and automated cartography – are everywhere to be found" (Curry, 1998). This growing importance of the GI industry has been recognised in the US by the presidential mandate for the National Spatial Data Initiative (Rhind *et al.*, 1997), and by European Commission (DGXIII) support for a similar project, the European Geographic Information Infrastructure (De Bruine, 1999).

This leads to questions regarding the uniqueness of GIS, and whether it is actually an industry being drawn completely into the fold of mainstream IT in what one commentator has called "the demise of GIS as a boutique industry" (Reeve, 1997, unpublished).

### 2.3.4 The Demise of GIS

While the GIS industry has traditionally seen itself as quite separate from mainstream IS the difference is not as great as it seems:

- GIS use non-spatial data structures for much of their data
- GIS do not all stress spatial analysis, and the quality of analysis is not universally high
- GIS is being drawn closer to mainstream IT as it becomes highly profitable

In this situation the spatial data basis of GIS may not prove to be as distinctive as has been thought. This is perhaps what leads Bernhardsen to say that GIS "signify much more than a software system that processes, stores, and analyses geographical data" but is "associated with any activity involving geographical data" (1999: 2). Obermeyer and Pinto (1994: 4) point out that "other types of information systems are also spatially referenced – the inclusion of street addresses or zip codes instantly makes them so". It thus becomes clear that the differences
between regular IS and GIS lie in the use of georeferencing, and in the associated ability to do analysis that is both specifically spatial and cannot be done by regular information systems. Examples of the latter include the overlay, route analysis and cookie cut operations typical of most mainstream GIS.

The fundamental difference is the underlying presence or absence of a 'model of space'. However, even this distinction is being challenged in recent years. Non-spatial IS can, as has been mentioned above, store and manipulate GI of certain kinds. It can also perform certain limited geographical analysis. Thus, for example, if one has a database that includes details of shopping habits for individuals together with addresses and postcodes it is trivial to group the other characteristics by postcode and then to analyse them to produce a profile of the shopping habits of people living there. This could then form the basis of a direct mailing campaign directed to specific postcodes. What cannot be done is to map and thus geographically visualise the results.

Two recent developments have changed this, however. These are the growth of the Internet, and the development of spatial data tools for users of regular information systems (Reeve, 1997, unpublished). The rise of the Internet is one of the most significant developments of the 1990s. Prior to this it was a relatively minor technology, but the development of the World Wide Web in the early 1990s has led to an explosion in internet use: "the internet is probably now the most rapidly expanding technology – ever" (Calvert *et al.*, 1997). Part of this growth has included GI. It is now possible not only to access GI over the internet but also to run applications by remote file query and exercise "data-to-information applications supplied remotely" (Lencowski, 1997). Though some problems such as speed of transfer and volume of data have still not been resolved "the vision of GIS as an integrating technology probably can only be realised if the Internet does prove successful" (Calvert *et al.*, 1997). The importance of this is that GI can be accessed remotely and that spatial analysis can be carried out using tools located elsewhere to produce usable information. The user in future will not be tied down to a GIS toolbox located locally.

The second major recent development has been the development of spatial tools for standard databases. These take advantage of the fact that GIS have always tended to be dual systems making use of standard databases side by side with a spatial model and spatial tools to create

such tools for use with standard software such as Oracle, and Microsoft Access (Reeve, 1997, unpublished). The result of both these new developments is that anybody who wishes to use GI and analyse it spatially may now do so without needing to use a GIS. In short "the global ubiquity of geospatial information, supported by global connectivity, will continue to change the primary uses of information" (Lencowski, 1997: 88) and such use will not merely occur within traditional GIS.

There are a number of consequences of these developments. The first is that the GIS industry is increasingly being referred to as the GI industry as the information becomes more important than the system. This is reflected in the names of representative organisations such as IRLOGI, the "Irish Organisation for Geographic Information". The second is that GI analysis and what is traditionally called GIS will not disappear, but rather will become (and to some degree already have) part of a wider and ubiquitous information technology that incorporates spatial models, spatial tools and GI together with non-spatial data. The demise of GIS as a boutique industry does not mean the death of GIS but rather its transformation. One of the key factors in the original importance of GIS, its ability to function as an integrative technology taking spatial data from many sources and adding value to them to create information, has been enhanced by these changes. Ultimately this is the power of GI, and of its analysis in spatial terms: according to Rhind (1997: 9) the linking of datasets "vastly expands the range of applications" that can be undertaken. For example the combination of twenty datasets for a particular area will yield "190 pairs of sets" and over a million total possible combinations which can be used for analysis (ibid. 9). Thus the power of spatial analysis has grown precisely because it is no longer confined to the boutique industry of GIS and is now more widely used and can integrate more data from different sources. The final consequence is that the emphasis needs to shift from GIS to GI. GI is becoming more widely used in more forms than ever before, and the power of spatial analysis of that data is greater than ever before.

# 2.4 Pre-Digital GI and Power

Having discussed the nature of GI and the changes wrought by the Information Revolution it is now proposed to look at interrelationship between power and GI historically. Accurate useful GI in its most basic form, the mental map, allows people the power to navigate their environment safely (Downs and Stea, 1977) and thus to survive. The type of power at issue in this context is, however, more specific than the power to cope with and even master the physical environment. Instead it is intended to look at the role of GI in the exercise of social power. More specifically it is intended to look at the way in which GI, particularly in the form of the map, has been used as an instrument of power, generally by vested interests of one sort or another, in a variety of ways.

Prior to the early 1960s and the embryonic beginnings of digital GIS, GI existed in a number of diverse forms, the most obvious being the paper map, though "no substance has escaped being used to frame an image of the world we live in" (Wood, 1992: 4). Thus it also included the "stick charts" of Marshall Islanders in the Pacific, Eskimo "coastal maps in ivory" (Wilford, 1982: 7) and a profusion of other culturally specific graphic depictions of space. There was also a wide variety of non-graphic repositories of GI including written or other verbal descriptions, various statistical and other information, the individual person's mental or cognitive 'map', and, from the late 19th century onwards, aerial photographs. Although GI is extraordinarily diverse, however, the majority of examples used will be cartographic because "the most complete and consistent descriptions of the geography of the world have long been given in this form" (Rhind, 1997: 3).

Though the use of GI as an instrument of power historically will be discussed under a number of specific headings it should be remembered that these headings are not mutually exclusive. It should also be noted that they are not completely comprehensive. The use of GI as a tool of power will be discussed under the headings: Creation of World Views, Land Ownership and Taxation, Colonialism, and Military/Political GI.

# 2.4.1 GI and World Views: The Creation of Place

"... this, essentially is what maps give us, reality, a reality that exceeds our vision, our reach, the span of our days, a reality we achieve no other way." (Wood, 1992: 5)

As this quotation indicates one of the chief functions of GI, and a major source of its power is in the construction of reality by giving order and meaning to the world. One of the most fundamental ways in which people do this is through the creation of the mental maps, something that appears to be a basic human activity (Downs and Stea, 1977).

A mental map can be defined as the spatial understanding of each human being: the picture each of us has of the world and reflects reality as it appears to us. Such a mental map has two components: information which is derived from personal experience and has such practical uses as finding one's way, and information which is derived from outside sources and which makes up ones picture of the world outside one's experience (Gould and White, 1992). Both elements of the mental map are powerful: the former because it enables the solving spatial problems and thus surviving, and the latter because it gives meaning to the wider world. Whatever the sources of information available and used, however, they represent the world as it is to the individual: a collection of organised knowledge that can be manipulated to solve spatial and other problems (Downs and Stea, 1977). It may not represent empirically measured external reality, however. "It reflects the *world as some person believes it to be*; it need not be correct" (Downs and Stea, 1977: 6). While such mental maps vary between individuals they tend to be more similar between people of the same culture, particularly in relation to the creation of a wider world picture.

One common tendency is to see one's own place as the centre or most important place in the world. In traditional societies this orientation of the world around an ethnocentric 'centre-point' was religiously justified by the division of the world into sacred and profane space on the basis of mythical events and religious meanings (Eliade, 1987). Typically the sacred is the 'world' of one's civilisation with its associated gods, and the surrounding 'chaos' constitutes the profane space of the rest of the world (Eliade, 1987; Tuan, 1975). Map 2.1 displays such a cosmology as a map.



Map 2.1: Religious World Views: The World of the Yurock Indians Source: Tuan (1977)

This tendency to place oneself at the centre of the world map is remarked upon by Harley (1989: 6) who points out that "such a rule is as evident in cosmic diagrams of pre-Columbian North American Indians as it is in the maps of ancient Babylonia, Greece or China, or in the medieval maps of the Islamic world or Christian Europe". The maps of medieval Europe referred to by Harley are known as *Mappae Mundi* or 'T in O' maps, and in many ways closely resemble the world image of the Yurocks. In this case they reflect Christian beliefs and so are centred on Jerusalem, and represent the rest of the surrounding world in a schematic fashion largely based on interpretations of the bible (Robinson, 1984; Wilford, 1982; Black, 1997). Map 2.2 is an example.



Map 2.2: A T in O Map Source: Wood (1992)

Such maps create a sense both of love of homeland and also reinforce the power of the religious orthodoxy which is seen to be the basis of the shape of the world. Such social cohesion and patriotism can be exploited by institutions such as the priesthood or the elite that rules the society. Thus Harley (1989) makes the point that "ideological 'Holy Lands' are frequently centred on maps. Such centricity, a kind of 'subliminal geometry', adds geopolitical force and meaning to representation." (Harley, 1989: 6). This phenomenon does not end with the secularisation of society since non-religious world views are often buttressed in precisely the same fashion.

#### 2.4:2 GI, Land Ownership and Taxation

Until relatively recently the tendency was for a great many world maps to centre themselves on Europe and thus to both reflect and bolster the perceived importance of Europe. One of the most important symbols of this Eurocentrism was the Mercator Projection which exaggerates the relative size of what is now the developed world (and thus the colonial powers) at the expense of the rest of the world (Wood, 1992). This, according to Harley (1989: 6) "helped to confirm a new myth of Europe's ideological centrality" and "support[ed] the perspective of colonial or neo-colonial powers in the northern hemisphere" (King, 1996: 37). Although the centrality of Europe has been challenged by many initiatives such as the Peters Projection (King, 1996; Black, 1997; Wood, 1992), such ethnocentric mapping has not disappeared. Harley (1989) notes the same ethnocentrism in American maps of the American hemisphere, while Map 2.3 shows a Chinese example of such ethnocentric mapping.



# Map 2.3: Ethnocentric Mapping Source: Chaliand and Ragean (1986)

"In those days Caesar Augustus issued a decree that a census should be taken of the entire Roman v orld." An veryoue want to his own town to register. So Joseph also went op from the town of Nacanati in Gables to udea, to Bethlehem the town of David, because he belonged to the house and line of David ". (Lake 2: 1-5)

### 2.4.2 GI, Land Ownership and Taxation

"Maps naturalise and formalise, fixing constructions of identity and geography. And since they are often associated with conservative reinscription of the *status quo*, with enclosing and circumscribing geographies and identities, maps tend to fix dominant ways of seeing geography and hegemonic constructions of identity." (Philips, 1997: 45)

As this quotation indicates maps often serve the interests of the powerful in society and thus help them to maintain the *status quo*. One of the most important and oldest such uses of GI is in the maintenance of systems of land ownership. Once established these create a "need to establish records of transactions and agreements that were independent of individual or collective human memories" (Burrough and McDonnell, 1998: 1) and thus ensure that ownership and the tenure system are secure. The development of the techniques and technology of mapmaking from earliest times were bound up with the recording of ownership (Chrisman, 1997). As well as the recording of ownership and transactions this process also involves valuation and the collection of property tax.

According to Chrisman (1997: 3) "some of the first written records from Mesopotamia and Egypt contain property boundary information as a part of legal transactions". Not only this but they also accurately mapped such information as field boundaries with the names of their owners (Wilford, 1982; Chrisman, 1997).

In Classical times this trend continued and the Romans were the first to use an actual state register, "the *capitum registra*", and employ state surveyors (Bernhardsen, 1999; Chrisman, 1997; Burrough and McDonnell, 1998). One of the main purposes of this register aside from legitimating the ownership of land was the maintenance of an accurate record of the tax base. This factor also influenced Roman administration in other ways, causing them to take regular censuses such as that described in the Book of Luke<sup>4</sup>. The term 'census' itself reflects this; 'census' is originally a Latin term meaning "valuation of every Roman citizen's estate; registering of a man (his age, family, profession, etc.); sum assessed; property" (Oxford Latin

<sup>&</sup>lt;sup>4</sup> "In those days Caesar Augustus issued a decree that a census should be taken of the entire Roman world.....And everyone went to his own town to register. So Joseph also went up from the town of Nazareth in Galilee to Judea, to Bethlehem the town of David, because he belonged to the house and line of David." (Luke 2; 1-5)

Minidictionary, 1995). The connection of the term to taxation is clear from the fact that it is a valuation or an assessed sum.

Although the part played by mapping in land ownership in Europe declined after the fall of the Roman Empire, though the part played by census-style GI continued. Until the 1500s land was registered using written records based on surveys, the most celebrated example being the Domesday Book. The Domesday Survey was an expression of William the Conqueror's desire to know "about the land, how it was peopled and with what sort of men" (Loyn, 1982: 144). The result was the "Domesday Book where the particulars of every strip of inhabited land in the country were recorded" (Tetlow, 1974: 11). The details recorded included what was owned, where, how much land was owned and its value (Loyn, 1982), and also, according to Bernhardsen (1999: 29) "a count of inhabitants and livestock, as well as incomes earned and taxes paid". Taxation was central to the purpose of the survey which "incorporated elaborate statistics relating to the assessment of each estate, the population, the wealth, and the value" (Loyn, 1982: 146). The importance of the survey extended beyond this, however, since it was a record of and aid in the introduction of feudal land tenure and the associated new legal system (Loyn, 1982).

From the 1500s on maps began to reappear in association with land records, generally in the case of disputes and "when the production of maps escalated after 1500 it was particularly maps of this sort that were drawn" (Harvey, 1993: 79). Gradually the detailed surveys in set written form began to be supplemented by maps, and by the late 1500s the two forms began to merge, so that surveys began to produce maps, and maps were used as part of land settlements (Black, 1997; Harvey, 1993). Such property maps eventually acquired such legal significance that now the map boundary is the legal boundary regardless of whether or not there is any indication of this boundary in the physical landscape (Wood, 1993).

# 2.4.3 GI and Colonialism

GI played a large role in the exploration and colonisation of the world undertaken by certain European nations from the 1400s onwards. Advances in techniques of mapping and navigation on the one hand enabled the voyages necessary, while on the other hand the information brought back from 'new' lands expanded the store of GI in Europe. An additional role played by GI was in the legal and moral justification of European claims to the newly discovered lands.

The legal use of GI exemplified by the use of maps to record land ownership has its parallels in the colonisation of the non-European world where legal decisions to draw lines on maps impacted on the course of history. An early example of this is the Treaty of Tordesillas. A Papal decision in 1493 to divide the New (non-Christian) World between the two kings of Spain and Portugal was based on a selected line of longitude, inscribed as the Tordesillas Line on sixteenth century maps (Black, 1997). The uncertainty of methods used to measure longitude at the time enabled the Portuguese to claim what later became Brazil as 'Terra del Rey de Portugal' and thus "the purely abstract line on the map ... comes to dictate the terms of subsequent history" (King, 1996: 27).

In the 19th century by a very similar process almost the whole of Africa, previously virtually unknown, added to the empires of Europe (chiefly Britain and France). At this time Africa was largely unexplored and thus an empty space on maps. This allowed the assumption to be made that the land was empty and ripe for exploitation, forming part of the overall Victorian use of science to legitimate imperial expansion (Muir, 1997; Jackson, 1992). Native cultures could not argue with the logic of these maps in the construction of which they had had no say (King, 1996). Similar uses of 'silence' regarding native cultures on maps is evident in North American civil and military maps, and in the mapping of Latin America by the Spanish and Siberia by the Russians (Black, 1997).

The practical division of Africa was also heavily GI-based, although this GI did not reflect actual African geography. In 1885 the Berlin Conference completed the division of Africa by the European powers, based upon the needs of the European industrialists, and on European rivalries, and conducted largely in the absence of any actual information regarding conditions on the continent (Dikshit, 1997; Muir, 1997). As a result the imposed boundaries showed no connection with or understanding of the pre-existing spatial organisation of peoples within the continent (Douglas, 1997; Muir, 1997). The resulting boundaries remained after decolonisation so that "lines drawn on maps at the conference tables of Europe, according to the interplay of Great Power politics and in partial ignorance of the territories concerned and

their human contents, have, for all their many faults, served to define the 'power containers' of the modern state system" (Muir, 1997: 199).

Just as a refusal to map the presence of native peoples have been used to justify appropriation of their lands, so too has the use of an unusual form of GI, the placename. In many colonial situations the renaming the land was a psychological "ritual of conquest" (King, 1996: 28). The assumption of the right to name the territory implies ownership. It also effectively destroys or drives underground the cultural landscape that existed up to that time: in New Zealand "the intricate pre-colonial geographies of the Maori were erased....as a first step, it was renamed in a replay of the process of asserting dominion spelt out in Genesis" (Pawson, 1992: 23). The fact that many of the names imposed had strong military resonance's further emphasised the conquest that had taken place. Maori names only remained predominant in less favoured areas where "remnant Maori populations" persisted (*ibid.* 23). Similar renaming occurred in North America where the persistence of new names became a reliable indicator of the success of colonisation (King, 1996). The psychological importance of these names is reflected by the recent attempts to have Mount McKinley in Alaska renamed Denali, which were vetoed at federal level by non-Alaskans causing considerable resentment of continuing cultural imperialism among native peoples (Harley, 1990)<sup>5</sup>.

# 2.4.4 GI and Military/Political Power

As is clear from the colonial examples listed GI has significant political and military importance. Its uses include the actual planning and carrying out of military engagements, the use of propaganda mapping, geopolitical analysis, and the resolution of boundary disputes. It is significant that according to Black (1997: 2) the oldest printed historical atlas in the world from twelfth century China "reveals that from the outset the selection of maps and presentation of material...involved issues of politics and propaganda".

<sup>&</sup>lt;sup>5</sup> The power of placenames is not confined to conquest: King (1996: 112) points to names such as "Wealthy City" that are hoped to be "self-fulfilling prophecy", while the inappropriate naming of the Great Plains as 'The Great American Desert' effectively delayed settlement for over a generation (Billington, 1979; King, 1996; Bowden, 1976)

Perhaps the most important military use of GI is as a planning and operational tool, a fact highlighted by the fact the military origins of many cases national survey bodies (Bernhardsen, 1999). In Britain, for example, the three official cartographic bodies are all military: the Ordnance Survey, the Office of the Hydrographer of the Navy, and the War Office (Jewitt, 1992). One of the earliest comprehensive surveys in Europe was conducted in Scotland after the Jacobite rebellion of 1745 while the origins of the Ordnance Survey itself lay in the need to have maps of potential battlegrounds in the event of a Napoleonic invasion half a century later (Black, 1997). During the earlier War of the Spanish Succession much of the success of the Allied armies under Marlborough was due to accurate information on the terrain of individual battlefields gained from personal reconnaissance and detailed surveys conducted by British engineers (Churchill, 1969).

Aside from the use of GI in military operations it also may have a considerable impact on making them necessary. A large number of the world's wars are fought over disputed boundaries, including the 1998-1999 Ethiopia-Eritrea War, fought over an undefined boundary, and the ongoing conflict between India and Pakistan in Kashmir, fought over the disputed ownership of the whole state. Two such boundary disputes in the 1840s provide one of the most explicit examples of the linkage of GI and political and military power.

In the 1840s the US was in conflict with both the UK government and the Mexicans over disputed borders in Oregon and Texas, a situation exploited by James Polk to win election to the presidency. "Realising that the people were more concerned with the annexation of Texas and the occupation of Oregon...[he] pledged himself to secure the transcontinental boundaries needed to make the United States a world power" (Billington, 1970: 382). Oregon, in particular, was one of the keys to Polk's election victory: his election slogan, "fifty-four forty or fight", referred to the latitudinal extent of the American claim (*ibid.* 533). Once in power Polk came to a compromise with the British in 1846, settling the border at the 49<sup>th</sup> parallel, but the claim in Texas led to war with Mexico which resulted in complete victory for the US (Billington, 1970). In the resulting Treaty Mexico was forced to surrender the Texas claim and California and the rest of the southwestern United States. Through these two actions Polk

almost doubled the size of the United States and made it a world power by gaining control of the Pacific coast (Billington, 1970)<sup>6</sup>.

On a global scale geopolitics (the study of way in which the geographical realities of the earth impact on global politics) has had a huge impact on the course of events this century. The most influential geopolitician of the century was Sir Halford Mackinder whose ideas, first enunciated in 1904, influenced politics until after the Second World War. His fundamental thesis was that the steppe land of Asia was the 'geographical pivot of history' that dominated the world so long as it was united (Mackinder, 1969). A major influence on his ideas seems to have been the Mercator Projection which he used to present his ideas (disguised by being framed by an oval border) which exaggerates the size and thus importance of Russia (Map 2.10).



Map 2.4: Mackinder's Map Source: Mackinder (1969)

<sup>&</sup>lt;sup>6</sup> A significant military role in the 'Bear Flag Revolt' was played by a team of US army surveyors mapping the South West, illustrating in a particularly vivid way the connection between GI and military power (Billington, 1970)

#### 5.1 Digital GI and Privacy: Issues and Examples

These ideas had a large impact on international politics at the time and later, influencing among others the German geopoliticians of the Nazi era, and therefore playing a role in the invasion of Russia. After World War Two, though airpower had changed the nature of global geopolitics, a fact recognised by the US, Mackinder's ideas continued to have importance, helping to convince the West of the danger posed by the USSR. During the Cold War both sides used maps that suited their own purposes to convince their people that hostile enemies surrounded them.

# 2.5 Digital GI and Power

As can be seen GI has always been an instrument of power, both in terms of achieving a desired result involving movement in space, whether winning a battle or finding the way home, and in terms of serving the interests of certain groups, particularly those in power, over others. The impact of the digital revolution on GI has changed the way in which it is used quite substantially as has been seen. The consequence has been the magnification of the amount of information that can be combined and the increase in the speed and power with which it can be manipulated (Rhind, 1997). One particular difference between the traditional power of GI and digital GI is scale. Formerly GI, if used as a method of exerting power over people was used at the scale of populations or groups, but not at the level of the individual. Although in the past census information and land ownership information has been collected on an address by address basis it was impractical to use it on this scale since the amounts of data were to large to be conveniently individually handled in analogue form. Similarly, though individual houses could be placed on a map it was not practical to associate other information. This is no longer the case. Now digital GI allows "the shift of the focus of attention from a geographic area to an individual feature. Data layers composed of simple features are the basic building blocks for the data which will flow over a nation-wide spatial data infrastructure" (Morrison, 1997: 19).

#### 2.5.1 Digital GI and Privacy: Issues and Examples

GI and privacy intersect on a number of different scales. Traditionally, as has been seen, GI has tended to be seen as focusing on larger scale matters than the specific individual in a population. As can be shown, however, such a view is based on a narrow definition of GI as being only concerned with map and aerial images, ignoring the often-associated statistical information. According to this view " geographic information has nothing to do with personal privacy - geographic information is factual information about land and resources" (Onsrud et al, 1994).

This view of GI is plainly no longer applicable in a world in which GI is being used not only in making land resources decisions but also decisions regarding individuals, based on characteristics of those individuals gleaned from them personally or extrapolated from known characteristics of the small areas in which they live. An example of this phenomenon is the fact that "the ability to integrate data by tying that data to its geographic location is one of the marketing industry's most promising tools in compiling data from widely disparate sources on households and individuals" (Onsrud *et al.*, 1994: 1).

In this regard what is in some ways an even more worrying development is that where data protection legislation prevents the cross-matching of actual information on individuals ways may be found to circumvent this through the use of detailed geographical statistics. Thus "it is perfectly legal to make decisions about individuals based on a data profile, a construction of suppositions, but not to make decisions based on facts" (Curry, 1994). The result is a highly detailed picture of an individual's likely characteristics being built up and used in ways that affect the individual, rather than using actual information on the individual. Though the person's information is thus technically protected their privacy can still be invaded due to the highly detailed nature and small scale of the various types of information used is not 'real' information but rather is conjectural any decisions taken are less certain and thus this could have adverse consequences for the individual (Curry, 1994; Curry, 1998).

Curry (1994, 1998) also points out some other important issues with regard to GI and its use. The first is that of "the widespread availability of unregulated data" (*ibid.*) which makes it very difficult to know which data are accurate and timely, and thus increases the risk to the individual from decisions made with an inadequate information base. Secondly the widespread use of GI in GIS means that such information is conferred with all of the power of mapped information. Though information may actually exist as a table of statistics regarding an area (census district for example) once it is mapped it has a much greater power to convince and the result can be that "one infers" from the average characteristic of any area "that any given individual within the area will have that characteristic" (*ibid.*). Finally Curry (1994) points out that technological change as it occurs can alter the expectation of people for privacy. This is not only the case in regard to the expectations of the ordinary individual who gradually becomes accustomed to new privacy invasions, but can also manifest itself in the lessening of the right to privacy in law as judges make decisions based on this perception of what is reasonable (Curry, 1994). This danger is one reason for the institution of comprehensive privacy laws that will prevent such gradual relaxation of privacy protections.

With regard to examples of the changing nature of privacy in regard to GI examples are numerous and varied and range from the areas of remotely sensed imagery to that of small scale marketing information compiled purely in tabular format on databases. In some such cases the invasion of privacy may be purely incidental as in the case where aerial photographs or highly detailed satellite imagery is created for a purpose such as resource location but flight paths pass over private property. Alternatively the compromising of individual privacy may be integral to the purpose of the collection of the data as is the case in the marketing sector where such information is used to target particular potential customers or in government where such information may be used to tackle crimes such as welfare fraud.

In the area of active surveillance from above privacy interests have not been very directly affected until recently. While some countries, notably the US and former USSR have long had the ability to detect high levels of ground detail (as little as a few inches resolution) their spy satellite imagery was highly secret and thus did not tend to interfere with personal privacy on a significant scale (Morton, 98). Commercial remotely sensed imagery had until the 1990s been chiefly supplied by Landsat and SPOT, the latter of which has a resolution of 10m<sup>2</sup>. While such resolutions were useful for many purposes they had few implications for privacy,

aside from the privacy of certain activities such as agriculture which occupied an extensive territory. The monitoring of drug cultivation is one such example (Madsen, 1994), and the use of SPOT imagery by the European Union to police its 'set aside' scheme of paying farmers to leave land fallow is another (Pattie, 1993). A privacy related concern which has also been raised is the use of such technology to invade the privacy of minority groups around the world and thereby exploit or repress them (Madsen, 1994)<sup>7</sup>.

Such limited examples aside, however, a ten metre resolution meant that most individual acts could not be effectively monitored and thus that individual privacy was not under threat from commercial remote sensing. Aerial photography by contrast can detect more significant detail than commercial satellite imagery. In such cases, however, the cost of getting such imagery, means that overflights tend to be one-off. In the US such overflights were held in court not to impinge on privacy whether undertaken by police or private organisations (Curry, 1994) and whether they involved the use of orthophotography or other observational equipment. A similar situation would appear to be the case in Ireland in relation to aerial photography for other purposes than surveillance, while actual aerial surveillance by the Gardai is a recent development. The threat of aerial photography to privacy would seem to have always been somewhat limited, however since to really have a significant impact such photography would have to be ongoing, and since the conspicuosness of any overflight gives the individual warning. It is conceivable that the courts would hold that continuous overflight for the purposes of photography constituted a nuisance.

Recent events have changed this situation, however. Whereas in the past to obtain detailed imagery it was necessary to have access to highly classified imagery from spy satellites, or to fly over in a plane and thus be observed, this is no longer the case. In 1998 and 1999 commercial imaging satellite systems with 3 metre and then 1 metre resolution were due to go into orbit (Morton, 1998; Millar, 1998). Such imagery is now supplied over the Internet, as is imagery from Russian spy satellites. Licences for satellites with resolutions as low as 85 cm have been granted by the US, though it is "unlikely that licences will be granted for resolutions much higher, not so much for national security concerns but because higher

<sup>&</sup>lt;sup>7</sup> Madsen (1994) points to the use of remotely sensed imagery in a variety of ways which are detrimental to such groups including the identification of natural resources followed by the repression of the groups whose land contains them, and even direct military use of RS imagery supplied by the US or France against persecuted minorities in Pakistan, Burma (Myanmar), and Sudan.

resolutions start to invade personal privacy" (Morton, 1998). Despite this limit on the resolution of such imaging it can be seen that 85cm resolution clearly has almost as many impacts on personal privacy as a conventional overflight using a camera, though the images will not allow individual identification.

In regard to non-image GI the situation is similarly complex. Some systems which have clear privacy implications, although not because of the creation of imagery, are those which use satellites in one way or another to track or monitor phenomena. Examples of this are the EU 'spy in the sky' which is being created to monitor ships at sea for a number of reasons including safety, the monitoring of fish catches and of the reporting by such vessels. Such a system will have obvious safety benefits as well as helping to monitor the exploitation of declining fish stocks, though some fishermen may feel it to be intrusive and to compromise the privacy of their job activity (Siggins, 1994). The development of cheaper satellites makes possible the use of such monitoring technology to items such as "far-flung railroad switches, power lines, even the cows, water tanks, and fences on remote ranches" as envisaged in Australia (Millar, 1998). If this is possible then so too is the monitoring of individuals by satellite if they too can be made to wear or carry a transmitter. Less sinisterly such monitoring of cars and other vehicles will form an integral part of future "Intelligent Transportation Systems" which would use such monitoring in combination with sophisticated GIS to improve traffic efficiency and safety, though with some potentially negative impacts on privacy (Alpert and Haynes, 1994). For example, in-vehicle systems linked by satellite to a transport company's base can allow the real-time monitoring of a fleet of vehicles. The data involved includes routes, speeds and engine conditions and thus not only permits the company to plan routes and detect potential mechanical problems in advance, but also to monitor the activities of drivers (Punch, 1996).

At the other extreme of the GI spectrum from satellite based surveillance of one type or another are the databases that contain personal information with a geographic component. Even the simplest such databases can have a privacy impact. Barr (1996) points out that the simple provision of two publicly available registers in digital format, the electoral register and the telephone directory, has serious potential effects. "Once our names are added to the addresses or the maps that show our houses, the once neutral geographic information becomes personal information" (Barr, 1996: 30). Both of these registers perform this function in themselves as well as permitting other datasets based only on addresses or property maps to be given personal names to go with the other data held (Barr, 1996). While these registers are public and few people object to being on them they were not originally intended for the potential uses to which they can now be put. Such uses can involve simple checking of details of the length of time spent at a particular address for credit checking or more substantial analyses which involve linking other personal data to such comprehensive and detailed (but otherwise neutral) geographic objects (addresses). At the least complex end of this spectrum the availability of such datasets in the UK means that the sinister threat 'they know where you live' is "truer than ever for anyone with the money to pay for the data" (Barr, 1996: 31).

Beyond the level of mere lists of names and addresses come databases which contain the added data on other personal characteristics. Such databases, whether held by private or public organisations, have raised privacy concerns. Much of the concern about privacy has been raised by the activities of the marketing sector (Curry, 1998). "The ability to integrate data by tying that data to its geographic location is one of the marketing industries most promising and powerful tools in compiling data from widely disparate sources on households and individuals - something that was a practical impossibility a few short years ago" (Onsrud *et al.*, 1994). A prime example is that of Lotus MarketPlace which is a much-quoted example of the ethical and privacy implications of databases (Gurak, 1998).

MarketPlace was a product which was due to reach the market in 1991 on CD-ROM for use on personal computer (Curry, 1998). Intended as a marketing tool for small businesses, it contained "detailed information on the personal and shopping habits of approximately 80 million households (120 million Americans)" with a sophisticated search capability (Onsrud *et al.*, 1994). The public outcry about the implications of this product for personal privacy and its potential misuse for criminal purposes led the company to withdraw the product prior to launch (Onsrud *et al.*, 1994; Gurak, 1998; Spinello, 1997). This situation is not particularly unusual in the US, however, where there is no restriction on the building of databases through cross-matching data from disparate sources such as local government, a multiplicity of private sector datasets, census information, driver's licence and any other available data (*ibid.*). Despite the withdrawal of Lotus' product "such commercial files, with varying degrees of detail, are available on over 140 million Americans in approximately 100 million households" (*ibid.*). The data held in the case of National Decision Systems, a marketing company's database includes "address, phone number, age, gender, ethnicity, religion, children's ages, smoking habits, veteran status, marital status, household income, dwelling type, buying habits, and lifestyle" (*ibid.* 7). While the data provided does not usually include personal names these can be linked to the data from the phone book, as has been previously described (*ibid.*). As smaller organisations begin to build their own marketing databases on the basis of such large scale ones the pressures on privacy will increase. One potential use of such information would be the scanning of car licence plates of customers and linking it with their databases. Such highly invasive practices would enable organisations to offer a highly personalised service but at a huge cost to privacy (*ibid.*). While such practices are much more restricted in Europe due to the various data protection laws and the principles of consent and knowledge in provision of information by the data subject, similar (more restricted) databases are being built up in such jurisdictions also.

Public sector data is similarly extensive and has similar implications for personal privacy. As will be seen in Chapter Four, the collection of information on individuals is an integral part of the development of the modern state. States which are highly complex in terms of administration need detailed information on their citizens. In order to fund and administer such a state there must be an efficient civil service capable of both collecting taxes and of redistributing wealth according to need. Such a system is by its nature only feasible if highly detailed information on individuals collected (Giddens, 1985).

While such official information is traditionally confidentially dealt with in many European countries (including Ireland), and to a lesser extent in the US where it falls under the Privacy Act (1974), it nonetheless raises privacy concerns. In an extreme case such concerns, and an associated distrust in the ability of government to keep data confidential, led to the cancellation of the censuses of the Netherlands and Germany (Onsrud, 1994). This example notwithstanding the collection of more and more information has become the norm in government. Such information is typically collected for a variety of purposes by a variety of agencies of local and central government. The types of information include land ownership, salary, criminal record, family details, name, address, phone number, and in the case of the census a variety of highly personal information including lifestyle information, educational qualifications, and ethnicity. Quite early in the development of large government databases their extent and detail prompted fears that 'database trawling' would be used to cross-match

individual's records from different agencies with a view to finding potential irregularities. Such concerns prompted the US Privacy Act of 1974 which specifically deals with such government actions while in Europe data protection legislation prevents the use of data other than for the purposes for which it was collected (Curry, 1998; Strum, 1998).

When examining the whole issue of privacy in relation to modern digital GI, perhaps most significant is the nature of the relationship between the data subject and the organisation collecting, holding and using the information. While in past societies and in contemporary non-western societies such a high premium is not placed on privacy, leading some to argue that the information society is a return to the life of small communities where there was little or no privacy. The difference, however, is one of scale. In such societies any individual under scrutiny also had the option of scrutinising. The modern equivalent involves the information being dealt with "in an impersonal manner from distant locations" leading to a feeling of powerlessness and often to an ignorance of just what is held and by whom (Onsrud et al., 1994). This dichotomy between the power and influence of the individual and the organisation is key to the question of privacy since it is not necessarily the case that the individual wishes to hide all information. Rather the question is one of control of information and its use, and whether or not benefits accrue to the individual from the diminishing of privacy. In addition the often-significant potential benefits which accrue to the collector of the information and sometimes to the data subject, lead to a conflict between the privacy right and other rights, even to other rights of the individual (Strum, 1998). It is in this context where conflicting rights and the differing strengths of the respective participants come into play that data protection is vital.

# 2.6 Conclusions

GI can be seen to have a long history of use as an instrument of manipulation of people's lives. In the past such manipulation has largely been conducted at scales greater than the purely personal. Modern developments have changed all this, however. First the development of GIS and now its amalgamation into the wider telecommunications infrastructure has vastly increased the potential for the manipulation of GI, and for the integration of multiple datasets from many different sources for this purpose. The end result of these changes is that GI has become even more important than in the pre-digital era. The initial development of GIS led to the power to store massive amounts of information and combine and interrogate them in ways that were previously impractical. More recent developments are expanding this ability to those who until recently either could not afford the technology, or who were more interested in using more conventional database analysis, and treating locational information such as address information as yet another attribute. The result is a "democratisation…in which all individuals are potentially empowered with the available electronic tools to think geographically and to make visualisations of their thinking" (Morrison, 1997: 17).

However, these developments may also have a less welcome outcome. It has become clear that the power of modern analysis of GI, combined with the almost ceaseless collection and registration of personal information could pose a threat to privacy. Whereas in the past analysis of GI tended to concentrate on geographical areas (though sometimes GI was collected on a more small-scale basis), the potential is now in existence to conduct this analysis on the basis of individual addresses. This, combined with the power to amalgamate information, and the collection of data from individuals, removes the effective protection of privacy that formerly existed due to the difficulty of conducting analysis on such a small scale. In effect personal data can be combined with data that are not necessarily personal but because they are derived for individual effectively become so. In this context a number of issues arise:

- What is the importance of privacy;
- What trade-offs should be made between protection of privacy and the benefits of improved analysis of GI;
- What are the legal and ethical consequences of these changes;
- How does the control of personal information serve power interests?

Chapter Three Ethical Issues and Privacy

thical thinking has many different traditional strands that often do not accord with one nother. The two main modern divisions are between teleontological<sup>1</sup> and deontological<sup>2</sup> trands (Finnis: 1983; Singer, 1986). Simply put, the former school of thought is

# 3.1 Introduction

As has already been argued in Chapter Two, Geographical Information is an instrument of, source of, and method of articulation of power. The impact of the digital revolution on GI has been to make it easier to amass large amounts of GI and to combine such information in new ways. Such manipulation can create derivative information which is significantly more useful than the original information on which it was based. The result of the various improvements in GI technology has been a dramatic increase in the power of analysis and manipulation of GI. This has been coupled with a massive increase in the amount of GI being stored and an ability to perform operations of such information at scales ranging from the individual to the entire population. In consequence the potential of GI to be used as an instrument of power is also increased.

The wider debate on the ethical implications of the Information Revolution is thus equally applicable to the use of GI. One of the chief areas of ethical and legal concern, in relation to both GI and the wider use of IT has been that of privacy. In some regards the specific potential of GI and of technologies which manipulate GI means that the question of privacy is even more important in regard to GI than to more general information.

# 3.2 Ethical Dimensions of IT and the Issue of Privacy

# 3.2.1 Fundamentals of Modern Ethics

Concern with ethics dates at least to Classical times when, and according to Williams (1993: 1), "Plato thought that philosophy could answer the question", the question being 'how one should live'. At its most basic level this is the question addressed by *ethics*, and according to Singer (1986), and Finnis (1983) ethics is thus a very practical issue. The

'question' itself can be applied to society as a whole, or to "a set of standards by which a particular group or community decides to regulate its behaviour - to distinguish what is legitimate or acceptable in pursuit of its aims from what is not" (Speake, 1979: 112). It is therefore appropriate to speak of the ethics of information use, or of GI use.

Ethical thinking has many different traditional strands that often do not accord with one another. The two main modern divisions are between teleontological<sup>1</sup> and deontological<sup>2</sup> strands (Finnis, 1983; Singer, 1986). Simply put, the former school of thought is concerned with the ends or motives of an action, and the latter with the means of action.

According to Mason (1995) teleological theories can be divided into agent-oriented theories, and results-oriented theories. The former focus on "an agent's moral responsibility, intentions, state of knowledge, virtues, and self-interest"; the latter focus on 'public interest', evaluating an action in terms of its effects on all the stakeholders in a situation (Mason, 1995:112). The pre-eminent teleological theory is the results-oriented Utilitarianism of John Stuart Mill and Jeremy Bentham<sup>3</sup> (Singer, 1986). Utilitarianism can be simply summarised as "the ends justify the means". The 'ends' or 'Utility' is the creation of happiness, or minimisation of suffering for a maximum number of people. Any potential actions can then be analysed with regard to their costs and benefits to determine which best serves this 'Utility'. Two significant problems with Utilitarianism are that it lacks any concept of human rights, and the difficulty in determining the 'Utility' (Spinello, 1997).

Deontological theories by contrast focus on the act itself rather than potential outcomes and also fall into two main categories: Pluralism and Contractarianism. Pluralism is associated with Kant and is a rule-based philosophy focusing on adherence to 'duty' in all circumstances and regardless of outcome (Singer, 1986). For Kant's purposes duty is defined by the 'categorical imperative of universality': an act may be considered moral if as a maxim of behaviour it can be transformed into a universal rule of morality. However, the absolute nature of Kant's laws prevents effective action in the event that two moral rules clash. Modifications of the theory deal with this by creating hierarchies of rules, none of which is absolute (Spinello, 1997).

From the Greek telos meaning goal or purpose.

<sup>&</sup>lt;sup>2</sup> From the Greek *deon* meaning duty or to bind.

<sup>&</sup>lt;sup>3</sup> Bentham is again mentioned in Chapter Four in the context of his design of the panoptic prison used as an image of the operation of power through observation by Foucault.

#### ire informed by ethical debate and even in the absence of actual codes the accute itself

Contractarianism, focusing on rights rather than duties, is rooted in the Enlightenment philosophy and is the basis of modern human rights law (Spinello, 1997). Its focus is a theoretical 'Social Contract', an unwritten agreement between all parties in society including the civil government<sup>4</sup>. Under this contract people agree to respect one another's rights and government agrees to respect the fundamental rights of each person<sup>5</sup>. In other words "all men be restrained from invading another's rights, and from doing hurt to one another" (Locke, 1998). In this philosophy respect for the rights of others is the basis of morality and violation of peoples' rights is an immoral act. International agreements such as the Universal Declaration of Human Rights have brought this particular ethical system international legal importance. There are, nonetheless problems with Contractarianism including:

- The difficulty of precisely defining rights
- The difficulty of determining whether certain rights are absolute
- The difficulty of determining the limits to non-absolute rights
- The difficulty of resolving conflicts by balancing contrary rights, or conflicting rights and duties.

Most significantly this theory rejects the idea of the general welfare being more important than that of the individual which is at the heart of Utilitarianism (Spinello, 1997).

Though the place and relevance of ethics within philosophy are disputed, the importance of the debate between these different ethical theories in the modern world can be regarded as threefold:

- There is a clear linkage between legal theory and perceived morality and thus ideas that are ethical come to be enacted into law. This linkage is clearest in the case of contractarianism, though utilitarianism has had a significant impact also: the idea of the 'public good' that can override individual rights is clearly a utilitarian concept. Ethical theory can thus come to have a profound impact on people since it is often the basis of the laws that govern them.
- The creation of ethical codes, or codes of conduct in the middle ground between the individual and the law is undertaken by many representative organisations and play an important role in the self-regulation of many professions and industries. Such codes

<sup>&</sup>lt;sup>4</sup> An idea developed by Hobbes as necessary to prevent the war "of every man, against every man" that is man's natural state (Hobbes, 1998: 72)

<sup>&</sup>lt;sup>3</sup> According to some philosophers of this tradition rights are not dependent on the contract but are natural to a person (Spinello, 1997).

are informed by ethical debate and even in the absence of actual codes the debate itself creates an awareness of areas of conflict and potentially harmful practice.

Since ethics is most concerned with the fair resolution of conflicts it has a particular value in areas of rapid change. When new technologies arise they can potentially change the balance of power between actors in a situation, as well as introducing new techniques and behaviour that can give rise to conflicts (Mason, 1995). Ethical debate in new technologies is thus vital, as it suggests methods of dealing with such conflict in new situations.

This last point is highly important in an era of rapid technological development. The rapid development of IT in particular has outpaced legal reform so that the law is often unable to cope with the consequences of new developments. In such an era of rapid change "choices are often more complex and difficult when laws do not exist or when their applications to new situations are unclear" (Laudon *et al.*, 1996: 513). In the absence of clear new legislation the only legal recourse is through litigation or criminal proceedings on the basis of laws that may not be adequate for new situations. This dependence on the taking of cases (with its attendant costs) to court could lead to long delays in any such legal clarification (LRC, 1998). In this context ethical debate can clarify issues and result in the formulation of acceptable codes of behaviour (often formally adopted by professional bodies) that protect people in the absence of legal sanction.

# 3.2.2 Ethical Tensions in the Information Age

"In today's information society, the almost universal prevalence of information and the immense power it represents has become a source of new moral and ethical demands" (Mason, 1995: 23)

As highlighted by Mason (1995) the power of information in modern society and the changes to behaviours allowed by IT have become a concern of ethics. Lauder *et al.* describe how IT "alters relationships among people, moving interactions away from the personal ..... when the impact of an action is on someone or some thing that feels distant or abstract, people tend to have less concern about the effects of their action ...... at the same time, increasing power, storage capacities, and networking capabilities of information technology can greatly expand the reach of actions and magnify their impact" (Lauder *et al.*, 1996: 513).

The increased distance of the actors from the people their actions affect is one of the key issues in the ethics of IT. Whereas a particular practice in the past might have raised questions in the mind of the actor because of the obvious impacts on the subject, the impacts of actions on somebody known only as data do not raise these concerns. It may also be possible to automate certain elements of decision-making on the basis of the data in the file, and thus actions may be undertaken without any judgement being made on the basis of the operation of an algorithm.

In the literature that attempts to detail the ethical conflicts of information management a number of different classifications of the issues which arise exist. There is broad agreement among them, however as to the most important issues. Mason (1995), for example, lists six key tensions that must be addressed in drawing up 'a new social contract' for the information age. These illustrated in Table 3.1.

Table 3.1: Mason's Six Ethical Issues in the Digital Age

1. Intellectual Property Rights	The issue of ownership of and profit from information.
2. Privacy (of personal information)	The degree of control of the individual over personal information.
3. Accuracy of information	The importance of information in the Digital Age makes its accuracy and timeliness vital. This has become the one of the most important legal issues in regard to IT.
4. Information Justice	This concerns how the benefits of information should be shared among the members of society and includes issues such as cost recovery.
5. Gatekeeping	The conflict between those who believe that all information should be free and those who believe in controlling its flow whether for profit or due to other reasons (privacy, censorship, etc.)
6. Technological Implementation	This issue covers the question of whether technology should be embraced at all costs, or whether quality of life issues should be dominant.

Source: Mason (1995)

This is merely one method of many categorising the ethical dilemmas raised by IT. Though many others exist, however, they largely agree about the issues involved. Thus Spinello (1997) divides the ethical domain of IT into two areas: computer ethics and the closely related area of the ethics of information management. These two categories include a variety of issues (illustrated in Fig. 3.1).



Figure 3.1: Spinello's Categorisation of Ethical Dimensions of IT

The information management category is the more relevant to the subject matter of this study and concerns: data acquisition, access, and information stewardship. These constitute the stages of information management and Spinello is concerned with the ethical issues arising at each stage. In the data acquisition stage, for example, some key ethical issues are privacy and the confidentiality (of business information). In the access stage the main issues are internal and external access, ownership and the right to sell data, and the conflict between privacy and other interests (such as business interests in credit risk assessment, for example). In the stewardship category fall timeliness, accuracy and security, and the issue of recombination of data with other data (which can also have privacy implications). This process-based method of categorisation is useful for information managers in clarifying the issues arising during information manipulation but does not clearly categorise the individual issues in the way that Mason (1995) does.

hat of balancing the right to privacy with the rights of others to benefit from the use of a formation

Finally Laudon et al.'s classification identifies five ethical aspects of IT:

- privacy and freedom
- property rights to information and intellectual property
- system quality
- IT effects on quality of life
- threats to information systems

It is clear that the issues involved are broadly the same although the method of classifying them is somewhat different. For the purposes of this study it is felt that Mason's classification is the most concise and useful, providing clear categories of concern and adequately reflecting the many interrelationships between them.

# 3.2.3 Privacy as an Issue in the Information Society

The importance of the issue of privacy as an ethical concern is clear from its identification as such in all of these classifications. It is also clear both from Mason's classification and Spinello's process-based model that any individual concern such as privacy does not exist in isolation from the others. Taking Mason's categories it is clear that all the other categories have important privacy implications:

- Intellectual Property: The ownership of information by somebody other than the data subject may lead to privacy conflicts when profit is sought from the information.
- Accuracy of Information: The accuracy of private information is vital to the interests of the subject since it may be used to make decisions impacting on him/her.
- Information Justice: Information justice seeks to balance the rights of individuals and of organisations one example is the balance between the right to privacy and the right to profit of the owners of information.
- Gatekeeping: The issue of gatekeeping relates among other things to issues such as security of information held on a system, hacking, confidentiality and the responsibility to protect private information from excessive interference.
- Technological Implementation: This is a most fundamental question which lies behind all of the others, namely how to balance the obvious benefits of technology against issues of quality of life. In regard to privacy the most obvious implementation issue is

that of balancing the right to privacy with the rights of others to benefit from the use of information.

Ethics thus provides a useful way of examining issues of conflicting interests in areas of rapid change. One of the main benefits is that this can be accomplished long before legal remedies are achieved. Ethical analyses of the digital revolution make it clear that privacy is one of the most significant ethical questions raised by changing information practices and new technologies. Equally importantly, however, it is clear that the privacy issue cannot be dealt with in isolation. Information privacy is clearly related to at least some degree to all of the other ethical issues relating to IT. Such issues as data accuracy, accessibility, security, ownership and the right of the individual to have their information corrected must therefore also be addressed to some degree in resolving privacy issues. The terms of international data protection legislation such as the Data Protection Act (1988) in Ireland reflects these connections (see Chapter Five). Given its obvious importance in the writing on the ethics of IT, and its centrality to this thesis the following section will deal in greater detail with the issue of privacy.

# 3.3 Privacy

Privacy is an issue subject to considerable debate in legal, philosophical and other fields. Despite its clear importance to many people there is considerable disagreement regarding its precise nature, its importance, and the prevalence of the idea of privacy. At one end of the spectrum of opinion are those who believe that privacy is entirely culturally contingent, and actually damaging to the individual by making him/her vulnerable. At the other end are those who feel that privacy is vital to the protection of the integrity of the person, the existence of intimate relationships, and to the development of multiple complex social roles. Equally uncertain is whether privacy is a human constant or whether it is culturally contingent (Schoeman, 1984).

### 3.3.1 Defining Privacy

Privacy is notoriously difficult to define. This difficulty stems from its nature as a complex range of diverse interests, and from its close links with emotions. Privacy is a

concept that includes the desire and right to have seclusion from other people, to avoid being observed, and to avoid having information about oneself known to others. It is also a concept that has intensely strong emotional overtones: the importance of privacy to intimate relationships is an example. A further difficulty in defining the concept derives from the fact that privacy expectations vary according to context. Thus, in the case of information privacy it is important who has access to the information and the purposes for which it is used. Information that is not private between husband and wife may well be private in regard to anybody who gains access to it, for example. These complexities make giving a precise concise working definition of such a range of issues and emotions all but impossible. It is useful, however, to begin with a relatively simple definition of privacy and use this as a basis for the elaboration of the wide variety of concepts it contains.

Privacy can most simply be defined as "being apart from the company or observation of others; seclusion...freedom from undesirable intrusions and especially publicity" (Longman Pocket Dictionary). Even this limited definition reveals the breadth of issues covered by the term: ranging from the state of aloneness to the avoidance of publicity. This is not, however, the limit of the even the dictionary definition of privacy. Privacy includes freedom from observation, one definition of which is "the gathering of information by noting facts or occurrences" (*ibid*.).

Beginning from this definition it can be seen that while privacy applies in the familiar context of private property, freedom from intrusion and being spied on, it also applies to more obscure issues such as the collection of information on individuals. Privacy thus is a 'cluster-right' that exists in a variety of different situations and that can be adversely affected by a variety of actions.

# **Data Privacy**

Just as privacy applies to information collected on an individual without his/her knowledge it can also be argued that it applies to information volunteered by the individual. Such information, although freely surrendered, is generally given on the understanding that it will be used fairly and at least partly to the advantage of the subject. The voluntary surrender does not mean that the information is no longer private and potentially sensitive, and an individual may continue to have a stake in the use of such information although in the purest sense of the word it is no longer absolutely private, having been shared. However, the necessity that the individual surrender such information in order to

participate in society, and for example to possess a bank account and pay tax, means that such surrenders of information are not wholly voluntary but are constrained by the need to live in a complex information driven society. In this situation information must still be regarded as private information held in trust by an outside agency.

Although the information may be held by a large organisation it is in some ways still private and new actions concerning the information may have further privacy implications. Thus, for example, when such information is transferred to a third person observation is now being undertaken by this third party and thus constitutes a separate infringement of privacy, although the same information is being used. Similarly, when such information is combined with other information in a fashion that allows it to be used in new ways there are potentially new privacy implications. In this case the nature of the observation has changed and may have intruded into areas that were previously inaccessible when the sets of information were kept separately. Thus, although private information may be volunteered, changes in the way in which it is used may raise new privacy concerns. There are thus varying expectations (and rights) of privacy even in regard to private information which has technically become less private through being shared, expectations and rights which are protected to some degree by data protection legislation (see Chapter Five).

# The Contingency of Privacy

The changing privacy expectations that may reasonably be expressed by the individual, even in regard to the same information or the same type of activity on the part of another, as circumstances change is one of the main difficulties in defining it precisely. Just as circumstances can change the expectation of privacy, so too the identity of the person making the intrusion: family members may be permitted far more latitude than strangers, for example.

This is one of the most significant problems with defining privacy; namely that it is contingent upon circumstance and upon the person of the person intruding or observing (Inness, 1992). This is true of even one of the most fundamental aspects of privacy – the privacy of the home. In this case the degree of privacy is not merely a function of the place as might be expected but also of the person. It is possible that a hierarchy will exist where certain people can simply walk in, others knock first but enter automatically, while others wait for permission.

The contingent nature of privacy not only makes it difficult to define the term satisfactorily, but also makes it difficult to defend comprehensively. One problem is that difficulty of definition makes the creation of adequate privacy laws extremely difficult (Inness, 1992). A second is that the 'fuzziness' and contingent nature of the right to privacy makes some commentators discount its importance, and even deny its actual existence (Inness, 1992; Thomson, 1975; Thomson, 1990).

# 3.3.2 Arguments against Privacy

There are two main thrusts to the argument that privacy either does not exist or is unimportant. One legally based argument depends on the fact that privacy is such a diverse entity that it falls under the protection of other areas of law and thus has no independent existence. The second argument is based on the value of privacy and contends that privacy is not actually important, and thus is not deserving of existence. This latter argument can be further subdivided on the basis of the reasons suggested for the de-valuation of privacy, one of which is economic and relates specifically to privacy of information, and the other based on the effects privacy has on society.

The former position is exemplified by Prosser (1960), who makes it clear that privacy does not exist as a separate legal right. Instead it has four separate and distinct bases in the law of torts:

- "Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs";
- "Disclosure of embarrassing private facts";
- Publicity placing somebody "in a false light in the public eye";
- Taking of somebody's "name or likeness" for one's own advantage (Prosser, 1960: 107).

Though this argument that privacy is actually a complex of four other legal rights does not deny the importance of privacy its emphasis on its origins in and protection by a number of diverse torts discounts the independent existence of privacy.

In a similar vein Thomson (1975; 1990) advances similar arguments that privacy is a derivative of 'a cluster' of property and personal rights. However, Thomson goes further

than Prosser and argues that privacy does not actually have an independent existence. This is not merely because the right to privacy is contained in these other rights, but because "privacy does not explain our having any of the rights in the right to privacy cluster" (Thomson, 1975: 286). In other words since privacy is not the basis of any of these other privacy-protecting rights it cannot have an independent existence. This in turn explains why nobody has "any very clear idea" what privacy actually is. (Thomson, 1975: 272). Among the implications is that there is no right to informational privacy except in cases where a crime is committed to get at the information since "none of us has a right over any fact to the effect that that fact shall not be known by others" (Thomson, 1975: 282).

from universal and is in

The economic argument put forward by Posner (1978) is that personal privacy is subordinate, for economic reasons, to the privacy rights of organisations. The underlying assumption is that neither privacy nor techniques for its invasion are 'economic goods' in themselves. Rather they are a means to such goods (income, for example), and are thus subject to economic forces. It is therefore argued that individuals should not have a property right to personal information, as it is society's interest that this information be available. The exception is where "such rights are necessary in order to encourage investment in the production of socially useful information" as is the case with trade secrets for example (Posner, 1978: 336). Since economic interaction requires information about other members of society in order to make true assessments of them there exists "a duty not to be a hypocrite". Conversely there is a right "to protect ourselves from disadvantageous transactions by ferreting out concealed facts about other individuals that are material to their implicit or explicit self-representations" (Posner, 1978: 338). The consequences of this economic analysis of privacy are:

- Trade secrets should be kept secret;
- Personal information in general should not be private;
- Eavesdropping and surveillance should be limited "to the discovery of illegal activities" as otherwise communication might be hindered (Posner, 1978: 341).

The second treatment of privacy sceptical about its value acknowledges the 'distinctive value of privacy' but questions the culture that gives privacy this important role. Instead it is argued that this distinctive value accorded to privacy makes people vulnerable by implying that there are "thoughts and actions concerning which we ought to feel ashamed or embarrassed" (Wasserstrom, 1978: 330). It is suggested that getting rid of many of the inhibitions associated with privacy would make people "more secure and at ease in the

world" (Wasserstrom, 1978: 331). Such openness would allow people to be less worried about being watched or observed and strengthen interpersonal relationships by making them more honest. Problems with the argument are potentially that such honesty would make personal interactions too complex, and that intimacy would be damaged as there would be nothing that would only be shared within such a relationship (Wasserstrom, 1978).

Other criticisms and doubts sometimes thrown at the concept of privacy are based on what is seen as its historical and cultural contingency. Privacy, according to this view, is far from universal and is in fact a development of the Western world in modern times. It can therefore be seen largely as an aberration rather than a universal right.

### 3.3.3 Historical and Cultural Dimensions of Privacy

It becomes clear in any investigation of the nature of privacy that privacy norms are not constant either through time or through space. According to Bensman and Lilienfeld (1979) a well-defined sense of privacy only exists in certain historical periods, and can decline again having been achieved. The sort of privacy known to modern Westerners, thus, was largely unknown to many of our ancestors and this is reflected in the origins of the term 'private'. According to Schoeman these lie in the Latin term privatus meaning, which ultimately derives from the verb privare which means to deprive (Schoeman, 1992). This reflects a situation in most traditional societies where there is an intense social network and physical crowding, low consciousness of the self (as distinct from the group identity) and where public roles are not differentiated from private ones (Bensman and Lilienfeld, 1979). According to Schoeman (1992) in the Classical world just such a situation existed where the public role was most important, while in private one managed one's purely material needs. Bensman and Lilienfeld (1979) state, however, that ancient Greece did have a developed concept of privacy though during the Medieval period this was largely lost (Schoeman, 1992; Bensman and Lilienfeld, 1979). Most areas of life were open to scrutiny including marriage and sexual intimacy, personal expression, religious and spiritual belief, personal relationships, one's economic status, and the right to work (Schoeman, 1992):

"What to labour at, when to labour, with whom, whom to marry, whether to have children, whom to have in one's house, whom to associate with - none of these areas provided people with socially shielded options" (Schoeman, 1992: 126).

Essentially the difference between modern society and such a society is in the degree of separation of roles. In such societies most of life is of necessity lived out in public, individualism is not socially acceptable or feasible and there is little opportunity for privacy or seclusion while all aspects of life were lived out in the same company.

Bensman and Lilienfeld, however point out that although this was the case there was some degree of development of privacy in many of these societies, though it was largely confined to those of higher social standing. Such individuals had the material resources to live partitioned lives with an element of privacy since privacy is a product of the possession of leisure time in which to withdraw (Bensman and Lilienfeld, 1979). This situation was the case in the ancient world, and for most of subsequent history (Bensman and Lilienfeld, 1979). This social stratification was also evident in the use of seclusion in such societies: for tabooed members of the lower classes the imposition of privacy was a punishment (*ibid*.). The gradual alteration of this situation resulted from a number of factors including greater mobility, the breakdown in kinship and social ties, more complex social interactions, and improved education (Schoeman, 1992).

Although such a historical view appears to suggest that privacy is exclusively a modern western development it appears from the study of other contemporary non-western cultures that this is not the case. However, the differing nature of the privacy norm in different societies may make it difficult to recognise the existence of such a norm: few societies have the material well-being of modern western society and thus the particular forms taken by privacy may not be possible. Thus:

"our contemporary norms of privacy are 'modern' and 'advanced' values largely absent from primitive from primitive societies of the past and present" (Westin, 1967: 59).

Nonetheless some privacy norms do appear to exist in all societies, though the degree varies radically. According to Westin (1967: 60) the norms regarded as "natural' needs of all men living in society" by westerners would not be to the satisfaction of most societies. Though privacy does exist in such societies it is usually differently expressed, and in many
societies psychological means of creating privacy replace the physical ones (such as solitude) used in the Western world. This is necessarily the case where crowding and communal life make solitude impossible (Westin, 1967).

Thus Murphy (1964) quotes the example of the use of the veil by Tuareg men. The veiling of the face is a means of achieving social distance and constant adjustments of the veil are made reflecting the changing company and the social interactions between them. A highly developed system of psychological privacy and varied social interactions such a system often protects are thus evidenced (Murphy, 1964). Another psychological method of achieving privacy is averting the eyes which a withdrawal of presence when physical withdrawal is not possible (*ibid.*). Hall (1989) notes a similar use of psychological withdrawal in wider Arab culture, necessary to achieve a sense of privacy in large extended family homes. This creation of psychological space is crucial to the sense of privacy in any society, whether or not physical seclusion is actually possible (Strum, 1998).

In other societies where crowding is a pressure people move past each other without touching "where Europeans, who have more privacy, are continually doing so" (Murphy, 1964: 64). A similar strategy for the maintenance of some privacy occurs in "simpler" societies through the use of language: "languages of primitive peoples are more elaborate, more ceremonious, and more courteous than that of twentieth century Americans" (Posner, 1978: 339). Posner surmises that such careful structuring of language is due to the lack of physical privacy in such societies: language thus has to be much more carefully structured to take account of third parties and the effect of ones words on them. In effect communication is stilted due to the need to use language as a privacy shield. Westin (1967) points out that the Javanese who live in open houses with no physical privacy use etiquette, emotional restraint and a 'general lack of candour' to create privacy. By contrast the culturally similar Balinese have highly private dwellings and their home life reflects this by being open and warm (Westin, 1967). Westin (1967) also points out that even cultures such as those of Samoans, the Tlingit of Alaska, and Formosans, that appear to possess no sense of privacy in fact do possess privacy mores.

#### 3.3.4 Privacy as a Universal Value

It seems certain thus that, notwithstanding the claim that privacy was unknown historically, privacy of some kind is universal. Though historical societies may appear to have little privacy by contrast with current western norms the examples of other societies quoted above show that even in the absence of any western style of privacy efforts are made to protect privacy. In some societies such as the Tlingit the privacy norms are minimal while in others significant efforts are made to create privacy, using psychological methods to create a private space when an actual space does not exist

One way of explaining this is to look at privacy as existing in two forms as suggested by Schoeman (1992):

- Simple privacy: allowing some privacy but within the social norms of one's society;
- Individualistic privacy: allowing behavioural privacy and individual expression.

The former is a state of privacy where seclusion is possible in some form though one's behaviour in private is not at one's own discretion. Rather one's behaviour is determined by norms that constitute "a rigid and internalised form of social control" (Schoeman, 1992: 15). According to Schoeman much of "socialisation is directed to erecting internal barriers to norm violations" (Schoeman, 1992: 15). Typically found in less complex societies such privacy allows the performance of those acts deemed unacceptable for public exposure (including defecation and sexual intercourse in many cases). Clearly in such a situation privacy is quite limited in its effects and is not at all analogous to the right valued in modern society. This constitutes the second type of norm. It permits the individual a wide choice of behaviour, and promotes self-expression, "private life, individuality, the integrity of various spheres of life, and various associations with people" (Schoeman, 1992: 15).

Thus privacy is something that can be assumed to be a universal of human society. It exists in a variety of forms though a broad distinction can be drawn between societies with a minimal type of privacy that does not permit behavioural latitude and those where privacy is used to maintain independence through the establishment of social distance. Such social distance and the development of different options of behaviour for different situations are a vital element of what makes privacy important in the modern world.

#### 3.3.5 The Importance of Privacy

"Privacy, therefore, has a great deal to do with power. Society's power is limited and that of the individual is increased." (Strum, 1998: 6-7)

Although the universality of privacy can be seen as a gauge of its importance not all privacy is the same as has been seen. While simple privacy may be of importance to the societies in which it is the only form of privacy it is not the concern of this study. In this context it is only individualistic privacy that counts: this is the form of privacy which is generally regarded as important in the modern world. A variety of justifications have been used for regarding privacy as important. Most of these justifications concentrate either on its importance to interpersonal relationships, and particularly intimate relationships, or on its importance for human dignity (Inness, 1992; Boling, 1996). Another justification related to that of human dignity is that privacy is vital to the function of a free, democratic society because of the space it gives the individual for self-expression and growth (LRC, 1998; Strum, 1998)

The most famous article in the debate on privacy is that of Warren and Brandies (1890). Writing in relation to privacy in regard to the press they concentrated on the moral right to individual human dignity, and an inviolate personality as the basis of the right to privacy. This is an important argument in the privacy debate: that in a complex world it is necessary that a person be able to withdraw from public existence and that a violation of this privacy violates dignity (Warren and Brandeis, 1890; Strum, 1998). Responding to Prosser's (1960) dismissal of the argument concerning inviolate personality (by reducing privacy to the question of reputation and the infliction of mental distress), Bloustein (1964) argues that this misses the central connection in the various privacy-related torts named by Prosser. This is that privacy is "an aspect of the pursuit of happiness" (Bloustein, 1964: 187) and thus that there is an essential spiritual character to such cases. What is at issue is "not a form of trauma, mental illness or distress, but rather individuality or freedom" (Bloustein, 1964: 187). Privacy in this analysis is distinctive, fundamental, and is an aspect of human dignity, the denial of which diminishes a person (Bloustein, 1964).

Similar arguments based on human dignity and the respect for persons are made by other authors. According to Benn (1971) people are rational agents who need to be able to make choices that are respected: one such choice is that of retreat from society into privacy. To

put this another way "without a sense of the individual as an intrinsically valuable being, there can be no societal perception of a need for privacy" (Strum, 1998: 5). Even covert surveillance alters the individual's ability to make such choices. In effect it means that the world is different than the individual's assumption, and that therefore the choice is made under false pretences. Overt surveillance has a direct impact on the choices of the individual by causing self-consciousness altering behaviour (Benn, 1971). By observing the individual overtly, Benn argues, he/she is forced to participate in the observation and thus objectify him/herself<sup>6</sup>. The objectivity thus caused (and also by attempts at control of private behaviour by outsiders) destroys private life which is the 'true' person. In this view of privacy it is a means of creating one's individuality by differentiating the self from others, of developing self-knowledge and reconciling oneself with one's conscience (Gerstein 1970, Gerstein 1978). Privacy is thus a key to freedom and to self-development (Strum, 1998; LRC, 1998). This aspect of privacy is also stressed by the argument that people have a 'moral title' to their lives which society accepts, and "privacy is the social ritual by which that title is conferred" (Reiman, 1976: 314). This means that people should be free to determine how much of them is revealed to the world because privacy "protects the individual's interest in becoming, being and remaining a person" (Reiman, 1976: 314). Privacy is thus a question of the integrity of the person and permits them to be themselves (Fried, 1968; Strum, 1998).

According to these arguments another key aspect of privacy is its importance to the formation of intimate relationships (Inness, 1992) because such relationships necessitate the relinquishment of information to one another: for this information to be meaningful in creating an intimate bond it must be private (Fried, 1968). Equally important to the development of intimacy is the freedom from objectifying outside scrutiny of the relationship itself (Gerstein, 1978). Another argument concerning the importance of privacy is in regard to its role not only in intimate but also in all relationships in a complex society. In such a society people need to maintain different social roles in their relationships with different people. The type of interaction in different relationships and the amount of information revealed in each vary. Privacy is necessary to maintain these differences (Rachels, 1975).

<sup>&</sup>lt;sup>6</sup> This idea of objectification of the individual by observation is the key to the power of the panoptic method discussed in Chapter Four.

Finally privacy has been argued to be important in regard to permitting relief from social norms, and thus in allowing self-expression. This is of vital importance in a free society. The ability to get outside social norms allows one to think in non-standard ways, evaluate and suggest alternatives to the norms of society, as well as to act in ways which are frowned upon by the majority of society (Gerstein, 1978; Gavison, 1980; Schoeman, 1992). Such privacy and its attendant behaviour while frowned upon in small insecure communities where traditional behaviour and solidarity are likely to be valuable survival mechanisms, is of value in rapidly changing, highly complex societies (Schoeman, 1992).

Thus it appears that privacy is a very important principle in modern society for a number of reasons. It is highly complex issue involving questions of liberty, intellectual integrity, interpersonal relationships, and the ideals of a free society (Gavison, 1980). As such privacy is of vital importance to the functioning of modern democratic societies (LRC, 1998), and may be highly advantageous in encouraging non-standard opinions that enable quick reaction to changing circumstances.

#### 3.3.6 International Legal Protection of Privacy

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." (Article 12, Universal Declaration of Human Rights, 1948)

The importance of privacy is widely accepted in both philosophical and legal circles, although there are also schools of thought that feel that privacy does not deserve to be considered to have an independent existence. However, the level of legal protection of privacy still varies. Various international instruments such as the UDHR, ICCPR and ECHR provide for the protection of privacy among the other rights identified. They do not, however, attempt to define the precise nature of privacy and in consequence it must be questioned whether they can be effective. Though a state may sign up to these accords it seems likely that the implementation of the provisions relating to complex rights such as privacy will be uneven simply because of disagreement regarding the nature of the right of privacy (See Chapter Five).

In national legal systems there is less agreement concerning the issue. The US has perhaps the best developed body of case law concerning privacy (as is evidenced by the US focus of many of the publications in the debate concerning privacy), and judgements have found considerable basis for protecting privacy in the Bill of Rights. In Europe the situation is less clear. While some jurisdictions such as Germany have enacted comprehensive privacy legislation, others like Ireland lack any clear unified body of law in relation to privacy (LRC, 1996b; LRC, 1998). The issue of privacy in Irish law will be discussed in greater detail in Chapter Five.

#### 3.5 Conclusions

Privacy is a right which tends to be poorly defined legally and philosophically and yet held in some respects to be one of the most important since it determines the ability of the individual to function freely in a democratic society. Recognition of the importance of privacy is uneven although the specific guarantees provided for the right in international treaties. While there are many different aspects to privacy, one is the freedom from unwanted observation. This right at its most extensive includes the freedom from indirect observation through the collection of information on an individual: information privacy.

The development of large-scale databases of personal information has been viewed as potentially erosive of this right. The threats to personal privacy are clearly evident in the capabilities of systems and the use of personal GI both within GIS and normal information systems pose a particular threat. With an adequate geo-referencing system and system of unique addresses to not only link diverse items of personal data on the basis of the address, but to use sophisticated geographical analysis on such data.

In the following chapter the connections between the collection of information and the exercise of power over the individual will be examined, highlighting the importance of the right to privacy in potentially preventing such manipulation.

# Chapter Four

nan misery" (Kling, 1996: 4)

# Theoretical Issues of Information and Power

"Nam et ipsa scientia potestas est." (Knowledge itself is power.) Francis Bacon (quoted in p. 25 of Dainith, 1997)

### 4.1 Introduction

As is clear from Chapter Three the digital revolution has raised many ethical issues of practical importance in adapting to an Information Society, one of which is privacy, itself clearly a very important human right and fundamental to life in complex modern societies. Although the revolution has been under way for a number of decades it is only in the 1990s that it has become a major public issue. According to Johnson (1996) this is in large measure to a number of occurrences of the early 1990s including:

- The Clinton government's high profile policy on information infrastructure
- The emergence into popular culture of the Internet,
- Falling prices of personal computers (which reached 30% the US population by 1993)
- Mergers of corporations dealing in information
- The increasing power of hardware, and availability of software (Johnson, 1996).

Accompanying this increased public interest has grown a literature concerning this revolution and its social consequences.

Such literature and comment falls in the main into two distinct categories:

• Techno-utopians who foresee a bright future arising directly from the adoption of new technology and thus see the information society as a more just and equitable one where information performs and enabling function.

• Those who emphasise potential negative impacts, the so-called 'dystopian' vision, and "examine a darker social vision when any likely form of computerisation will amplify human misery" (Kling, 1996: 41).

What both these bodies of literature tend to have in common is a tendency to view technology in isolation, assuming that technology by itself determines the future of society for good or ill, as well as a tendency to portray extreme visions of the Information Society (Robins, 1996). They do, however, fulfil an important function as they highlight the issues involved in any debate about the value of particular advance in IT. In regard to the issue of privacy the pessimistic viewpoint is that IT will enable the creation of a potential 'Orwellian'<sup>1</sup> nightmare of surveillance and social control through observation and the recording of information (Davies, 1995). Against this the utopian argument is that the power of information will not be confined to particular interest groups but rather that information will be a democratic and equalising force.

The importance of these particular genres of the literature on IT is that they emphasise the power of information either for good or ill. In particular relation to privacy the dystopian vision highlights an important issue with relation to privacy – the power of information over the individual. The literature on privacy emphasises many things including its importance to human dignity and to the maintenance of complex social roles and liberty in society. The issue raised by IT based literature is equally important in regard to privacy in the information age, however.

It is the fact that the information revolution has increased the potential power of information, as well as making its collection easier, which is most significant. In an Information Society information is the "key to wealth and power" and this leads to a "growing demand for information which in turn generates a demand for further and better methods of acquiring such information" (LRC, 1998: 7). There is thus a tendency in such a society for information to be collected for its own sake, as well as being subjected to more powerful techniques of manipulation. Where this information is personal information, and in particular the sort of sensitive information that is regarded as particularly private, the consequences are not only

<sup>&</sup>lt;sup>1</sup> A reference to Orwell's dark social vision in the Dystopian 1984.

serious for human dignity, but also for the exercise of power in relation to the individual. It is this fact that exercises those dystopian writers who predict the development of a surveillance society.

In this context it is proposed to examine a number of theoretical viewpoints applied to the issue of information and power in society, before proceeding to a discussion of the Irish legal protections of privacy in Chapter Five. Such theories can be found in the writings of many modern philosophers and social theorists, including, for example, Foucault, Giddens and Schiller. That the connection between information and power has long been understood is clear, however, from the earlier quote from Francis Bacon. In regard to the question of privacy the key issue in regard to many of these theories is the connections they draw between the absence of privacy through the existence of surveillance or observation, and the exercise of power over the individual and over populations.

#### 4.2 Schiller and Marxian Theory

Karl Marx was a student of Hegel's and later became the most influential of the many thinkers in the 19th century that reacted to the obvious evils of capitalism by some form of socialist analysis. Marxism is a philosophy, which concentrates on the struggle between classes (capitalist and proletarian) to control the means of production. The operation of capitalism is based on the extraction of a surplus from the proletarian class (through exploitation of their labour) which is then accumulated as capital. Marx based his analysis on historic change. Seeing that rule of society had passed from the hands of the aristocracy to that of the bourgeoisie he concluded that the same inevitable process would lead to eventual government by the proletariat. Thus history had a direction and progressed from rule by aristocracy in feudalism to rule by the capitalist class (bourgeoisie) in capitalism to an inevitable rule by the proletariat in a communist form of government. Marx shows his Hegelian influence in his historical determinism (Hondereich, 1995).

Marxian thought was inherently political and had as its aim the realisation this government by the proletariat. This historical project, coupled with action, led to the formation of various communist regimes in the twentieth century, though not to the hoped for international workers revolution. The inevitable association of Marxian analysis with Marxian politics has led to the discrediting of both, in the eyes of many, in recent years. The collapse of the Soviet Bloc and the adoption of some degree of market capitalism by almost all of the remaining communist states of the world<sup>2</sup> inevitably leads to claims of the superiority of capitalism, and of the invalidity in Marxian analysis<sup>3</sup>.

However, this objection rests on the failure of certain forms of government that took their inspiration from a mixture of Marx's thought and that of others, the most notable being Marxist-Leninism. Despite this objection Marxian analysis is a very useful tool for the examination of the development of capitalism, and the operation of the capitalist system<sup>4</sup>. Within this context Marxian perspectives have a great deal to offer in the study of the Information Revolution which is perhaps the chief development of advanced capitalism.

### 4.2.1 Marxian Theory and the Information Society

Marxian theory despite the end of the Cold War and other changes has nonetheless retained a great many thinkers, though they often call their approach Political Economy or Critical Theory. Such approaches can "offer a systematic and coherent analysis of advanced capitalism's reliance on and promotion of information and information technologies" (Webster, 1996: 74)

The approach of such thinkers is based on traditional Marxian concerns. These include the system within which Information Technology has developed, namely capitalism, the structures behind the information, and the historical context of this development (ibid.). Thus central issues for Marxian analyses are still the issues of class, profit and capital, and thus they are concerned with "the role of *power, control and interest*" (Webster, 1996: 76). The central issue is who reaps the benefits of IT.

<sup>&</sup>lt;sup>2</sup> With the notable exception of North Korea

<sup>&</sup>lt;sup>3</sup> The adoption of capitalism has not proved the panacea many suggested. In places such as the Russian Republic capitalism seems to have failed as surely as communism.

<sup>&</sup>lt;sup>4</sup> Societies It has been argued that the collapse of the Soviet Bloc, while undermining "for the time being the historical challenge to capitalism, rescued the political left (and Marxian theory) from the fatal attraction of Marxism-Leninism" (Castells, 1997: 1)

"The spectacularly improved means of producing, organising, and disseminating information has transformed industrial, political, and cultural practices and processes." (Schiller, 1996b: 46)

Information Technology developed within a capitalist society, and has been embraced by it. Emerging Information Technologies have quickly been appropriated for profit purposes by business interests once their value is recognised. The most recent example of this phenomenon is that of the Internet which has existed since 1969, when it was developed by the US military as a method of protecting communications systems by distributing them so widely that they could not be destroyed. With over 100,000 computers and millions of users by the mid, 1990s it was still predominantly a tool of academia (Haywood, 1995). However, in the latter half of the, 1990s it's growth has continued to the extent that many homes now have access. By the "third quarter" of 1997, for example, forty-seven million people in the US used the Internet, twenty-two million of them from home<sup>5</sup>. It has also finally been recognised by the commercial sector that is increasingly using it to advertise, sell products and for a whole source of other purposes. This, combined with the strain being placed on infrastructure by the huge usage (and worries about some of the uses to which it is put) leads to speculation that it will ultimately become a more regulated and managed phenomenon. This management "almost certainly on some form of fee paying basis, has significant implications for millions of users" (Martin, 1995: 124). This increasing privatisation of the Internet is a worry for many of is traditional users who fear that the ability to communicate on the Internet may be confined to those who can pay fees<sup>6</sup>:

"One more time in American history, a new communications technology is being promoted with uncritical acclaim, while it is being turned over to corporate management" (Schiller, 1996b: 87)

It is then questionable how much of the legacy of academic control such as the ethos of free information exchange, or the existence of discussion forums will survive. What has become a true 'cyberspace', the perfect motif for the 'global village', may then lose its special nature (Barry, 1996; Johnson, 1996).

What this clearly demonstrates is that "the capitalist system's long-established fractures are the key architectural elements of the so-called 'information society' " (Webster, 1996: 77). Thus

<sup>5</sup> http://www.cmcnyls.edu/public/Papers/IQSurv.HTM

key factors in the development of the Information Society (if not always in the genesis of the technological innovations themselves) are traditional Marxian concerns such as corporate capitalism, class inequality and the rule of the market. As such Marxian analysis suggests that commonly expressed technological utopianism is extremely naive as the fact that private profit is the prime motivation for the development of the Information Society.

The developments of the Information Revolution can thus be seen to reflect a number of key issues:

1. Corporate capital is in control of most information and most information flow. It acts on a world scale, and mergers have tended to concentrate information and its control in the hands of fewer and fewer corporations. In the arena of software and operating systems Microsoft's early dominance has been maintained by the successive purchase of any company that develops a good idea. A similar trend sees increasing concentration of information generation and distribution in the hands of particular companies as evidenced by the growing trend for movie, music, news production and distribution to be concentrated in the hands of a decreasing number of individual companies. (Haywood, 1995)

2. Market forces ensure that information is only available to those who can pay for it. Thus big business interests have access to huge amounts of sophisticated information and the means of circulating it and analysing it, while the average person has less and less access. The concentration of more and more information in only a few hands means that eventually all quality information may have to be paid for. In a situation where information is only available on propriety grounds "much information, once purchased, is then removed from the public view", a radically different scenario from that envisaged by those who led the initial development of computers (Haywood, 1995: 93). The interest in intellectual property law and other ownership laws (one of the only ethical areas so far seriously reflected in law) reflects this compared to substantially less interest in civil liberties law.

3. Class divisions mean that in a market situation those who have resources are likely to have better access to information and related technologies (Schiller, 1996b). Even the Internet

<sup>&</sup>lt;sup>6</sup> Access to the Internet is not egalitarian at present due to the cost of the equipment needed.

which is often cited as the 'great leveller', the ultimate technological utopian instrument, is only accessible to those with a certain minimum income.

Thus the possession of the technological means to access the Internet for example is very limited. In addition to the necessary computer skills, and the time to use the Internet, person must have:

- Access to a computer;
- A phone line and modem;
- The resources to pay a phone bill;
- The time and skills necessary to use it.

These are the minimum requirements. In addition the growing commercialism of the Internet means that many sites require payment. All of this will be irrelevant to somebody whose family subsist on social welfare, as the cost will be exorbitant. These costs also mean that the preservation or even exacerbation of social divisions is not merely a national concern, but is also a source of inequality on a global scale (Schiller, 1986). The costs of infrastructure will be too much for many economies<sup>7</sup>. Thus "the 'information gap' may be widened, with those economically and educationally privileged able to extend their advantages" (Webster, 1996: 91).

The further disadvantage of inferior education may further exacerbate the condition of the least well off on both national and international scale. On a national scale the same people who cannot afford the technology are the least likely to attain basic literacy and numeracy skills, to leave school without qualifications, and never to achieve computer literacy (Schiller, 1996b; Haywood, 1995). Similarly a state which has difficulties providing technological infrastructure will be unlikely to be able to provide an adequate standard of education.

An interesting corollary of this is the fact that information is not all of equal quality. Thus while the better off have access to quality information, the general public can only be offered information in aggregate form as an aggregate grouping (Schiller, 1996b; Schiller, 1996a).

<sup>&</sup>lt;sup>7</sup> Despite the contention that late development can be advantageous; while Thailand may have benefited through skipping the phase of copper based telecommunications straight to mobile and fibre optics, most African countries are not in this position (Haywood, 1996)

The commodification of information, the need to make a profit and the low spending power of the public in comparison to commercial interests means that public information is not generally a profitable commodity. In order to make a profit on such information it must be sold to a mass audience and thus tends to be undifferentiated and appeal to the 'lowest common denominator', as is the case for example with modern television (Webster, 1996; Schiller, 1996b).

"In this sense the 'information revolution' has given the 'information poor' titillation about the collapse of royal marriages, daily opportunities to 'gawp' at soap operas, graphic discussions of the sexual prowess of sportspeople - but precious little information that may let them in on the state of their society, the construction of other cultures, or the character of and reasons for their own situations" (Webster, 1996: 92).

This last point concerning the availability of information that would enable people to make informed decisions is of considerable importance (Schiller, 1996a; Schiller, 1996b; Schiller, 1986). The control of the information content of those media accessible to the general public has been analysed extensively by Noam Chomsky. His work suggests that such control enables the shaping of docile public opinion, amenable to the desires of the ruling class or interest group. Because of its subtlety this sort of control is much more powerful than the coercion and censorship of totalitarian regimes, while allowing the citizenry the illusion of freedom (Chomsky, 1987).

#### 4.2.2 Surveillance

The explanation for surveillance in Marxian critical theory is closely tied up with the factors already discussed; namely the dominance of capital and class struggle. In this context surveillance is carried out by the state, a capitalist institution to monitor the subordinate classes to ensure the restriction of dissent. The interest served is that of the hegemonic capitalist class, and those targeted are particularly those who are likely to stir up trouble such as socialist activists and other radicals (Webster, 1996).

On the side of information gathering by non-state organisations the rationale is even more obvious and concerns the ability of capitalists to more effectively market goods to the public through the possession of more accurate information about their lifestyles. This in turn is seen as part of a wider attempt by capitalism to extend further and further into everyday life through the fostering of consumer capitalism, a passive, home centred, lifestyle where people are convinced to buy happiness. The Information Revolution encourages this by encouraging people to stay at home in front of the television, by confronting them with a consumerist lifestyle through this medium, and by decreasing the importance of the "self and communal organisation" (Webster, 1996: 95). This is achieved by, for example, inducing dependency on machines for the source of one's pleasure (e.g. television, the home computer), rather than creating one's own. This encourages a stay at home lifestyle which stimulates the accumulation of possessions, while also ensuring that people are less likely to associate in groups (which could be dangerous), and also means that people are exposed far more to the 'messages' beamed into their homes. Finally the ability of Information Technology to monitor the lifestyle of the individual through the use of loyalty cards, home shopping (whether over the Internet or the telephone), and other such schemes enables the focused marketing of goods which conform to known behaviour patterns and appetites. This serves the dual function of encouraging consumerism by stimulating sales while also cutting the capitalists marketing overhead and thus increasing profits.

### 4.2.3 Marxian Theory and IT in summary

Marxian theories of one sort or another prove immensely useful in the analysis of many aspects of the Information Society from the largest scale<sup>8</sup> to the human scale<sup>9</sup>. Ultimately the Information Revolution while not initiated by capital did develop within a capitalist system and has achieved a symbiotic relationship with capital<sup>10</sup>. Information is largely controlled by capital but capital has become dependent on information, and could not possibly operate on the global scale it does without advanced information technologies (Schiller, 1996b).

<sup>&</sup>lt;sup>8</sup> Globalisation; maintenance, stimulation or creation of inequalities between people on a world scale; the creation of what has been termed an international 'Virtual Class' (Kroker, 1996: 171) which is as mobile as capital; the equivalent international underclass; the decreasing importance of the state as a player in world economics.

<sup>&</sup>lt;sup>9</sup> The creation of new elites through the bourgeois dominated education system; the compounding of the problems of areas of deprivation - the problems are now international and so local action may be ineffective; the failure of the information society to help those who are already disadvantaged (Schiller, 1996b).

<sup>&</sup>lt;sup>10</sup> This symbiosis is perhaps best indicated by the fact that in many cases capital and information assume equivalence in the modern world where people get paid by credit transfer, most transactions are electronic, and nothing of any substance in the traditional sense changes hands.

#### 4.3 Globens and the Nation-State

Within Marxian analysis surveillance is one further aspect of the dominance of capital, and the control exercised by capital over both society and over the individual. Surveillance is a simple tool of maintaining order within the state, and for increasing profitability for companies. The international character of the global information market means that information can potentially flow freely (Schiller, 1996b; Schiller, 1986). Thus national laws are unlikely to protect an individual from the unscrupulous. The international nature of many large capitalist institutions makes the task of governments still harder. Invasions of privacy are thus one element of the dominance of capital and the state over the individual:

"Control of information instrumentation, invariably, goes hand in hand with control of the message flow, its content, surveillance capability, and all forms of information intelligence." (Schiller, 1996b: 93).

The danger that is raised as a real possibility by Marxian analysis is that the combined factors of globalisation, the merging of the large corporations that control information flow, and the privatisation of the infrastructure of information may lead to even greater inequalities:

"This foretells a time when most of the ingredients of national consciousness, failing a serious effort to defend the common good, will be completely under the control of a handful of private, giant communications comglomerates" (Schiller, 1996b: 87-88).

In such a situation not only the power of surveillance, but the ownership of all information would potentially rest in the hands of a small elite group of organisations.

Marxian analysis thus stresses the declining role of the state and the increasing irrelevance of the international boundaries that define such states to the movement of information and the operation of capital (Schiller, 1986). However, one problem with this analysis is that it reduces the state to the role of tool of the capitalist system (Schiller, 1986). However, the single organisation that collects most information on individuals is still the state, and much of this information is for its own administrative purposes rather than in the interests of capital. It is therefore worthwhile to examine a theory that seeks to explain the use of surveillance by the state.

73

#### 4.3 Giddens and the Nation-State

Another structural theory which has a much more direct relevance to surveillance and privacy (and which in many respects resembles that of Foucault) is that of Anthony Giddens regarding the origins of the nation-state and the closely related rise of bureaucratic government. Giddens, one of the best known social theorists of modern Britain, is best known for his efforts to reconcile the issues of structure and agency in Structuration Theory. His analysis of the nation-state and surveillance is largely structural, however, and remains firmly in the modernist camp.

In Gidden's analysis two key issues in the development of modern society are the importance of "violence, war and the nation-state" and of "heightened surveillance" (Webster, 1996: 52) in the origins of modern society. In this context "modern societies have been 'information societies' since their beginnings" (Giddens, 1987: 27). Thus the current importance of information is very real, but is part of a much longer-term trend.

Nation-states have only come into existence in recent history (since the 17th century), but they dominate the globe in the way no other political unit has before. This is partly due to their claim to, and in general their achievement of, total authority within their own borders. According to Honderich the modern state is:

"The political organisation of a body of people for the maintenance of order within its territory by coercion, or, more loosely, the body of people so organised or its territory....The State, however, is taken to have the power to regulate the behaviour of all individuals and of any other organisations within its boundaries. For this purpose the State has, or at least claims, a monopoly on the use of force." (Hondereich, 1995: 850)

Such authority was something perhaps claimed by previous state forms but not achieved partly due to their lack of appropriate organisational ability to achieve such control. The second key characteristic of the modern nation-state is that each nation-state extends to the borders of another such state. In short there is no place on earth that is not a part of a nation-state; the political map of the world has no 'blank spots'<sup>11</sup>. Just as it is impossible to find a place that is

<sup>&</sup>lt;sup>11</sup> This is a relatively recent phenomenon - until late in the last century European maps showed many 'empty' areas; the United States still had a frontier. Such areas were outside the system of nation-states.

not part of some state's territory, so it is impossible to live in the modern world without belonging to some state (Giddens, 1987).

As a result when people think in terms of " 'society' we are actually referring to nation-states" (Webster, 1996: 58). As a result a great deal of the identity of any person is based on their nationality<sup>12</sup>. One of the reasons for the continued instability of the patchwork of nation-states is the fact that not everybody's nationality coincides with their state. Another key feature of the nation-state is its organisational complexity that is required to maintain its control within its borders, and to deter aggression from the other states which adjoin it. Modern life is much more highly organised than society has been at any time in the past, and this is intimately linked up with the nation-state, which is described by Giddens as being by its nature an information society (Giddens, 1993a). All states have been information societies according to Giddens but the nation-state, because of it's high degree of administrative unity is extremely so (Giddens, 1987). The needs of this administration presuppose information gathering, as it is impossible to administer an area and population adequately without detailed knowledge of their characteristics. This results in surveillance which has two main bases, the first in the nation-state's violent nature<sup>13</sup>, the second in the state's need to administer its territory and the population of that territory who frequently are given rights and services to ensure their loyalty (Giddens, 1987).

#### 4.3.1 Violence and Surveillance

Despite the various characteristics of the nation-state that give it the appearance of essentiality and permanence, it is in fact both a recent historical innovation, and is also extraordinarily mutable. The state is both a recent invention in human history and also an extraordinarily unstable one. This links back into Giddens' assertion that the nation-state is intimately connected with violence and warfare.

<sup>&</sup>lt;sup>12</sup> Evident in many ways including the willingness of the proletariat to embrace nationalism far more quickly than international class solidarity (Webster, 1996)

<sup>&</sup>lt;sup>13</sup> The 'right' to wage war is held to be situated only in recognised states, anything else is terror. In terms of internal violence the an integral part of the (philosophical) definition of the modern state is that it "is taken to have the power to regulate the behaviour of all individuals and of any other organisations within its boundaries. For this purpose the State has, or at least claims, a monopoly on the use of force" (Hondereich, 1995: 805).

The origins of most nation-states are held by Giddens to lie in war, and the independence and continuity of the nation-state is based on the ability to defend itself. The result is that being prepared to wage war is a key aspect of the nation-state (Webster, 1996). The key importance of national territory to the definition of the state means that the ability to maintain one's borders intact is vital to any state in the modern world<sup>14</sup>.

Another factor which rises from this is that "modern warfare/defence has become much more decisively implicated with the wider society" (Webster, 1996: 61). This has meant the change from small armies raised as a levy from the nobles to standing professional armies. The increasing involvement of non-combatants in modern war is also a factor, illustrated by the increasing levels of civilian casualties in wars this century, particularly once the bombing of civilians became commonplace. The casualty rate of Germany, Poland, Russia and Yugoslavia in World War II was around 10 percent (Webster, 1996). This has the effect of making a war an issue of populations rather than armies, reflecting the fact that wars are carried out on the basis of nations rather than kings<sup>15</sup>.

One consequence is the industrialisation of modern warfare that depends on the ability of industry to provide the necessities of fighting ever more sophisticated wars. This has led to the stimulation of much of the development of Information Technology by military organisations, particularly the US military (Levidow and Robins, 1989)<sup>16</sup>. The key importance of information to the waging of war has been recognised since time immemorial<sup>17</sup>. Adequate knowledge of the enemy's dispositions and plans enables the commander to better organise his own actions. This has led to the development of ever more sophisticated dissembling tactics, and as warfare has become more sophisticated so too have the information gathering and processing tools used both on the battlefield, and in the observation of one's potential enemies.

However, the need to monitor outside forces which may or may not be enemies, is accompanied by the need to monitor one's own population in case of threats from within

<sup>&</sup>lt;sup>14</sup> In this perhaps lies the key to the fact that countries regularly go to war over uncertain borders, even when these are worthless areas, as is the case in the current war between Eritrea and Ethiopia

<sup>&</sup>lt;sup>15</sup> World War II is called the 'Great Patriotic War' in Russia evokes this concept particularly well.

<sup>&</sup>lt;sup>16</sup> This is as has been seen particularly the case in the development of GIS and related technologies such as satellite remote sensing and GPS

(Giddens, 1987). The effects of warfare on information technologies can thus be seen on three levels: the development of more sophisticated weaponry, culminating in smart weapons; the establishment of secure and highly complex communications networks; and the need to *surveille* (of necessity this includes the requirement to watch and to locate and track) those who are a threat to national security, whether within to outside the borders to be defended. Thus the nation-state's violent nature has been a direct factor in the development of surveillance and information technologies through military -sponsored research. Another aspect of the modern nation-state that Giddens relates to its military nature is its organisational complexity. This includes the general extension of rights and services to the population (Giddens, 1987). These in turn breed surveillance.

### 4.3.2 Organisation/Administration and Surveillance

In order for a state to survive it must have internal peace and co-operation with the government. While in the early stages of the consolidation of power this may be achieved by violence, a much more profitable strategy is to achieve voluntary co-operation from the populace. A major part of this is the construction of a national identity through the fostering of national myths and cultures (thus the importance of national education systems). A second major factor is the organisation of society in such a way as to ensure people are content and yet are willing to pay taxes, serve the state and obey the law. Surveillance forms a major part of this process (Giddens, 1987).

At the most basic a state needs to know its population for two primary purposes: to know who can be called upon to fight in a national army, and to ensure efficient administration of taxes (Giddens, 1987):

"Tax policies come to be used both to monitor and to regulate the distribution and the activities of the population, and participate in the burgeoning of surveillance operations of the State" (Giddens, 1987: 157).

<sup>17</sup> C.f. Sun Tzu's The Art of War

One of the worrying factors for Giddens of this is that such organisation and surveillance is an integral part of life, and that there is no obvious way of effectively opposing it (Webster, 1996). In addition the potential for totalitarian rule exists within this organisational superstructure, which is nonetheless essential to the life people lead, and are accustomed to lead (Giddens, 1987).

Giddens attitude to commercial surveillance is that it is both a tool for the maintenance of efficiency of production through the monitoring of the employee by management, and also for the monitoring of customers and the public at large. In the former case the very existence of management as a sector of the corporation is felt to be founded upon surveillance of employees to ensure the best return on investment through maximum efficiency in the use of time. In the latter the objective is again to achieve the best return through the accurate identification of markets, as Marxian analysis observes (Giddens, 1987).

#### 4.3.3 The Nation-State and Surveillance in summary

"There is a fundamental sense....in which all states have been information societies, since the generation of state power presumes reflexively monitored system reproduction, involving the regularised gathering, storage and control of information applied to administrative ends. But in the nation-state, with its peculiarly high degree of administrative unity, this is brought to a much higher pitch than ever before" (Giddens, 1993a: 263).

In Gidden's theoretical work surveillance is a necessary function of the high degree of organisation of modern life, both of the state and of capital. The implication is that modern life is by its complex nature automatically informatised, a surveillance society (Giddens, 1987). This has its good and bad points; while surveillance is prevalent as a method of social control and ultimately of the organisation of populations for war, it also is a method of ensuring the modern standard of living. The efficient delivery of services by both the state and commercial organisations is directly related to their knowledge of the target population (Webster, 1996). Thus the surveillance of corporate bodies, while invading privacy also allows for the provision of a better services to the public; similarly the surveillance of the state allows it to provide many benefits to its citizens, including security, health care, education,

and protection<sup>18</sup>. In addition much of the information collected may be made available to the public and thus be of benefit to them<sup>19</sup>.

Nonetheless it must be acknowledged that this surveillance does not exist in a vacuum. It is intimately connected with the functioning of power in society. The questions of power in terms of 'who exercises it?', 'who benefits from it?' and 'who has access to it?' are the central concerns of Marxian analysis. The question of power in terms of how it actually operates on the individual within the matrix of society leads to the writings of Michel Foucault on the emergence of the 'disciplinary society', and particularly the panoptic methodology of the exercise of power over individuals.

#### 4.4 Foucault, Power-Knowledge, and the Panopticon

"A stupid despot may constrain his slaves with iron chains; but a true politician binds them even more strongly by the chain of their own ideas; it is at the stable point of reason that he secures the end of the chain; this link is all the stronger in that we do not know of what it is made and we believe it to be our own work; despair and time eat away the bonds of iron and steel, but they are powerless against the habitual union of ideas, they can only tighten it still more; and on the soft fibres of the brain is founded the unshakeable base of the soundest Empire" (Servan, quoted by Foucault, 1979: 103)

Michel Foucault's central interests included the study of the history of certain forms of social institution, and the associated knowledge disciplines, for example the prison and criminal justice system and the associated discipline of criminology. In such study his concerns focused on the use of knowledge to exert power and create 'discipline'. The term discipline, for Foucault, thus refers to two separate things: "bodies of knowledge" such as criminology, and disciplinary practices which are "forms of social control and social possibility" (McHoul and Grace, 1995: 26). The disciplines of knowledge are, thus, intimately related to the exertion of power through disciplinary practices. This interest in the use of knowledge as a

<sup>&</sup>lt;sup>18</sup> The Scandinavian countries which have very high levels of surveillance also have some of the best citizen services in Europe.

<sup>&</sup>lt;sup>19</sup> In such cases the safeguard of provision of information in aggregate form also ensures that people will not be identified, while allowing them to have much greater information concerning state of the society in which they live.).

form of social control is very relevant to the information society<sup>20</sup>, as are his ideas regarding the use of knowledge (or information) to create a 'disciplinary society'.

There is, however, a significant difference between the focus of Foucault's work and that of Giddens and Schiller. Rather than focusing on a method of power imposed from the top down upon the population, Foucault is concerned largely with the operation of the mechanisms of power at the lowest level, that of their interaction with the individual. Additionally Foucault stresses that although power is exerted to serve the interests of certain powerful interests in society, it is not imposed from the top down, but is rather exerted through a network of interactions within society.

The two particular works of Foucault that are relevant to privacy itself are the History of Sexuality, and Discipline and Punish; the former is a history of the development of sexuality and 'sexology', and the latter a history of the penal justice system. In the former case the methodology used to 'discipline' is the 'Confession', and in the latter the 'Panopticon'. The Panopticon is of more direct concern to those worried about the idea of surveillance and 'data-veillance', while the confession is only of indirect relevance as it is concerned with the enculturation of the surrender of private information.

#### 4.4.1 The Panopticon

"He who is subjected to a field of visibility, and who knows it, assumes responsibility for the constraints of power; he makes them play spontaneously upon himself; he inscribes in himself the power relation in which he simultaneously plays both roles; he becomes the principle of his own subjection. By this very fact the external power may throw off its physical weight; it tends to the non-corporeal; and the more it approaches this limit, the more constant, profound and permanent are its effects" (Foucault, 1979: 202)

The Panopticon is a prison design developed by the Utilitarian philosopher Jeremy Bentham. Bentham's "grand project was for legislation: the exploration and theoretical foundations of a

<sup>&</sup>lt;sup>20</sup> Knowledge is information that has been contextualised to give it greater meaning as has been discussed in Chapter Two. Knowledge about somebody therefore necessarily involves the collection of information about

perfect system of law and government" (Honderich, 1995: 85). One of Bentham's central ideas (in addition to 'Utility'<sup>21</sup>) is the 'association principal' that ideas are associated. This is similar to Pavlov's reflex except that the "association of ideas was purely mental" (Russell, 1993: 741). This association of ideas principle meant that given the right circumstances it would be possible to "make men virtuous" (Russell, 1993: 741) in other words make them act for the overall good. The Panopticon's design is intended to use the association of ideas to reform the prisoner.

The Panopticon had a relatively simple physical layout. It took the form of a hollow cylindrical cellblock enclosing a courtyard inside which was a central observation tower for the warders. Each cell in the cylinder had windows on its outer and inner face permitting observers in the central tower to view the activities of any inmate against a bright background. The arrangement and design of the cells thus allowed continuous pervasive observation of the prisoners by the centrally positioned warders. The warders themselves could not be seen, however, because the tower's internal structure ensured that light never passed through to reveal its occupants, or their absence (Foucault, 1979; Zuboff, 1988).

The Panopticon formed part of Bentham's perfect social system and operated on the principle of association of ideas since the observation tower was constantly visible and thus occupied the thoughts of the prisoner. Never knowing for sure whether he was being watched, but always suspecting it, the prisoner would thus regulate his own behaviour rather than risk being caught doing something (Foucault, 1979). Over the course of a sentence this became a habit and thus the criminal is not punished but rather reformed through the careful regulation of behaviour. The result was what Bentham "called a 'mill for grinding rogues honest'" through the use of surveillance and the removal of privacy (Honderich, 1995: 85).

#### 4.4.2 The Confessional

"Incitements to speak were orchestrated from all quarters, apparatuses everywhere for listening and recording, procedures for observing, questioning, and formulating" (Foucault, 1977: 32, 33)

him or her.

The confession, the second methodology of exercising power through information is one of the primary instruments of power, according to Foucault (Foucault, 1977). It is also his other major contribution to any debate on the issue of privacy.

school, or the psychiatric institution (Foucault, 1977

The confessional method of exercising power through information began in the thirteenth century with an "order given to all Christians ..... to kneel at least once a year and confess to all their transgressions" (Foucault, 1977: 60). What began as a Catholic Church institution that helped to keep the faithful in check, its results are traced by Foucault to modern phenomena such as the psychiatrist's couch (Foucault, 1977). The method pioneered by the Church thus survived the loss of power that occurred during the Reformation, and was adopted by a variety of other institutions and disciplines, never losing its importance (Foucault, 1977, McHoul and Grace, 1995). Instead "it spread; it has been employed in a whole series of relationships: children and parents, students and educators, patients and psychiatrists, delinquents and experts. The motivations and effects it is expected to produce have varied, as have the forms it has taken: interrogations, consultations, autobiographical narratives, letters" (Foucault, 1977: 63).

Just as the Panopticon manipulates the prisoner to co-operate, however, the Confession has also engaged the co-operation of individuals who are exposed to the power it exerts. A powerful effort to create an 'incitement to discourse' leads to the confessional methodology of self-examination and self-revelation assuming the aura of normality and has ceased to be questioned:

"The obligation to confess is now relayed through so many different points, is so deeply ingrained in us, that we no longer perceive it as the effect of a power that constrains us; on the contrary, it seems to us that truth, lodged in our most secret nature, 'demands' only to surface" (Foucault, 1977: 60)

In the History of Sexuality (vol. 1) this development is traced in regard to the growth of the disciplines of sexuality within which "Western man has been drawn for three centuries to the task of telling everything concerning his sex" (Foucault, 1980a: 23). These disciplines had as their aim the control of population and reproduction so that it functioned in an economically

<sup>&</sup>lt;sup>21</sup> Discussed in relation to ethics in Chapter Three.

more efficient fashion in an industrial society (Foucault, 1977). The confessional model is the basis of much of the practise of these disciplines though it is sometimes used in combination with the panoptic model, particularly in an institutional setting such as that of the secondary school, or the psychiatric institution (Foucault, 1977).

Sex and sexuality, however, were merely one aspect of the use of the confessional methodologies in the disciplinary society. The importance of the confessional in modern society means that everybody experiences "the formidable injunction to tell what one is and what one does, what one recollects and what one has forgotten, what one is thinking and what one thinks he is not thinking" (Foucault, 1977: 60). This culture of confession makes it easy for information to be extracted from individuals in a variety of ways, and makes easier the effective bureaucratic administration of society.

### 4.4.3 The Panoptic Mechanism

"How shall I compare this prison in which I live unto the world" (Shakespeare - Richard II)

Although Bentham's design was expressed as a prison, its design and operation were intended to be applicable to the disciplining of people in any institution at a time when the increasing complexity of society was giving rise to such institutions as the disciplined professional army, the school, the insane asylum, the hospital, the factory and the reformatory among others (Foucault, 1979). Such institutions needed to discipline large numbers of people in order to function efficiently and the panoptic idea was adopted by many to enable this (Foucault, 1979). For Bentham this universal applicability to any institution in which the behaviour of individuals was to be controlled was one of the greatest benefits of the panoptic idea (Foucault, 1979; Foucault, 1980c).

Thus the Panopticon, though presented as a prison design, is "the diagram of a mechanism of power reduced to its ideal form....it is in fact a figure of political technology that may and must be detached from any specific use" (Foucault, 1979: 205). The methods of panopticism are 'polyvalent' in application: "whenever one is dealing with a multiplicity of individuals on whom a task or a particular form of behaviour must be imposed, the panoptic schema may be used" (Foucault, 1979: 205).

#### The crowd, a compact mass, a locus of multiple exchanges, individualities merging trees

Foucault argues that the mechanism of the Panopticon is not even confined to institutional and architectural settings where direct observation is possible. The purpose of the mechanism is to "spread throughout the social body....become a generalised function", and thus to "strengthen the social forces" (Foucault, 1979: 207- 208). According to Foucault the Panopticon and other institutional equivalents are a "discipline-blockade" but the "discipline-mechanism" of panopticism can be removed from its institutional context into wider society (Foucault, 1979: 209). This mechanism is "a subtle coercion for a society to come": the "disciplinary society" (ibid. 209).

One important element in the operation of this discipline mechanism is that although it adopts the panoptic model of operation through the influencing of behaviour by observation such observation does not need to be direct. Observation is also carried out by the collection and recording of information. This system often depends on the individual being willing to surrender this information in the first place, and thus the mechanism of the confession, by which people are willing to part with personal information becomes a potential part of the overall disciplinary mechanism. In effect the confession becomes a mode of observation within the overall panoptic mechanism, making the person both more individual and more visible.

The discipline-mechanism operates on the basis of three principles used to manipulate the person over whom power is exerted:

- It makes the individual visible
- It isolates and individualises the person
- Observation does not have to be constant because it is unverifiable (Foucault, 1979).

The first principle means "visibility is a trap" (Foucault, 1979: 200) as it ensures the potential exposure of one's activity to notice. The second principle is harder to create outside the constraints of the prison where each prisoner can be kept in an individual cell. However, the separation of the individuals from one another "is a guarantee of order" (Foucault, 1979: 200) that has the following effect:

"The crowd, a compact mass, a locus of multiple exchanges, individualities merging together, a collective effect, is abolished and replaced by a collection of separated individualities. From the point of view of the guardian, it is replaced by a multiplicity that can be numbered and supervised " (Foucault, 1979: 201).

Without imprisoning individuals it is virtually impossible to achieve this effect fully outside the confines of an institution, but individualisation can be achieved to some degree through the collection and recording of information on each individual. The creation of individual records thus isolates each person to some degree by creating individual stakes in appropriate behaviour. The solidarity of the crowd can be broken to a degree when each individual feels that his/her actions are noted separately.

Finally Bentham lays down the "principle that power should be visible and unverifiable" (Foucault, 1979: 201). This is perhaps the most important of the three principles in the mechanics of power. The individual knows at all times that s/he is potentially being observed but can never tell whether such observation is in progress (Foucault, 1979). The result is that "surveillance is permanent in its effects, even if it is discontinuous in its action" (Foucault, 1979: 201).

The important characteristics of the resulting mechanism are:

- Efficiency of the exercise of power: this is perfected as the number subject to power is maximised while minimising the number of those exercising it
- Prevention: the constant possibility of observation acts to dissuade unwelcome activity before it even occurs
- Non-intervention: the operation of the system is 'light' as it minimises the need to actually challenge the individual who regulates his own behaviour
- Effect on the mind: without any physical act the system acts on the person, giving "power of mind over mind" (Foucault, 1979: 206)

In essence the fourth characteristic is the most important point as is the key to the other characteristics, ensuring as it does that the individual assumes the responsibility for his own behaviour. The ultimate fact then is that discipline is a "very real technology, that of individuals" (ibid. 225)

#### 4.4.4 The Mechanism outside the Institution

This extension of this mechanism through society involves a number of steps.

• "Functional inversion of the disciplines"

- Invented to neutralise the harmful individual, the function they play in causing positive behaviour can equally be applied to all individuals, for example, through making them more productive.
- "Swarming of the disciplinary mechanisms":
- The disciplines become 'de-institutionalised' and operate flexibly in wider society to monitor and influence the behaviour of people in ordinary life.
- "State-control of the disciplinary mechanisms":
  - As the disciplines 'swarmed' out, they became "co-extensive with the state itself" and were adopted as a tool of the state for "omnipresent surveillance" (ibid. 214). The creation of the police and other bureaucratic surveillance bodies bring "the whole social body into a field of perception" (ibid. 214).

Thus a disciplinary society is created through the expansion of an institutional model to become an "infinitely generalisable mechanism of 'panopticism'" (ibid. 216). The development of this form of power is thus intimately tied up with the emergence of a society "in which the principal elements are....on the one hand, private individuals and, on the other, the state" (ibid. 216). The purpose of this disciplinary society is to assure "the ordering of human multiplicity's" (Foucault, 1979: 218). This enables the exercise of social power at 'low cost', maximises its intensity and spread, and increases "both the docility and the utility of all the elements of the system [the population]" (Foucault, 1979: 218). In effect the individual, just like the prisoner, adopts a docile mien and behaves according to the norms from habit. Thus "the perfection of power should tend to render its actual exercise unnecessary" (Foucault, 1979: 201). In effect the underlying principle of the disciplinary society is "mildness-productivity-power" (Foucault, 1979: 219).

Just as in the Panopticon power operates through observation to reform the prisoner, the disciplinary mechanism is also a productive force. In its wider social function it is used in everyday life to strengthen "the social forces" (ibid. 208) and to "increase the possible utility

of individuals" (Foucault, 1979, 208 & 210). This productivity of power is directly connected with the fact that power is something exercised upon life directly. While power in the past was exercised through the threat of death, modern power acts through life itself, moulding the life of the individual in ways useful to the power network as a whole. This involves the greater productivity of the individual through the control of the use of time (Foucault, 1979; McHoul and Grace, 1995).

However, power does not only operate on the individual: "Power is situated and exercised at the level of life, the species, the race, and the large-scale phenomena of population" (Foucault, 1990: 137). This power operates as a network rather than being imposed from above and in effect everybody is tied together in a giant "laboratory of power" (Foucault, 1979: 204). This is the case because observation is mutual, and because of the self-regulation that involves each individual in enforcing the effects of power over him/herself. Everybody is thus involved in the creation of a system of power:

"In reality, power in its exercise goes much further, passes through much finer channels, and is much more ambiguous, since each individual has at his disposal a certain power, and for that very reason can also act as the vehicle for transmitting a wider power. The reproduction of the relations of production is not the only function served by power. The systems of domination and the circuits of exploitation certainly interact, intersect and support each other, but they do not coincide". (Foucault, 1980d: 72)

Although Foucault states that the individual is the instrument of the power that is exerted over him this does not mean that the individual necessarily co-operates fully with the disciplinary mechanism. Rather the existence of a network of power means that there is always room for opposition, since each individual is the bearer of power. Such opposition is frequently aroused by the interests which inevitably come to dominate due to the asymmetrical operation of the disciplines. In order to maintain power they must be constantly remain aware of such movements of opposition and manoeuvre to maintain their position (Foucault, 1979).

One important consequence of this network idea is that "the analysis, made in terms of power, must not assume that the sovereignty of the state, the form of the law, or the over-all unity of a domination are given at the outset; rather, these are only the terminal forms power takes." (Foucault, 1990: 92)

#### Privacy and the Disciplinary Mechanism

The power of Foucault's analysis is its explanation of the mechanisms by which privacy is invaded routinely and in an institutional fashion for the purposes of controlling the individual, moulding their behaviour in desired ways, and extracting time (and thus labour) from them. In combination with the use of surveillance goes the use of a fostered culture of confession to ensure that much surveillance can be done on a voluntary basis (information is voluntarily surrendered daily in surveys, bank slips and so on). Another very powerful aspect of this whole model is the fact that it does not rely on the imposition of power from above, but rather acknowledges that power operates throughout the social body, though it is engineered so that it meets the interests of the powerful. This lightness of power is a convincing explanation for the willingness of people to submit to it, though as Foucault acknowledges it nonetheless does create resistance.

The current state of society is not quite so disciplined as the panoptic prison itself, though surveillance is almost universal (in conjunction with voluntary information 'confession'). The gaze is not quite universal outside institutions, and in society lateral vision is possible, though the alienation of modern existence has perhaps cut many of the ties between individuals which enable resistance.

#### 4.5 Conclusions

The Information Society, the rise in the importance of Information Technology, and the recognition by economists of the existence of an Information Economy in which information and knowledge-based work is becoming predominant, has given rise to much theoretical speculation. The most blatantly technological of these are rather seriously flawed. They have a tendency to be technologically deterministic and ignore the realities of the societies into which they are imposed. Nonetheless the common theories of this type (technological utopianism and anti-utopianism) do offer a number of insights into the question of privacy in the information society and help to clarify that the major issue with regard to privacy in such a society is the exercise of power.

Building upon this foundation it can be seen that Marxian analysis places the Information Revolution firmly within the framework of Marxian concerns. Since information control is a function of the capitalist class's hegemony, it is natural to expect the erosion of privacy. The state and capitalist institutions *surveille* to control, by minimising dissent. In addition capitalist surveillance of workers enables them to be disciplined so that they work at maximum efficiency, and surveillance of the population enables the more efficient operation of the market, thus maximising profit. Another profit related factor is the value of information as a commodity. This ensures that its collection wherever possible can be potentially profitable, and is thus a final impetus for the invasion of privacy.

In a similar fashion the theory of the nation-state and violence, while acknowledging some of the Marxian concerns (such as the reasons for corporate surveillance of the population), adds a layer of sophistication to the debate by pointing out the importance of the state as an entity in its own right (not merely as a capitalist tool). The emergence of the modern state is accompanied by bureaucratic control. The modern state due to its need to protect itself has needed to develop ever more complex surveillance mechanisms to put into operation against enemies within and without (and this has been a major factor in the development of Information Technology). The requirement of defence also ensures tight administration, as the population must be potentially mobilised in the event of war. In addition states tend to buy the willingness to fight through the provision of services which require a competent administration. To support this war-readiness taxes must be collected, which adds yet another reason for surveillance.

While these theoretical models are useful in the analysis of power, social control and information, the one felt most useful for the purposes of examining the relationship of privacy and information (particularly with respect to GI in the information age) is Foucault's theory of power/knowledge. This consists of a combination of panopticism and the confession.

While the rise of the nation-state and the need to organise the population, and the needs of capital and its intimate relationship to the information society help to explain the operation and source of power conflicts in the Information Age, Foucault's explanations show the way in which they operate at the level of the individual. Foucault's analysis incorporates the

importance of capital, the state, a complex society and the extension of equality of rights. However, its strength is that it looks at the issue of power from the position of the subject.

The two technologies of panopticism and the confession together allow the functioning of discipline, but also of the information society itself, generating, as they do, vast quantities of information on individuals which is then used commercially and by government for a variety of means. A critical examination of the methods of collection of personal information in the modern world will reveal that it conforms to one or other technology or a combination of both. For example monitoring by tax authorities is largely surveillance in the panoptic mode, but much of the collection of information is through the voluntary filling out of forms.

In this can be grouped most government information regarding the individual, that held by financial and other such bodies. In each case the simple interaction with such organisations places the individual in a position where information is sought (even if this is only at a distance, as, for example, through recording one's image on the now ubiquitous CCTV video systems). The importance of the acceptance by the population of the confessional technique can also be clearly seen. The existence of a multiplicity of voluntary surveys seeking detailed personal information, such as those accompanying many newly purchased electronic products could not be effective without the desire to reveal information<sup>22</sup>.

Another important contention of Foucault's is that power is not exercised over individuals, but rather is exercised through them. This is most clearly illustrated by confession, but is also clear in the technology where it is the individual who becomes the bearer of the responsibility for his own discipline when under surveillance. Power thus forms a network of interaction within society in which everybody is implicated, but which some extract more from (capital and state bureaucracies in particular: this power network has as one of its chief effects the efficiency of societal organisation and of economic production). This same network of power engenders opposition and resistance, and this too exists as a part of the network of power. Consequently those in power must keep constantly developing strategies which ensure that they are favoured by the play of forces. Power is a constant battle.

<sup>&</sup>lt;sup>22</sup> Such surveys often request very detailed personal information on matters such as income while offering nothing but the slim chance of winning a 'prize' in return

Another interesting paradox raised by these works is that the very existence of the modern individual is directly related to the power of information. Thus the question of privacy which is so important to most individuals in our individualistic society may paradoxically be irrelevant. Surveillance is part of what has created the conditions of modern existence, the desire for privacy included. This may well be one of the paradoxes of a society with a facade of egalitarian laws built in front of a disciplinary machinery more complex and integral to everyday life than that of any other society in history.

Perhaps the most salient question this raises is whether privacy in the current world is really a matter of illusion. Perhaps those who discount the importance of privacy (pointing out the ease with which people routinely abandon it in a confessional society) are correct. Is there really privacy? The panoptic mechanism and the emergence of the disciplinary society clearly underlines the importance of privacy in terms of the freedom of individuals. Privacy itself the only protection from what Foucault contends is the source of power in modern society. Or is it too late? Has the "counter-law" of discipline "which supports, reinforces, multiplies the asymmetry of power" (Foucault, 1979: 223) already overcome the law of equality and rights?

These ideas and questions will underlie the examination of the interaction of privacy and GI in Ireland in the late, 1990s.

### **Chapter Five**

Legal Protection of Privacy in Ireland

## 5.1 Introduction

As has already been discussed the right to privacy is somewhat contentious, largely due to the difficulty in defining it, and also due to the complex of issues it includes. However, there is little doubt that privacy is regarded as being highly important in many societies. This is especially so in modern societies with complex social interactions where the expectation of privacy is very strong and encompasses many issues. In consequence the importance of privacy has grown as society has evolved into its current form. One result of this growth is the late development of debate on the importance of privacy<sup>1</sup>. As a result of the relatively recent origins of the debate and the consequent recognition of the importance of privacy, and the difficulty of legislating for privacy, the legal protection of privacy is often weak and fragmented.

## 5.2 The Right of Privacy in Irish Law

The right of privacy in Ireland falls into this category of fragmented legal protection. According to the Law Reform Commission (1996a, 1998), Ireland has no specific right of privacy or privacy law. Instead privacy is subject to partial protection with its diverse origins in international law, the Irish Constitution and case law, and native legislation with privacy implications.

<sup>&</sup>lt;sup>1</sup> The entire legal debate concerning privacy was sparked by the Warren and Brandeis article published in 1890.

## 5.2.1 Defining Privacy in the Irish Legal Context

It has been noted in Chapter Three that privacy is extremely difficult to define precisely. This makes its legal protection extremely difficult since without a definition of what comprises privacy the law cannot act to protect it. Although privacy remains as elusive in Irish law as elsewhere there have been efforts made to define it at least in terms of the elements of which it is composed. In Irish law the responsibility for researching necessary legal reforms and suggesting them to the Oireachtas is vested in the Law Reform Commission, established by Act of the Oireachtas in, 1975 for this purpose (Law Reform Commission Act, 1975). As one of the main areas the Law Reform Commission is mandated to work on is the law of privacy it seems best to accept the description adopted by them in their, 1996 Consultation Paper on Privacy and the follow up Report (1998). It is likely that due to their statutory role this will become the legal basis of privacy law in Ireland.

The Law Reform Commission, rather than defining such a difficult concept, chose to adopt a legal description of privacy based on that developed in Canada, and elaborated in Australia. This description is based on three areas of privacy, namely:

- Territorial privacy (privacy based on private property);
- Personal privacy (based initially on the idea of personal space and then on the essential moral autonomy of the person);
- Privacy in the informational context (based on the idea that information about a person belongs fundamentally to that person).

To this Canadian description they add the Australian refinement of a fourth category:

 Privacy from surveillance and the interception of communication (Law Reform Commission, 1996a, 1998).

They point out, however, that this last category is not a fourth separate category but rather is a particular issue that arises within each of the other categories possessing significance in its own right<sup>2</sup>.

<sup>&</sup>lt;sup>2</sup> It is to the issue of Surveillance and the Interception of Communications that both the Consultation Paper and Report were addressed.
This description of privacy is largely agreed with by Forde (1987: 538) who lists a number of Irish legal rights which "may be subsumed under the heading of privacy and personality". These are "not being physically interfered with" as well as "confidentiality in the broader sense, such as a right not to be searched or have one's home or property searched, not to be the subject of clandestine surveillance and not to have one's private affairs disclosed to the public." (Forde, 1987: 538). These largely enumerate the LRC definition of privacy of the self, of the home, and from surveillance. Privacy of personal information is included by Forde in his analysis of confidential information and includes issues such as forced disclosure of information, personal search, property search, interception of communication, and surveillance through data banks (Forde, 1987).

5.2.2 Ireland's Obligations under International Human Rights Law

Much of Ireland's protection of privacy grows directly out of international treaties rather than native law. This is true in the general sense of the overall right to privacy as well as the specific informational sense where international data protection initiatives have heavily influenced domestic law.

The most important body of international rights law is *The International Bill of Human Rights* comprised of the "Universal Declaration of Human Rights, the International Covenant on Economic, Social and Cultural Rights, and the International Covenant on Civil and Political Rights and its two Optional Protocols" (UNHCHR, 1996 - Fact Sheet No. 2). Together these form the international legal basis of all claims to human rights. Of the three, two make explicit reference to a right of privacy: the Universal Declaration of Human Rights (UDHR), and the International Convention on Civil and Political Rights (ICCPR). The UDHR's importance lies in the fact that it was the first international statement of human rights, adopted by the United Nations General Assembly in 1948. It makes a specific guarantee of a right to privacy in Article 12:

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the

protection of the law against such interference or attacks."(Article 12, Universal Declaration of Human Rights, 1948)

The UDHR, however, does not have the force of law, as it is not a binding Treaty. It is thus ignored by many states, and criticised by others as a culturally imperialistic attempt to force western values on the rest of the world<sup>3</sup>. It remains, despite these problems, the basic document upon which all human rights are ultimately legally based. According to the Secretary-General of Amnesty International: " the only agenda we need... is to implement it" (Cullen, 1998: 2).

Thus although the UDHR is important because of its universality it lacks legal force. This is provided by the other elements of the International Bill of Human Rights, the International Covenants. Of these it is the International Convention on Civil and Political Rights that is relevant to privacy which is protected under Article 17 (ICCPR, 1966). According to the Law Reform Commission it is this treaty in combination with the European Convention on Human Rights which actually provides the framework of international obligation in dealing with the privacy issue in Irish law (LRC, 1996a). The Covenant entered into force for Ireland in 1990 and Ireland is one of the states to also have ratified its First Optional Protocol (LRC, 1996a). This means that Ireland accepts the "competence of the HRC (Human Rights Committee)" to deal with complaints against the state by individuals, and thus makes the ICCPR an effectively enforceable treaty (McGoldrick, 1994). The wording of the privacy clause of the Convention of privacy) is not defined and there is not any list of what is and is not legitimate invasion of privacy (LRC, 1996a).

The European Convention on Human Rights was signed by Ireland in, 1950 and came into force in, 1953. The Article of the Convention dealing directly with privacy is Article 8, although Article 6 and Article 13 are also relevant (LRC, 1996a). Unlike the ICCPR the situations in which a person's privacy may be invaded are detailed, as well as the fact that interference must also be lawful and "necessary in a democratic society" (ECHR, 1953: Art.

<sup>&</sup>lt;sup>3</sup> The counter arguments such as that of the UN Secretary General Kofi Annan is that "It was never the people who complained of the universality of human rights, nor did the people consider human rights as a Western or Northern imposition. It was often their leaders who did so." (http://www.unhchr.ch/html/stms/sg971020.htm).

8). Ireland has not, however, enacted the Convention into Irish law and thus any action under the Convention can effectively be delayed for years as it passes through the Irish courts before reaching the European Court (Farrell, 1997). This failure to enact the Convention may be reversed under the terms of the 1998 'Good Friday' Agreement which states that: the "question of the incorporation of the ECHR will be further examined [by Ireland] in this context" (Agreement Reached in the Multi-Party Negotiations, 1998: 20).

### 5.2.3 Privacy and The Constitution and Common Law

Ireland's legal system diverged from that of Britain in 1922 at independence. All prior law is thus held in common with only the subsequent legislation and case law, and Ireland's constitution differentiating the two. The current constitution Bunreacht na hÉireann, was adopted in 1937 and "consisted of the completion of unfinished business left over from, 1922" (Morgan, 1990: 12). Thus Irish constitutional law is law is largely coherent for the period since independence, and is closely allied to British law, with the addition of indigenous legislation passed since, 1922, and court decisions in the same period (Morgan, 1990).

In the context of human rights it is the constitution, and related case law, which are most significant as it is these which have defined the "State-individual relationship", while legislation has been focused more on the organs of the state (Morgan, 1990). The rights provisions of the constitution include explicit protection for the following rights in Articles 41 to 44:

- Family rights
- Education
- Private property
- Religion (including freedom of conscience)

Article 40 also contains a number of provisions relating to personal rights:

- The equality of all citizens and a guarantee to vindicate the rights of citizens
- The right to life
- The right to freedom from unjust detention
- The right to an inviolate dwelling
- The right to freedom of expression and assembly
- The right to form associations.

Thus the Constitution does not explicitly guarantee a right to privacy though there is a right to private property (Article 43), and to inviolability of the dwelling (Article 40-5) which protect some limited aspects of privacy directly (Forde, 1987; LRC, 1996a; LRC, 1998).

As is the case in the USA, however, case law decisions have "so construed the provisions of the Constitution, in particular the fundamental rights provisions, as to afford a degree of protection to privacy interests (LRC, 1996a: 38). Thus, although no specifically privacy based case has been brought some facets of privacy are protected under the interpretations of various articles of the Constitution (Morgan, 1990). These include the privacy of the sexual relationship of a married couple which was protected by provisions for the protection of family life under Article 41 (LRC, 1996a). An attempt to extend the right to privacy to ban "state interference with private, personal conduct where no compelling state interest was involved" (Morgan, 1993: 16) was unsuccessful in Norris vs. A.G., however (Morgan, 1993).

In addition to the protection offered to privacy through judicial interpretation of the Constitution, additional aspects are protected by the common law. These include invasions of privacy which "amount to actionable trespass, nuisance, defamation, breach of copyright, and breach of confidence" (Forde, 1987: 539). The offences of Breach of the Peace and Eavesdropping also provide some protection (LRC, 1996a). However, the combination of constitutional law and common law amount to "far from complete protection" (Forde, 1987: 539). The absence of a definite Tort of Privacy such as exists in the US is thus a clear problem prompting the Law Reform Commission to advocate the creation of one (1996a, 1998).

#### 5.2.4 Legislative Protection of Privacy

In addition to the provisions of the Constitution with regard to the rights of the individual, there are certain elements of the legislative code, which protect privacy. There is not, however, any explicit Privacy Law such as that which exists in Germany (LRC, 1998). Instead the legislation that protects privacy is legislation focused on another issue such as regulating the national broadcasting station, the telephone network, or the postal system (Forde, 1987). Such legislation, as part of its main purpose provides some privacy protection in an incidental manner. For example, regulatory legislation for the telephone network may protect privacy through its outlawing of telephone tapping to protect the integrity of the telephone system. The number of Acts that have such an indirect bearing on privacy is quite large. The LRC (1996a), for example, lists thirteen Acts that afford some protection against privacy in the sense of the interception of communication, seven of which predate independence in 1922.

The one area of privacy that is the specific focus of Irish legislation is that of information privacy, particularly in the context of the Data Protection Act (1988), although the LRC state that "there is, however, no overall protection of private information under Irish law at present" (LRC, 1998: 9). The subject of information law in Ireland and its impact on privacy will be discussed in the Section 5.4, with particular emphasis being given to the Data Protection legislation.

### 5.3 Information Privacy and the Law in Ireland

These include the Data Protection Act of 1988, which is the fundamental piece of legislation dealing with privacy in the context of the information, dealt with in greater detail later. In the context of the Information Society a number of Acts impact on the situation. Although the most important when dealing with privacy is the Data Protection Act of 1988, due to be updated shortly, the Official Secrets Act and Freedom of Information Act, and the Criminal Damage Act also have some bearing.

#### 5.3.1 Criminal Damage Act, 1991

The Criminal Damage Act of 1991 is Ireland's legislation dealing with computer crime. It is not, however, a piece of legislation specifically designed to deal with such crime. Instead it forms part of a series of laws relating to criminal damage. The Act was actually intended to implement the LRC's recommendations on Malicious Damage, and the insertion of sections relating to computer crime seems to have been something of an afterthought, tacked onto legislation intended for another purpose (Kelleher and Murray, 1995). Its significance in regard to information privacy is largely concerned with its provisions for the punishment of hackers, and thus with protecting information stored on computer from unauthorised access and damage.

The Act defines four offences:

- Damage to property
- Threatening to damage property
- Possession of anything with intent to damage data
- Unauthorised access to a computer

(CDA, 1991: Sections 2, 3, 4, 5; Kelleher and Murray, 1995: 187)

The first two offences are quite general and relate to any criminal damage to property. However, property for the terms of the Act is defined as meaning "property of a tangible nature", or "data", meaning "information in a form in which it can be accessed by means of a computer and includes a program" (CDA, 1991: s. 1-1). Thus the two offences of damage or threats of damage can be brought to bear either in the relation to such damage occurring or being threatened to either data or programs.

According to Kelleher and Murray the third offence of possession of anything with intent to damage data may be the most effective offence under the act. It "is important as it may be difficult to prove that a hacker has actually caused criminal damage or accessed a system without authorisation. If it can be shown that the hacker had things in his possession which would be used for hacking then he could be convicted of an offence" (Kelleher and Murray, 1995: 201). One problem with this offence, however, is that the term 'anything' makes the

breadth of the offence very great and also makes it difficult to prove, as it is necessary to show intent to use the 'thing' to cause damage (Kelleher and Murray, 1995).

The final offence is fundamentally different to the others as it is "specifically intended to apply only to computer crime and has no other application" (Kelleher and Murray, 1995: 202). It applies specifically to activities of a hacking type as it means that "accessing data without lawful excuse" (CDA, 1991: s. 5-1) is a crime, whether or not access is actually obtained and whether or not it is possible to prove that damage has been done. This section of the Act also outlines the jurisdiction of the offence as applying not only within the state but also outside it. The latter is the case if a person in the state unlawfully accesses data outside it, or if a person outside the state unlawfully accesses data within the state (CDA, 1991: s. 5-1). Various different penalties are laid down for the different offences ranging from fines to imprisonment (CDA, 1991; Kelleher and Murray, 1995).

The importance of the CDA to privacy concerns is twofold. Its first obvious benefit is that it criminalises the unauthorised accessing of data. This potentially includes not only hacking but any access to data to which one is not entitled to access: thus an employee of an organisation could be subject to prosecution for accessing restricted personal data without permission. The second element of the Act relating to privacy is the question of damage or the threat to damage data, if such data are personal data. However, the recognition of the importance of data accuracy and integrity under the Data Protection Act, 1988, deals with this issue comprehensively. The importance of the CDA is thus largely confined to its criminalisation of unauthorised access.

However, many problems exist in regard to the Act, which have the potential to undermine its operation even in the event of such access. One of the chief criticisms of the Act is the imprecise definition of many key terms as without them "it may be difficult to effectively prosecute computer crime" (Kelleher and Murray, 1995: 251). Examples of terms the Act uses but does not define include 'computer', 'access' and 'storage medium'. The LRC has suggested that this should be rectified as their ambiguity may "render those sections of the Act which deal with computer crime unconstitutional as the terms are ambiguous" (Kelleher and Murray, 1995: 188). Kelleher and Murray go on to outline many other problems with the Act that may in effect make it unworkable including:

- Potentially criminalising the existence of a virus on a computer;
- Potentially criminalising the possession of a computer and modem;
- Potentially criminalising all uses of a computer (Kelleher and Murray, 1995).

The failings of the CDA thus include potential unconstitutionality and weakness of definition of offences, both of which make the Act potentially inapplicable. Its weakness can perhaps best be gauged by the fact that in eight years no prosecutions have been brought. The main problem is that "computer crime offences were included as an afterthought to meet a perceived threat" and the result is that there have been calls for its amendment or replacement almost since its enactment (Kelleher and Murray, 1995: 235). The limited protection of privacy of data thus afforded by the Act may largely be irrelevant.

5.3.2 Official Secrets Act, 1963 and Freedom of Information Act, 1997

#### The Official Secrets Act, 1963

Ireland inherited a culture of official secrecy of government from the British, embodied in the Official Secrets Acts of 1911 and 1920. The current Official Secrets Act was enacted in 1963 and repealed the previous British Acts (OSA, 1963: s3). The 1963 Act strengthened the provisions of official secrecy, and is very broad in its scope and in its definition of official secrets (McGonagle, 1998; Foley, 1998a). The definition of Official Information under the Act is as follows:

"Official information' means any secret official code word or password, and any sketch, plan, model, article, note, document or information which is secret or confidential or is expressed to be either and which is or has been in the possession, custody or control of a holder of public office, or to which he has or had access, by virtue of his office, and includes information recorded by film or magnetic tape or by any other recording medium" (OSA, 1963: s. 2-1).

In addition to this definition a certification by a Minister that something is secret "shall be conclusive evidence of the fact so certified" (OSA, 1963: s. 2-3). The Act provides that it is forbidden to communicate or disclose, obtain or retain any such information. The definitions of these terms mean that the "substance, effect or description" of any information is covered,

that "copying" is covered, and that communication of information includes "transmission", and refers to communication "in whole or in part" (OSA, 1963: s. 2 -2).

Until the passage of the FOI Act thus, any official document was considered secret unless otherwise stated and a ministerial declaration could also make something a secret (Foley, 1988). This meant that until this year Ireland was "the most secretive country in the EU and probably beyond" (Foley, 1998a). Although the result was a 'comfort zone' wherein civil servants and politicians could ensure that any inconstancies in their actions were not scrutinised (Donovan, 1998), this legislation did ensure that government held personal information was not permitted into the public domain. In one sense, thus the OSA protected privacy. However, official secrecy also meant that any personal information given to government was thereafter a secret and could not be checked by the individual concerned. In effect the individual surrendered all rights to such information when the information was surrendered. Such rights as the right of access and of amendment, and the right that information only be used for a specified purpose, that are a key to the Data Protection Principles did not thus exist. It was only with the introduction of the DPA in 1988 that the individual regained rights to such information. Thus although privacy was protected its protection was so absolute that the individual did not have any right in regard to the information.

The introduction of the FOIA (1997) has changed the parameters in which the OSA acts, however, replacing an official policy of secrecy with one of openness though the OSA remains in force. Section 48 of the FOIA, which enables this, states that: "a person who is, or reasonably believes that he or she is, authorised by this Act to communicate official information to another person shall be deemed for the purposes of section 4 of the Official Secrets Act, 1963, to be duly authorised to communicate that information" (FOIA, 1997; s. 4). According to McGonagle (1998), however, the FOIA does not go as far as was hoped and the OSA has been subject to "only minimal amendment to ensure that the new Act is not totally frustrated".

#### **Freedom of Information Act**

The different ethos of government involved in the FOIA is encapsulated in its provision for access to "any record held by a public body....subject to the provisions of this Act" (FOIA,

1997: s 6-1). In practice, however, the 'provisions' of the Act severely circumscribe this access. Twelve categories of information (see Table 5.1) are exempted from freedom of information their definition is quite broad in definition. According to McGonagle (1998) this is casts doubt as to the effectiveness of the legislation as "experience elsewhere has been that exemptions are invoked to the limit". In addition, as is the case with the OSA, which is still in force, a Minister can issue a certificate of exemption from the FOIA (section 25).

toes have

at release of the

Table 5.1: Exemptions from the Freedom of Information Act

- 1. Meetings of the Government (s. 19),
- 2. Deliberations of Public Bodies (s. 20),
- 3. Functions and Negotiations of Public Bodies (s. 21),
- 4. Parliamentary, court and other matters (s. 22)
- 5. Law Enforcement and Public Safety (s. 23)
- 6. Security, Defence and International Relations (s. 24)
- 7. Ministerially certified records under sections 23 and 24 (s. 25)
- 8. Confidentially obtained information (s. 26)
- 9. Commercially sensitive Information (s. 27)
- 10. Personal Information (including that relating to a deceased individual) (s. 28)
- 11. Research and Natural resources (s. 30)
- 12. Financial and economic Interests of the State and Public bodies (s. 31)

(Source: FOIA, 1997: Sections 19 to 32)

In addition the information that is not exempt is only subject to freedom of information if created after the "commencement of the Act" (s. 6-4), except where the information relates to the person making the request, or is necessary to understand information created after the commencement (Foley, 1998a). In regard to information of a personal nature<sup>4</sup>, such information is available to the subject of the information. It may also be made available to others in certain circumstances such as when the subject consents or when the "public interest that the request should be granted outweighs the public interest that the right to privacy of the

<sup>&</sup>lt;sup>4</sup> Defined as information which would ordinarily be known only to the person or somebody close to them, and which is held by a public body in confidence (FOIA, 1997: section 2)

individual....should be upheld" (FOIA, 1998: s. 28-5). The Act also appoints an Ombudsman to oversee the working of the Act (Sections 33 - 40), and grants a right of correction where information on an individual is incorrect (Section 17).

The Act has been criticised for a number of reasons including the dilution of its effect through the extensive list of exemptions (McGonagle, 1998), and the cost of making applications (Balls, 1998b). Additionally the attempts by some government departments to dilute the effects of the Act have been criticised (Foley, 1998a). However, although the Act may not live up to expectations it has had a number of important effects in regard to information privacy and data protection issues. The Act is not specifically privacy-related but it does have a number of provisions which impact on data privacy and related rights with regard to government held data. The most directly privacy-related provision of the Act is the exemption of personal information from its terms except in cases where the subject requests the information or where there is an overwhelming public interest in disclosure. This concern with privacy of the individual is also reflected in the power of civil servants in some circumstances to "decide to conceal your identity by, for example, blanking out your name if it appears on a form that has been requested" (Donovan, 1998). In addition there is an obligation to inform the subject when disclosure takes place, which means that the subject is at least protected by knowledge that the information is no longer confidential. In such cases there will be a " 'harm test' whereby you must be able to demonstrate that release of the information would be harmful" in order to prevent its release (Donovan, 1998).

In addition to this direct concern with privacy two further aspects of the Act are also effectively data protection provisions protecting the citizen in interaction with public bodies. Two of the Data Protection Principles which form the basis of data protection legislation in Europe are the right of access to records, and the right to correct such records (Council of Europe, 1981). These rights are enshrined in the FOIA: access is guaranteed (with exceptions) by the fact that there is freedom of information, while the right of correction is granted under Section 17. The provision of these rights, though already extant under the DPA, in regard to government information is an important reinforcement of data protection and its associated

rights. An area where the FOIA exceeds the provisions of the DPA is that it applies equally to manual (for example, paper) as to digital records<sup>5</sup>.

One final way in which the FOIA has an indirect impact on privacy and related issues is in its introduction of open government, however limited. Such a spirit of open government is fundamental in an era when the volume of information being collected about citizens, the manipulative processes to which it can be subjected, and the number of uses to which it can be put is expanding exponentially. In effect it means that we "can find out how much Big Brother knows about us and whether what he knows about us is demonstrably true" (Donovan, 1998). In this respect the FOIA, in addition to its practical initiatives, has an important symbolic role, specifically permitting them these rights in respect of government which is traditionally assumed to be the most likely enemy of privacy in the digital age.

#### 5.3.3 Data Protection Act, 1988

#### The Origins of Irish Data Protection

Ireland's data protection legislation has its origins in international initiatives chiefly at the European level. Two interrelated international initiatives by the Organisation for Economic Co-operation and Development (OECD) and the Council of Europe gave rise to the Irish DPA (Clark, 1989). In 1980 the OECD set forth recommendations that individual countries implement its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* and cooperage in facilitating transborder data flows. The principles which the OECD set out in this context were ratified by Ireland in1986 and are a forerunner of the data protection principles in the DPA, 1988 (Clark, 1989). The more direct influence, however, was the *Convention for the Protection of Individuals with Regard to Automatic Processing of Data* (1981) of the Council of Europe, ratified by Ireland on the same day as the OECD Guidelines.

<sup>&</sup>lt;sup>5</sup> As will be discussed below the EU Directive on Data Protection does extend data protection to manual records but the Directive, due for implementation on 24 October (1998) has yet to be effected in Irish law.

The focus of the Convention was on the rights of individuals rather than specifically on the facilitation of transborder data flows. Important aspects of the Convention included:

- Setting forth data protection principles and the rights of data subjects;
- Establishing a Consultative Committee at European level on which each signatory is represented;
- Setting out the conditions where export of data was permissible (Clark, 1989; Council of Europe, 1981).

Because the Convention was an internationally binding treaty obliging signatories to enact legislation for data protection it "is probably the most influential factor in explaining why and how the Irish Act was implemented in its present form" (Clark, 1989: 18). In addition the EEC Commission in 1981 issued Recommendation 81/679/EEC that the Convention be adopted by member states and ratified by 1982, although this recommendation was not strictly enforced (Clark, 1989).

The origins of Data Protection were thus not native to Ireland, and in addition the main thrust of the international initiatives was on the safeguarding commercial interests rather than on personal rights. Without such an initiative the fear was that various national laws would not work together, and that states that provided no protection at all would attract unscrupulous data controllers hiding from the laws in other jurisdictions (Clark, 1989). Rather than being led by civil liberties interests thus "at an international level pressure for legislation has been industry or commerce led rather than the result of any political or civil libertarian lobby" (Clark, 1989: 17). Though foreign in origin the potential of data protection was quickly realised by Irish business also since it encouraged security, confidentiality and good data management which could help to avoid legal liability for the "provision of incorrect data" (Clark, 1989: 22). The result is that "the introduction of this legislation was attributable to economic and practical considerations, rather than the protection of privacy rights....the advent of the Financial Services Centre at the Customs House Docks site was a key factor." (McMahon and Binchy, 1992: 698).

#### The Data Protection Act, 1988

The Data Protection Act was enacted in 1988 to fulfil Ireland's international obligations under the Convention and to enable the country to participate fully in international data flow. The strong influence of the Council of Europe Convention is clear in the Act which is based on a list of Data Protection Principles (see Table 5.2) similar to those set out in the Convention (DPC, 1988). It provides for certain protections for digitally stored personal information, for certain rights for the data subject, and for certain obligations on the part of the data controller or data processor. Unlike the FOIA, manually held information is not included in the provisions of the Act, although the EU Directive on Data Protection discussed below extends protection to manual records (EU Parliament and Council, 1995). In common with other similar legislation across Europe it establishes an ombudsman to monitor the operation of the Act, though this is not specifically required by the Council of Europe Convention (DPA, 1988; Council of Europe, 1981).

a universal system of

ta (Llov 1996)

intenal le given the

#### Table 5.2: Data Protection Principles in Ireland

1. The data must be collected for a specific and lawful purpose	
2. The data must be fairly obtained	
3. Use and disclosure of the data must be fair	

- 4. The data must be secure
- 5. Data must be kept accurate and up to date
- 6. Data must not be excessive
- 7. The data must not be kept for longer than necessary
- 8. There must be strict controls on data matching
- 9. A de facto national identifier must not emerge

(Source: DPC, 1988)

#### Data Subject's Rights:

In effect the Principles set out above impose a set of obligations on data processors and in consequence provide the data subject with rights corresponding to those duties. The most basic right under the Act is to know exactly what information is being held, by whom, and for what purpose (DPA, 1988: s. 2, 3). In practical terms this means that when the information is initially collected the individual should be informed of the purpose for which it is kept (Section 2). In the case of its use in direct marketing should be given the right to refuse to have it used for this purpose (Section 2-7). Once information has been collected the individual possesses a right of access just as is the case under the FOIA: on applying in

writing to a data controller the individual can obtain a copy of all information held on him/her (Section 4). The right of correction of inaccurate data also exists: this right allows the alteration of incorrect data and the deletion of data that are being held where inappropriate within forty days (Section 6). The latter also applies when the purpose for which data were collected no longer applies (Section 6). In the case of deletion or alteration the data controller or processor is obliged to inform all other controllers or processors to whom the information was made available in the previous year (Section 6-2).

#### Registration and the Data Protection Commissioner:

The Act establishes a national register of data controllers and processors to be administered by the Data Protection Commissioner who is charged under Section 10 with overseeing the operation of the Act, dealing with complaints against data controllers and processors, and enforcing compliance where necessary. Registration, unlike some other jurisdictions such as the UK, is not universal amongst data controllers and processors. Such a universal system of registration exists in earlier legislation of this type but was realised to be untenable given the exponential growth in the numbers of computers used to store personal data (Lloyd, 1996)<sup>6</sup>.

Instead the Act has a system of selective registration of the following categories of controller:

- Public authorities (16-1 a);
- Financial, insurance, direct marketing, credit-referencing or debt collecting agencies (16-1
   b);
- "Any other data controllers who keep personal data relating to (i) racial origin, (ii) political opinions or religious or other beliefs, (iii) physical or mental health.....(iv)sexual life, or (v) criminal convictions" (DPA, 1988: 16-1 c).

In addition all data processors (those who conduct data processing for data controllers where such functions are separate) are obliged to register (Section 16-1 d). An important point is that the data protection principles and the rights and duties that derive from them apply *to all personal data held in digital form*, regardless of whether the data fall into the categories required to be registered under the terms of the Act (Clark, 1996; DPA, 1988).

#### Codes of Practice:

An unusual aspect of the Act is its provision regarding Codes of Practice. The Data Commissioner is obliged to encourage "trade associations and other bodies representing categories of data controllers to prepare codes of practice to be complied with by those categories in dealing with personal data" (DPA, 1988: s. 13-1). Any such Code, if accepted by the Commissioner, can then be approved by the Oireachtas, in which case it acquires the force of law, in effect replacing the Act for the purposes of data protection within that industry (DPA, 1988; OECD, 1994).

#### **Operation of the DPA**

The Data Protection Act is thus a statute heavily influenced by European initiatives and bearing a close relationship to other European legislation. Its operation has been relatively smooth in the eleven years since it was enacted. Over that time the Data Protection Commissioner has received a steadily growing number of registrations as indicated in Table 5.3 which gives details of the growth in registration in the initial eight years of its operation from 1989 until 1996. A full breakdown of registration during these years is contained in Appendix One.

Year is not classed as sens	Number Registered	% Increase
1989	1194	- the DPC (discussed below)
1990	1432 while because the the frie	19.9 (DPC, 1998). Clearly
1991	1460	2.0 This makes the size of the
1992	1536	5.2 on to information that an
1993	1821	18.6
1994	1944	6.8
1995	2082	7.1
1996	2353	13.0
1997	2571	9

#### Table 5.3: Registration under the DPA from 1989-1996

(Source: Data Commissioner's Report, 1996: 13)

<sup>6</sup> The British Data Protection Registrar estimated the shortfall in registration in 1994 as over 100,000 (Data Protection Registrar, 1994)

As can be seen the overall number registered increased by over 100% in the interval from 1988-1997. The particular growth in certain years is often the result of a publicity drive by the Commissioner concentrating on a particular profession or other group. One such example was a campaign to increase registration from medical professionals during 1995-1996 which resulted in an increase from 180 to 242 'doctors, dentists and other health professionals', and from 349 to 495 'pharmacists' (DPC, 1997). Although the figures seem to indicate a very low registration rate this is in all likelihood due to the restriction of the requirement to register to those who hold the most sensitive personal information, and those with the greatest power to abuse such information.

In this context Table 5.4 is very important as it shows that the number of those registered who are registered because of the sensitivity of the data they hold is very significant. The figures must be read with some caution, however, as there is a possibility that some controllers may hold data under more than one sensitive category. Hospitals, for example, which obviously hold health data tend also to hold information on religious affiliation for administrative purposes. Nonetheless the number of such registrations, 1671 of a total 2353, is very significant as it shows that registration on the basis of sensitivity makes up over 70% of all registrations. When the number of registrations by institutions holding financial data (636), which is not classed as sensitive under the Act, are added the total rises to 2307<sup>7</sup>. It is justifiable to make this addition as, according to a survey by the DPC (discussed below) financial information is regarded as highly sensitive by the Irish public (DPC, 1998). Clearly sensitivity of information is one of the key factors in registration. This makes the size of the Register less relevant than the fact that almost every entry is in relation to information that an individual would like to be kept highly confidential.

<sup>&</sup>lt;sup>7</sup> Figure arrived at by adding the 1996 registrations of: Credit Unions and Friendly Societies, Associated banks, Non-associated banks, Building Societies, Insurance and Related Services.

Physical/Mental Health Racial Origin		957	
		156 terms of DPA (1988)	
Political Opinions		54	
Religious/Other beliefs		184	
Sexual Life		159	
Criminal Convictions		161	
1991	34		

Table 5.4: Breakdown of Registration	Based on	Sensitive	Information	in 1996
--------------------------------------	----------	-----------	-------------	---------

(Source: DPC, 1997: 14)

In looking at the complaints made to the Commissioner (Table 5.5) one finds that the level of complaint is also relatively low, with formal complaints in any given year never rising above 37 between the implementation of the Act and 1996. The publication of the informal complaints for 1995 and 1996 indicates a higher level of dissatisfaction than the official complaint level. However, the fact that such complaints do not reach the formal stage indicates that they were solved relatively easily where they were legitimate complaints under the Act. A second factor that emerges from the figures, however, is that the apparent halving of complaint levels from 1995 to 1996 is somewhat misleading. As the level of informal complaint remained relatively steady it must be assumed that people continued to have problems under the Act in the same numbers. It may be an indication that problems encountered were solved without the Commissioner having to resort to the use of the full power of formal intervention. This could either reflect a change in the style in which the DPC deals with complaints or a greater degree of co-operation from the registered organisations.

It is also significant, in light of the finding by the DPC that people are most sensitive about financial details, that in most years for which such information is available the largest number of complaints under the terms of the Act were made against the financial sector (DPC Reports, 1989-1997). This does not necessarily mean that this sector is any less compliant with the terms of the Act but rather reflects the immediate and drastic effect which a mistake, or other database problem, can have on an individual in dealing with financial institutions. Whereas a person may never be particularly affected by a record of their true or suspected political

allegiances being held by a political party, the refusal of a mortgage because of a flawed credit report will have immediate consequences.

Year to concentrate such	Formal Complaints	Informal Complaints*
1989		
1990	25	
1991	34 concerned with finding out	the chief concerns of the Irish
1992	30 ssues. The results pointed of	ut the prime importance of the
1993 details	24 fored cather, which perh	ips surprisingly proved more
1994 and than health information	24 0 0000000000000000000000000000000000	(8). Both financial history and
1995	37 million decadle in order allowed and	84 http://www.second.com
1996	18	85 and telephone number also
	98).	
		* From 1996 Report

Table 5.5: Complaints made to Commissioner under terms of DPA (1988)

(Source: DPC Reports from 1990-1996, inclusive)

#### DPC's Survey of the Attitudes of the Irish Population

In 1997 the DPC conducted a survey of the level of awareness of the Irish public of data protection and related issues. This was undertaken in part due to paucity of resources available to the Commissioner for education purposes, so that the most efficient allocation of such resources as were available could be made.

The survey addressed three broad issues:

- The level of awareness among the general public concerning data protection
- The awareness of the workings of the Office of the DPC
- The concerns of the public in regard to data protection issues.

In regard to the first two issues the results were somewhat mixed. Only 2% of the public "spontaneously" mentioned the DPC's Office when surveyed, though 25% knew something of the Office and its functions when prompted (DPC, 1998). The Commissioner concludes that

"while people would appear to have some appreciation of their legal entitlements under data protection legislation and an instinctive awareness of acceptable and unacceptable information practices in the computer age, awareness of the role of the Office of the Data Protection Commissioner in these matters was very disappointing" (DPC, 1998: 14). This reflects a situation where the DPC does not have sufficient funds for education of the general public and so has to concentrate such efforts on data controllers to obtain maximum benefits in compliance (DPC, 1998).

The third part of the survey was concerned with finding out the chief concerns of the Irish public in regard to data protection issues. The results pointed out the prime importance of the privacy of financial details, mentioned earlier, which perhaps surprisingly proved more important than health information (O'Sullivan, 1998; DPC, 1998). Both financial history and credit card (92% and 85% respectively) details came ahead of health information (83%) in a rating of 'very important' or 'fairly important'. Both RSI number and telephone number also topped the 70% mark (DPC, 1998).

In connection to the issue of the RSI number some further questions were asked regarding the issue of a National Identity Card and Identity Number. The issue of the use of the RSI number as a de facto National Personal Identifying Number has arisen due to efforts to widen the use to which it is put (discussed below). The results of the survey show a slight majority of the population in favour of a National Identity Card which could be used by state agencies to establish identity, but much less support for the right of private sector bodies to demand it. In regard to the question of use of an identifying number people are "concerned about the use of a national identity number for data sharing or matching, even by public agencies" (DPC, 1998: 14).

A number of further questions concerning data protection principles such as informed consent, fair use, and data sharing produced the following responses:

- Over 90% in each case felt that it was very or fairly important to control the nature of the information collected, who collects it and to be free from observation without consent.
- 89% were very or fairly concerned with the idea of "passive consent" where a data controller informs a subject by letter of a new use to which their information will be used

and assumes consent if no reply is received. The Commissioner felt that this was justification for his previous ruling against passive consent (DPC, 1998).

- Similarly high levels of concern were expressed about:
- Transfers to third parties without informing the subject
- The potential that organisations should be able to use information as they please.

These issues clearly show what the Commissioner described as "instinctive awareness of acceptable and unacceptable information practices" despite the overall low level of awareness of the Act itself and the functions of the DPC (DPC, 1998: 14). One finding is particularly relevant in light of various government initiatives in the 1990s: 88% of those surveyed were concerned by the prospect that one public agency should be able to pass information to another without consent (DPC, 1998). This issue arises in light of recent initiatives in regard civil service practice as exemplified by the Integrated Social Services Report and the Social Welfare Act, 1998.

#### ISS Report and Social Welfare Act, 1998

The 1996 Interdepartmental Report on the Development of an "Integrated Social Services System" sets out a vision of a much more efficient civil service. Based on a business service delivery model, its analysis is that the current organisational independence of the civil service bodies is inefficient. This is not good for "good service delivery, management and use of resources, nor programme control" (Govt. of Ireland, 1996: 11).

The proposed solution to this inefficiency involves a number of initiatives, some of which raise privacy issues, particularly in light of the fact that the DPC's survey revealed that they are of major concern to the public. The main initiatives are:

- Use of a unique identifier, the RSI number
- Integrated Systems development
- A 'one-stop-shop' customer service model
- A central 'means' database
- Issue of plastic cards for increased automation and security
- Computerisation of the General Registry Office (of births, marriages and deaths)

• Sharing of data between bodies using the identifier and integrated systems (Govt. of Ireland, 1996).

The proposed integrated service would be triggered at the registration of birth by the issuing of an RSI number to establish "secure identities and [allow] relevant relationships to be set up" (Govt. of Ireland, 1996: 21). At every subsequent contact with social services the extant data should then be checked and where necessary updated, and "if a person has cause to claim from a number of agencies s/he should only have to give the information once. State agencies should have mechanisms in place to share this data" (ibid. 21). Although the potential benefits of efficiency, improved customer service, reduced red tape, and improved value for public money are substantial, the Report itself acknowledges the potential data protection problems of such a heavily IT driven initiative (Govt. of Ireland, 1996).

According to the DPC's survey in 1997 the particular proposals likely to be of most concern to the public are use of a unique identifier, and the sharing of data across departments without needing to inform the subject, both of which are integral to the proposals (DPC, 1998). The proposals for the expansion of use of the RSI number as a unique identifier are that it should:

- Become the identifier for health purposes
- The student identifier for Department of Education
- The identifier for the General Registry Office data
- The means of transfer of information between Departments (Govt. of Ireland, 1996: 24).

To deal with the data protection issue with respect to RSI number and data sharing the ISSS Committee recommends a number of steps to weaken the power of data protection:

"legislative changes should be enacted to allow for the RSI number to be adopted as a unique public service identifier to overcome the data protection issue; 'specified purpose' as defined in the Data Protection Act, should be revised to encompass public sector bodies and the necessary legislation enacted" (Govt. of Ireland, 1996: 28). However the DPC counters this by a defence of the 'specified purpose' principle as "fundamental to data protection". In consequence "a merging of functions within central government (such as the ISSS) give great cause for concern as they disturb the very basis on which data protection is founded" (Govt. of Ireland, 1996: 107).

In addition to the expansion in the use of RSI number and data sharing, the committee proposes expanded use of the Social Services Card. Though never suggesting its use as a National Identity Card, the committee suggests that it should be used by more government bodies, and even, possibly, by employers to capture employment data. The use of the card as a means of identification for those availing of free travel benefits would mean that "the next logical step would be to include a photograph on the card for all users which would be a major control and security aid in identifying persons" (Govt. of Ireland, 1996: 39). Potentially this raises the issue of the eventual creation of a de facto National Identity Card. This is specifically contrary to the ninth principle of data protection (DPC, 1988), although just over 50% of the public surveyed did not object to the idea if it was used for state purposes (DPC, 1998).

The publication also explicitly acknowledges problems with a further four of the data protection principles, namely:

- 1. The data must be collected for a specific and lawful purpose
- 2. The data must be fairly obtained
- 3. Use and Disclosure of the data must be fair (in regard to the RSI Number)
- 8. There must be strict controls on data matching

(Govt. of Ireland, 1996: 106)

Some progress was made towards the objectives expressed in the ISSS Report with the passage of the Social Welfare Amendment Act (1998) which amends the Social Welfare (Consolidation) Act of 1993. The relevant section is Section14 of the 1998 Act (a substitution for section 223 of the principal Act) which concerns the 'administration of public sector data'. The importance of its provisions can be judged from the DPC's statement to the Dail Select Committee on Social, Community and Family Affairs during its passage through the Oireachtas. He said that it was "no ordinary amendment to the Social Welfare Acts" but rather was "one of the keys to how the information society in Ireland in the 21st century will be implemented" and will "set the tone for how relations between Government and the governed, citizen and State are conducted in that century" (DPC, 1998: 46).

Its chief relevant provisions are as follows:

- A number may be issued to any person "who is the subject of any transaction with a specified body" (SWA, 1998: s14-1)
- The number must be given to public bodies where this is required for the "purposes of the person's transaction" (SWA, 1998: s14-1)
- A 'public service card' is to be issued with certain defined information either 'inscribed' or electronically encoded, "and with such other information either inscribed or electronically encoded on the card as may be prescribed" (SWA, 1998: s1-1). This card must be produced in transactions with public bodies.
- It is illegal to use, or to attempt to get somebody to produce a personal public service number or card except by a member of a public body in the course of a transaction.
- "A specified body holding information may share that information with another specified body who has a transaction with a natural person relating to a relevant purpose" (SWA, 1998: s 14-1) provided the information is relevant to the transaction.

As has been stated above the DPC had significant doubts about this legislation and urged that its provisions in section 14 be enacted in separate legislation to allow a public debate on the important issues involved. As a stopgap measure he proposed various amendments most of which were adopted (DPC, 1998). His chief worry was about the development of a de facto Personal Identification Number System (PINS) and national identity card. Concern about a de facto PINS was due to the fact that "PINS, in conjunction with automatic data processing, tend to increase the power of the administration" by excluding "the data subject from the information circuit" (DPC, 1998: 45). In this context he particularly suggested the removal of references to "Oifig an Ard Chlaraitheoir" (The General Registry Office) as it "may have everything to do with the creation of a National Population Register and a National Identity Number System" (DPC, 1998: 48). This amendment was not made, however.

The Act thus enacts certain provisions of the Report, namely the use of the RSI number (renamed the Personal Public Service Number) by the civil service as an identifier, data sharing between organisations and the wider use of the public service card. However, the full recommendations of the report are not implemented although there is potential for the Act to allow the development of a PINS. Thus there is no photograph on the public service card, the public service number is only issued in relation to transactions (which are defined financially) and thus not at birth, and the sharing of data is circumscribed by the necessity that it only be done when relevant to a transaction.

## Other Initiatives with Data Protection Implications

In addition to the provisions of the Social Welfare Act (1998) two initiatives in 1999 also have potential data protection implications. These are the Finance Act (1999) and the introduction of Multi-Agency checkpoints. The former empowers the Revenue Commissioners to "access the bank accounts of named individuals where there is reason to believe that the financial institution possesses information which would be relevant in calculating the individual's tax liability" (Faughan, 1999). This can be done "on foot of a signature of one of the three Revenue Commissioners - whereas formerly this had to be done on foot of a High Court Order or an appeal commissioner", with the nature of the necessary evidence to justify the action being left to the Revenue Commissioners, Mr. Dermot Quigley, (speaking on the *News at One* - RTÉ Radio One: 12 February, 1999) there is "no question of a trawl" of ordinary taxpayers accounts: access will only be to specific accounts in named banks, and the individual will be given "reasonable notice".

The introduction of Multi-Agency Checkpoints announced in February 1999 provides for the setting up of checkpoints to eliminate fraud. These are manned by Gardai together with members of Social Welfare, Revenue and Customs. When cars are stopped by the Gardai to check road tax, insurance and other vehicle related issues, the members of other agencies then check the individual's information in hand held computer consoles for the purposes of ascertaining inconsistencies (The Irish Times, 1999d).

# 5.3.4 Irish Implementation of EU Directive 95/46/EC

The most significant recent development in regard to Irish data protection was the issue of 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" on October 24 1995 (EU Parliament and Council,

1995). This provided for the compliance of member states with its terms "at the latest at the end of a period of three years from the date of its adoption" (Article 32-1). However, Ireland has yet to implement the provisions of the Directive although "the Bill is imminent" (Office of the Data Protection Commissioner, 1999).

The Directive grew directly out of the1981 Council of Europe Convention on Data Protection that gave rise to the Data Protection Act, 1988. In recital 1 of the Directive it is made clear that its objectives include "promoting democracy on the basis of the fundamental rights recognised in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms" (Recital 1). Due to the origins of both the Directive and DPA (1988) in the same Convention most of the provisions in the Directive "either match or are at least very similar to provisions in our existing law", although it does contain "some totally novel provisions" (Dept. of Justice, Equality and Law Reform, 1997: 5).

Of these 'novel provisions' the most important are:

- A three tier system of registration (Art. 18)
- The extension of protection to personal data in manual form (Recital 27)
- "New and detailed rules relating to transfers of data to countries other than the EU Member States" in Articles 25 and 26(Justice, 1997: 42).
- An obligation on the controller "to prevent personal data from being stored or used for hidden purposes" (Justice, 1997: 17) under Art. 6.
- Explicit statement of the information the data subject should receive (Art. 10 & 11)
- The processing<sup>8</sup> operations themselves will be publicised (Art. 21)
- Additional rights for the data subject in terms of access, and of "blocking" (Justice, 1997: 30) under Article 12.
- The ban, subject to certain qualifications, of automated decision-making which has an effect on a data subject (Art. 15).

<sup>&</sup>lt;sup>8</sup> Processing is defined as "any operation or set of operations which is performed upon personal data" and includes "collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction" (Art. 2(b))

- The setting out of "criteria for making data processing legitimate" (Art. 7), and additional regulations in regard to sensitive data (Art. 8).
- The extension of the right to object to data processing beyond merely the use of data for direct marketing provided in the 1988 Act (Art. 14).
- An obligation for appropriate security which is to be maintained by contract if processing is not done 'in-house' (Art. 17).

Purpose of processing

The major changes to the operation of data protection in Ireland under the Directive will thus involve changes in the nature of the register, enhanced subject rights and duties of controllers, and the extension of data protection to manual data. The extension of protection to manual records is not, however, automatic: such records must be held in organised filing systems. In addition there is a twelve-year delay before all of the provisions of the Directive come into operation in regard to manual data. Although the provision for manual data is not directly relevant the other issues deserve to be outlined in slightly greater detail.

Ireland currently has a system of two-tier registration that involves registration and nonregistration only. By contrast the Directive provides under Articles 18 to 20 for a system of three levels of "notification" of the supervisory authority. The levels of notification are as follows:

- Automatic notification in cases of automated data processing with optional simplification of (or even exemption from) such notification by the Member State if:
  - Processing will not have a negative impact on the subject (provided such processing is specified in terms of purpose, the categories of data, the type of subject, the recipients and the retention period);
  - The controller appoints an official with responsibility for independently ensuring the application of the law and keeping a register of processing activities;
  - Processing only relates to the provision of a public register;
  - Processing is conducted by a non-profit organisation of information relating to its members (as defined under Art 8-2 d).
- Notification of types of data processing likely to "present specific risks to the rights and freedoms of data subjects" (Art. 20-1). Such operations must be checked before they

commence either by the supervisory authority, or by the independent data protection official within the organisation.

The precise information required for notifications is set out in Article 19 of the Convention. Any notification must include a minimum of the following information:

- Name and address of controller
- Purpose of processing
- Categories of subject and of the data
- Recipients of the information
- Proposed third country transfers
- Description of the measures being taken to ensure security of processing

In regard to subject rights some of the most important changes are in the explicit definition of such things as 'fair obtaining' which also requires that personal data are not "being stored or used for hidden purposes" (Justice, 1997: 17). The current DPA neither set out conditions of fair obtaining, nor did it "expressly interpret the meaning of 'fair'" (Justice, 1997: 24). Articles 10, 11<sup>9</sup> and 12 set out the information which must be communicated to the data subject:

- Identity of the data controller
- Purposes of the collection of the data (i.e. the purposes of processing)
- Where it is necessary "to guarantee fair processing in respect of the data subject" (Art. 10(c) the following must also be given:
  - Identity of the recipients of the data
  - The information that a right of access, and of rectification exists
  - In the case of collection from the subject the subject must be informed whether a reply is compulsory, and of the consequences of unwillingness to provide the information
  - In the case of data acquired from source than the subject s/he must be informed of the data categories being collected.
  - "Communication to him in intelligible form of the data undergoing processing and of any available information as to their source" (Art. 12 a)

<sup>9</sup> Article 10 pertains when data are collected directly from the subject; Article 11 pertains when the data are otherwise obtained

• Knowledge of the "logic involved in any automatic processing of data... in the case of .. automated decisions" (Art. 12 a)

Article 12 also provides a further right to "rectification, erasure or blocking of data" which is inaccurate or which it would be wrong to process. Any third party recipients of such data must be informed of the alteration, erasure or blocking (Art. 12 a). This provision adds 'blocking', a concept borrowed from German data protection law, to the already existing rights to correction and erasure. This means that the controller can store data, but not used or processed, and blocked data must be clearly marked (Justice, 1997: 30). In addition the requirement to inform third parties having is changed. The requirement under the DPA to is to inform all those who received the data within one year of these changes; under the Directive this must be carried out without any time limit, unless this "proves impossible or.. involves disproportionate effort" (Art. 12 c).

Other extensions of the subject rights involve certain limited situations. Article 14 provides the right to object to processing for direct marketing purposes as in the 1988 Act, and also the right to object "on compelling legitimate grounds relating to his particular situation" in the case of certain types of processing (Art. 14 a). Article 14 also grants the individual a right "not to be subject to a decision which ..... significantly affects him and which is based solely on automated processing of data" to evaluate personal characteristics, including creditworthiness, unless it is legally necessary.

The Directive significantly enhances the protections afforded to Irish citizens over those of the, 1988 Act as well as forcing even greater openness on the part of data controllers and processors. The chief advantages directly conferred on the individual are greater rights to information on the data held both when it is collected and later, the new right to block data, the right to be free of automated decision making, the right to object to certain forms of processing. Additionally the explicit stating of the conditions necessary to make processing legal as well as the extension of protection to files which are not held digitally substantially enhance individual rights. Extending the requirement to register and the explicit protection of information in the case of transfer to non-EU jurisdictions also adds significant protections for the individual. In the former case this is due to increased openness and transparency that allows the individual to examine what is happening, and in the latter because it ensures the

individual some protection in an era when massive quantities of information can be transferred across borders easily.

Given the benefits which accrue to the individual the failure of the Irish government to implement the provisions of the Directive into law has worrying implications. This is particularly the case given the fact that the provisions of the Directive will not come into effect for "processing already under way" (Art. 32-2) for three years. In addition, manually held data is exempt for a total of twelve years from that date from some of the most important provisions of the Directive, namely those relating to data quality, legitimate processing and special categories of information.

### 5.4 Conclusions

The protection of privacy in Ireland is limited. Privacy is not clearly defined as a right in the Irish constitution though some limited protections of privacy exist through an implied right. Similarly legislation and court precedents provide only weak and fragmented protection of certain limited aspects of the right to privacy. In regard to the general right to privacy there are two positive factors that may alter this situation in the coming years:

- Ireland's obligations under international treaties at European and UN level provide that the state must guarantee a right to privacy
- The Law Reform Commission as part of its mission statement is concerned with the right of privacy, which it regards as a fundamental human right deserving of protection, and has already issued a report on the law relating to surveillance and interception of communication (LRC, 1998).

These may in time lead to comprehensive privacy legislation covering all of the four aspects of privacy as described by the Law Reform Commission (1996a, 1998).

In relation to the specific issue of 'privacy in the informational context' the LRC states that Ireland does not have any "overall protection of private information.....at present"; instead there is "some piecemeal protection for personal information" (LRC, 1998: 9). This piecemeal protection includes the Data Protection Act and Freedom Act and arguably to a limited degree the flawed Criminal Damage Act. The mainstay of information privacy in the context of this study is data protection legislation in combination with freedom of information legislation, which reinforces the provisions of the former with regard to public sector data.

Current data protection legislation is based on a number of principles that set out the philosophy behind data protection and form the basis of the various rights it imposes. It has been in successful operation for over ten years. The rights and duties for data protection are enhanced under the terms of the EU Directive on Data Protection, the provisions of which are due for "imminent" introduction to the Oireachtas in Bill form (Office of the Data Protection Commissioner, 1999).

Although there is a comprehensive Data Protection Act, thus, comparable to any similar legislation in Europe, and although the Directive is due for imminent enactment, some important problems remain with privacy law in Ireland even in regard to data protection. In regard to privacy in a general sense protection is still inadequate according to the LRC and without the introduction of new legislation any improvement must come from case law. However, "case law depends to a considerable extent on the involvement of persons who can afford to bring (or defend) cases" and is thus not a sure way of extending protection (LRC, 1998: 8). According to the LRC, therefore, the immediate enactment of legislation to protect privacy is necessary, particularly as "the right of privacy is under and actual and present threat" (LRC, 1998: 8). One benefit of such a law or law would be the provision of clear legal context for any litigation regarding new unanticipated threats to privacy which can be anticipated in an era of rapid technological change.

In regard specifically to data protection a number of concerns must also be raised. Although the legislation is comprehensive its existence in a country with poor protection of privacy is clearly due to its international origins and value to commercial interests rather than concerns for privacy. This view seems to be reinforced by the failure to implement new data protection legislation, now a year overdue, and by the efforts of the civil service to undermine the most fundamental principles of data protection outlined in the ISSS Report, and, to some degree, implemented in the Social Welfare Act (1998). In view of the fundamental importance of privacy discussed in Chapter Three, and the value of information in the exercise of power discussed in Chapter Four, the absence of a clear sense of commitment to privacy and data protection is worrying.

### **Chapter Six**

.2.1 Aims

# **Methodological Issues**

doing it was tell that the best possible approach to take was to look at the situation in regard to organisations with large databases of personal CI on the period is call. The internor of the merview procedure was to determine the organisation's treatment of personal information as a such issues as access to data security of data and quality of data. The issues 6.1 Introduction

The theoretical and legal literature clearly shows the importance of privacy as an enabling right in a complex democratic society, and its importance in the exercise of freedom. However, technological advances have changed the context of privacy. It is now possible, using Information Technology, to effectively place somebody under surveillance through the use of personal data. One such category of data that possesses considerable potential to infringe privacy is Geographical Information. Modern developments in the technology of GI manipulation have made such actions even easier.

For this reason it was decided that a study of the issue of privacy and GI in Ireland at present would be of particular value. This involved two separate parts. The first, a literature and statute study, concerned the protection afforded to the right of privacy in Ireland with particular emphasis on those laws protecting privacy in the information context. This study formed the basis of Chapter Five. The second part of the project took the form of a questionnaire survey, the methodology of which occupies the remainder of this chapter. This questionnaire survey was administered to representatives of organisations holding large-scale databases of personal information that possessed some geographic component.

### 6.2 Methodology of Questionnaire Survey

#### 6.2.1 Aims

The aim of the survey was to assess the state of privacy in regard to GI held in Ireland. In so doing it was felt that the best possible approach to take was to look at the situation in regard to organisations with large databases of personal GI, on the national scale. The intention of the interview procedure was to determine the organisation's treatment of personal information as regards such issues as access to data, security of data and quality of data. The issues addressed were largely informed by the data protection principles upon which the Irish DPA is based, since these form the basis of data protection in this country.

#### 6.2.2 Questionnaire Design

The initial step taken was to draw up a list of issues connected with the privacy and data protection of GI in Ireland, shown in Table 6.1. Of these issues the legal question in terms of the protection of privacy, and access to information, and also of the extent to which the law is up-to-date was dealt with through the study of the relevant legislation and commentary on such laws described in Chapter Five. Many of the other issues listed in Table 6.1, and in particular the technical issues, were, however, felt to be amenable to examination through the method of a survey.

### Table 6.1: Factors of Importance to Data Protection and Privacy

•	Legal safeguards	•	Type and amount of information
•	Data collection	•	System of input and update - safeguards
•	Nature of the database used	•	International dimension
•	Accessibility of data	•	Internet Linkage
•	Security of systems	•	Government power v. Private sector power

As a preliminary step to the creation of a questionnaire a diagram was drawn of the interaction between as many of these factors as were felt to be practically relevant to questionnaire design (see Figure 6.1).



Figure 6.1: Diagram of Interrelationships of Data Protection Issues

The main groupings of issues that emerged in constructing this diagram were:

- Database issues;
- Procedures of data collection;
- Input of data
- Update of data;
- Access to the data;
- Security of system;
- Compliance with the legislation regarding data protection.

It was felt that the questionnaire design should concentrate on eliciting answers of a descriptive nature. There were a number of reasons for this, namely the complexity of the subject area and the various interactions between the different factors that impact on privacy

and data protection. It was felt that such an 'open' format of questioning would enable the interviewees to volunteer information, and to draw parallels between different questions, and to link related issues. It was also hoped that such a format would enable the interviewees to express opinions about the importance to their organisation of the related issues of data protection, privacy, accuracy and security, rather than merely answering questions in a set format. An additional factor in deciding to design the questionnaire in this way was the necessity of facilitating the interviewees in answering the question. Since the intended study group was expected to be non-homogenous, a questionnaire open to interviewee input was deemed essential.

Accordingly a questionnaire was designed using the seven headings (outlined above) that were extracted from Figure 6.1 as an organising framework. The first draft of the questionnaire accordingly contained sixty-six questions in seven sections, arranged by theme. This embryo questionnaire went through a number of iterations each of which added questions to ensure that each section had a comprehensive coverage of its subject. At this stage of the process the questionnaire re-evaluated and radically overhauled. The resulting questionnaire, broadly similar to the final version, contained sixty-two questions in five sections (Input and Update were merged, as were Access and Security as they covered similar ground). The advice of an expert in questionnaire design and the conduct of surveys was then sought. Following the implementation of the advice received, the resulting questionnaire was piloted on three organisations, IRLOGI (the Irish Organisation for GIS), The Alumni and Senate Electoral Register of Trinity College, and Statoil Ireland (in relation to their loyalty scheme). This piloting process highlighted a number of issues regarding the phrasing of and the overlap between some questions, as well as the practical issues in administering the questionnaire. The questionnaire was altered to reflect these issues by the consolidation of questions, and the addition of explanatory notes for interviewees on others.

6.2.3 The Final Questionnaire

As already described the final questionnaire was divided into five sections of differing length based on the original diagram of privacy and data protection issues (Fig. 6.1). There was a

total of fifty question. The different sections are described below. The full Questionnaire is reproduced in Appendix Two.

# Section 1: Data and its Collection

1.1. (a) What categories of data are collected. (b) Are they stored under these headings? If no, can you give some examples?

1.2 Is there any method used to refer the data to space.

1.3 Do you have a sensitivity ranking for the data you hold. (as regards individual privacy) If yes can you describe it. If no, could you rank the categories you mentioned in Question 1.1 according to their sensitivity (high to low).

1.4. Do different individuals records ever get linked together. Please give some examples.

1.5. Please rank the five most important categories of information (in terms of analysis performed on the data).

1.6 Briefly describe the process by which the initial data are collected. Is there a form?

1.7 Could you give an example of the types of procedure used to check data quality and consistency.

1.8. What information audit trails are there.

1.9 If there are such materials kept, At which stages of the process of data input, update, manipulation does this occur.

-for how long are they kept, -and how are they disposed of.

Section One can largely be described as having two broad subsections. Questions 1.1 to 1.5 are concerned with the nature of the data themselves. The intention was to find out:

- What categories of information were sought and whether the same categories used in data collection were used in data storage;
- What precise category of data was used as a geographic indicator (if any);
- Which if any of these categories was regarded and treated as particularly sensitive;
- Whether each individual's record was individually stored (or whether they were linked, for example on the basis of family relationship);
- Which categories of information collected were most important in terms of the most commonly performed analyses of the data.
The second subsection (Questions 1.6 to 1.9) concerned the issues involved in the collection of data and the checking of data quality. This part of the questionnaire concerns the actual process of collection, quality control procedures and the maintenance of archives of backup and original information. The importance of the quality control issue is in regard to the data protection principle of accuracy and includes checking data consistency of data and that it has been input correctly. The maintenance of archives of information is important so that provenance of information can be checked in the event of alterations or changes to information.

#### Section 2: Data Input and Update.

2.1. What is the organisational structure in terms of data collection, input and update.

2.2 What training relevant personnel have.

a) What is the skill level when they start.

b) What if any training on the job do they receive.

2.3. Is data input and updated manually, automatically or both

2.4. Is there a documented procedure for data input and update. If not is there a standard working procedure (for input & update) in which employees are trained.

2.5. Outline its chief steps.

2.6. Are there any other safeguards to ensure accuracy at the input stage; at the update stage

2.7. What is the policy regarding update.

2.8 Is input entirely comprehensive or are some fields optional.

In Section Two data input and update were dealt with together to avoid redundancy and repetition. Following on the second part of Section One it is also concerned with the question of the accuracy of information.

Question 2.1 concerns the organisational makeup in terms of data input and update and seeks to ascertain issues such as the degree of spread of responsibility, the numbers of people involved and whether they are in contact with one another, and the context within which accuracy safeguards operate. Questions 2.2 to 2.7 are all concerned with the maintenance of accuracy of information from initial collection to input and update. In assessing this it was felt to be vital to examine the skills and training of employees, input and update procedures,

Questions 3.4 and 3.5 specifically address the use of GIS, and other spatial tools, if applicable. The final question of the section concerns the hardware specifications that relate to access. In effect the question relates to the whether the system is networked or not, and, if networked, the nature of access.

## Section 4: Access.

#### a) General

4.1. What technical security procedures (if any) are in operation. If passwords: What is the Policy on changing passwords?

4.2. What other non-technical or organisational procedures are there.

4.3. Who can access the information on the system. Are there any restrictions placed on access to any categories of information within this framework. If yes, which data items/categories are most commonly limited.

4.3 Are there different levels of access in terms off changing data.

4.5. What protections are there against deliberate falsification of information

by an employee, by an outsider (e.g. hacker), by the individual data subject. Within this context are there checks of informational consistency? Do changes of information outside of standard updates need outside verification.

The first two questions concerning general access relate to security procedures, both technical and organisational. Plainly these are two of the most basic questions when attempting to assess the issue of privacy in an information system. Protection of the system against unauthorised access is of concern to the institution concerned, as they will have a proprietary interest in their information. From the point of view of the person whose information is being held the issue is simply that of the protection of personal information from being accessed by an unauthorised individual, whether within or without the organisation.

The next questions relate directly to access. Question 4.3 concerns access to information in read-only terms (the ability to read information but not to alter it), and whether there are any limitations placed on such access. Question 4.4 concerns access to information in a 'write' capacity. Question 4.5 is again concerned with data quality, and the potential to falsify information. The question also concerns the issue of such falsification coming from a source

outside the organisation, whether a hacker or the data subject. There is a degree of redundancy in this question as the issues concerned are touched on in Section One and in the earlier questions in Section Four. Such redundancy was allowed to remain in the questionnaire to elicit further discussion in cases where issues had remained unclear due to the complexity of the topic.

#### b) Internal.

4.6. Is there a record of who accesses the data and the purpose for which it is accessed. If yes, How long is this record kept for.

4.7. What would be defined as unusual accessing of database. Are there procedures to check for this?4.8. Can data be downloaded to paper, disk, other systems (e.g. personal PC), or other media.

If yes, In what circumstances is this allowed. Is it permitted to remove such material from the premises. If yes, In what circumstances is this allowed. In either case, What safeguards against the unauthorised removal of such material by employees.

Once again there is some redundancy in this section as it deals with issues touched on in the section on general access. This was felt to be important, however in drawing out clarification of issues. Questions 4.6 and 4.7 concerns the issue of records of access to, and alteration of, the database being maintained, and any procedures to check for unusual access patterns. Question 4.8 relates to the issue of downloading of information from the system whether as hard or soft-copy, and the removal of such material.

c) External.

4.9. Are data services offered via the World Wide Web. If yes, At what Internet address.

4.10. If yes, What information do those services access and obtain.

4.11. What security procedures are in place for such services.

4.12 Is data ever shared with outside organisations. If yes, with what other organisations is information exchanged as a matter of course.

4.13. In what ways are such data exchanges carried out?

4.14. If there is networking to other institutions (banks for example), what measures are in place to secure this.

4.15 If there is networking to other institutions, what type of access does the person accessing the system remotely have.

4.16. Do staff have email accounts. If yes, Are these purely internal, or external. What protection of them is there (passwords, etc.).

4.17. If yes (to 4.16), To what extent are email accounts policed or monitored. Is there a company policy on this? If yes, outline it please?

4.18. If yes (to 4.16), Are email accounts transferable between employees.

4.19. Are there specific requirements to be met before information can be given out over the telephone in response to requests. If yes, please outline them.

4.20. Banks/Financial institutions (only): What security procedures for automated telephone banking are in place.

4.21 Government (only): With which other Government Departments / Semi-State bodies do you share information most commonly. Rank the top five.

Section Four (c) attempts to tackle the issue of access to information from outside the organisation whether through the Internet and other wider area networks, or through the sharing of information between organisations. The question of access to services through the Internet (Questions 4.9 - 4.11) is a new one and it was anticipated that few Irish organisations would have such services in place.

The sharing of information between organisations (Question 4.12 - 4.15) was felt to be unlikely in most cases although some sharing between government bodies was felt to be likely (in the context of the Social Welfare Act of 1998, for example). Question 4.12 concerns the organisations with which information is shared and Question 4.13 concerns the methods used in such data sharing or data transfers. Questions 4.14 and 4.15 deal with the issue of whether there is network access in the case of such sharing, and, if there is, the form it takes.

Questions 4.16 to 4.19 relate to the potential of information being distributed outside the organisation either by telephone or through the use of email facilities by staff. Question 4.20 relates to the issue of telephone transfer of information in relation to automated telephone banking using touch-tone phones, and the procedures for the protection of such transfers. Question 4.21 relates to the sharing of government sector data anticipated under the Social Welfare Act (1998) and other legislation.

## Section 5: Data Protection & Codes of Practise.

5.1 Is your organisation required to register under the terms of the Data Protection Act. 5.2. If yes, Have you registered.

5.3. Are there specific procedures in place to ensure compliance with DPA.

If yes, Please outline the main aspects of these procedures

5.4. How would you rate the impact of the Act on your organisation within the Irish context.

5.5. How would you rate the impact of the Act on your international activities (if relevant).

5.6. Does the organisation belong to a professional or other representative body. If yes, please specify.

The final part of the questionnaire concerns compliance with the terms of the Data Protection Act. Question 5.1 and 5.2 concern the requirement to register and whether registration has taken place. Question 5.3 deals with procedural issues implemented by organisations to ensure such compliance (such as the appointment of a Data Protection Officer, for example). Questions 5.4 and 5.5 are related to the issue of the impact of Data Protection legislation the activities of an organisation both within the country and outside (if relevant). The final question relating to professional bodies was included due to the provision in the Irish DPA for the drawing up of Data Protection Codes of Practise by such bodies.

#### 6.2.5 Selection of the Study Sample

As the aim of the study was to study the issue of privacy in regard to public and private sector organisations holding large scale databases a list of such organisations was drawn up as potential interviewees. This list included government agencies, local government bodies, financial institutions, insurance companies, direct marketing organisations, credit referencing organisations, loyalty club scheme operators, and some medical organisations. A key factor in creating this list was the likelihood that the organisation in question would possess a database that would be national in scale, or very near to that. Thus the Dublin local authorities and the Eastern Health Board were included in the study as overall the greater Dublin area contains one third of the state's population.

This initial list (see Appendix Three) was then prioritised so that those organisations that were felt to be most important to the study's aims were placed at the top of the list. These organisations were then contacted in the order they appeared in on the list to arrange interviews during May and June of 1998. There followed a process of telephoning organisations to get the name of an individual responsible for the information system itself, or for data protection. The telephone contact was then followed by a letter explaining the nature and purpose of the study and requesting an interview. A sample of the basic letter template used is available in Appendix Four.

#### **Revenue** Commissioners

During this process the original prioritised list had to be revised in light of a number of factors:

- Ireland has only one credit referencing agency dealing in personal (as opposed to business) credit references;
- The number of direct marketing bodies that actually maintain databases of individuals is very small as the other organisations lease or buy the main lists.

Accordingly there were far fewer such organisations than originally anticipated. Following a lengthy period of contacts and attempted contacts a total of thirty organisations proved willing to co-operate with the study. The interviews were conducted between May and July of 1998.

The composition of the study group is outlined in Table 6.2. As can be seen government and financial institutions predominate with the others including representatives of the health, direct marketing, and credit referencing agencies, as well as semi-state bodies.

## Table 6.2: Final Interviewees

**AIB Bank** 

National Irish Bank Irish Permanent EBS Building Society First National Building Society Dept. of Education Irish Nationwide Building Society Revenue Commissioners Social Welfare Gardai Siochana Ordnance Survey Ireland Central Statistics Office Land Registry Dept of Health - GMS Board Dept of Agriculture

## ACC Bank

Dublin Corporation Fingal County Council Dun Laoighre County Council South Dublin County Council ESB Telecom Eireann Irish Life Eastern Health Board IRIS Bill Moss & Associates Precision Marketing Information Ltd Irish Credit Bureau St. James Hospital Family Album

The questionnaire was administered in an interview. This was felt to be necessary to facilitate explanation and discussion of the questionnaire, and the recording of the contextual comments of the interviewees. The complex nature of the subject matter of the questionnaire, and the necessity of structuring it so that a wide variety of organisations could be interviewed made the questionnaire quite complex. Thus it was felt to necessitate such an opportunity for explanation in the case of confusion about the meaning of questions.

In some cases, particularly in the Civil Service bodies with extremely large databases a number of people participated in the interview. This was the case in Revenue, Social Welfare and the Central Statistics Office. The interviews generally lasted for between thirty and forty-five minutes. In some cases, however, the complexity of the information systems and the volumes of information stored led to longer interviews.

## 6.3 Conclusions

In order to study the practical organisational aspect of privacy and data protection in Ireland with respect to digitally held GI, it was decided to conduct a questionnaire survey. The questionnaire was designed bearing in mind the data protection principles and the interaction of factors shown in Figure 6.1. The questionnaire design also reflected the need to administer it to both government and private sector organisations. The necessity to be applicable to organisations with quite different computer systems and internal organisational structures, as well as the complexity of the subject matter (reflected in Figure 6.1), meant that the questionnaire needed to be quite long and complex in order to be comprehensive. It was accordingly decided that the best method of survey involved face-to-face interviews that would facilitate the explanation of any question that caused difficulty. It was also felt that such a face to face interview would allow the interviewee to express opinions and add contextual information to any answer.

Accordingly the questionnaire was administered to a study group of thirty public and private sector organisations that held personal GI of some kind. The survey involved the detailed examination of the information such organisations held, their treatment and use of it, and their methods of protecting such information to ensure that it was not compromised, as well as seeking information on their attitudes to the Data Protection Act (1988). Chapters Seven and Eight will reveal and discuss the results of this survey.



## 7.1 The GI Industry in Ireland

The GI community in Ireland is small compared to that in Britain and has only achieved organised representation on a national level much more recently. Prior to 1995 the only organisations that approximated this function were Eirgis, a small, private sector user group, and the Inter-Departmental Working Group on GIS in government. In 1995 IRLOGI (The Irish Organisation for Geographic Information) was set up following an approach from EUROGI (European Umbrella Organisation for Geographic Information) requesting that an organisation be set up to represent the Irish GI community in Europe (Cox, 1998). Table 7.1 outlines IRLOGI's Mission Statement.

## Table 7.1: The Mission Statement of IRLOGI.

#### **Mission:**

To represent the Irish GI community and to stimulate the development and effective use of Geographic Information in Ireland.

#### **Objectives:**

Be the focus for the collection, exchange and dissemination of geographic information
Encourage the development and adoption of quality and reliability standards for GI
Represent the interests of the Irish GI community nationally and internationally
Encourage and support education and training in GI

(source: http://www.irlogi.ie/aims.html)

Traditionally there have been three main emphases in Irish GI:

- Environmental analysis and monitoring;
- Facilities management;
- Government GI use.

In recent years, however, there has been a considerable growth in the use of socioeconomic GI. Such use of personal GI is chiefly in geodemographics and marketing applications. Effectively the Irish GI community is in transition as this sector continues to grow in size and importance (Ovington, 1999). This change is reflected in the inclusion of marketing applications of GI in IRLOGI's GIS Ireland 98 Conference, which sought to cater to the growing interest in the potential of GI for such use.

As has already been mentioned in Chapters One and Two this growth in the use of personal GI has been facilitated by a number of new developments both in the technology of GI manipulation, and in the context of Irish GI data and metadata. The national launch of the OSI/An Post GeoDirectory, and the existence of similar private sector products for the large cities, is of great importance to the GI community. One of its chief effects will be in the facilitation of the use of GI collected with an address attached for sophisticated spatial analysis. In effect this means that when the GeoDirectory is fully complete (December 1999) any personal information that includes an address can be considered to be GI for the purposes of digital spatial analysis. This will vastly increase the amount of spatial analysis possible and facilitate the growing interest in the use of socio-economic and personal data. It is against this background of a changing Irish GI community, and the launch of products that enable the use of address-linked personal information as GI, that the results of the survey must be considered.

## 7.2 Data Collection

The section on data collection covers a number of issues fundamental to the question of privacy of information regarding the person. Perhaps the most fundamental issue is that of the actual information being collected. While this is obviously largely a question which depends on the operations of the organisation in question, certain items of information are widely sought.

The most often collected categories were address (thirty), name (collected in twenty-nine cases but only entered into the system in twenty-eight), a reference number, date of birth or age (thirteen), and the PPS number (ten). Of the less universally required categories of information details of a person's occupation (ten), income (ten), family relationships (ten), telephone number (six) and medical details (six) were of the greatest significance. Other

categories specifically mentioned included sex, religion, home/property ownership, insurance details and other financial details. In a majority of cases the collection of the less common categories of information coincided with particular organisation-types. Thus financial institutions tended to collect information on financial transactions, utilities on supply-related issues, local authorities on issues such as rent relief, and central government information relating to service provision.

The second part of this question asked whether the information collected was stored in the same form in which it was collected, given the possibility of using information for purposes other than those which are obvious to the subject, such as the generation of credit scores or marketing categories from other data. Only four organisations stated that they stored data under other headings. Of these four two derived a credit score from the other information, one "occasionally creates new categories for the purposes of marketing", and one uses the basic information to derive other information such as relationships between people through software algorithms.

Question 1.2 related directly to whether the information collected could be considered GI. All of the respondents had some method of linkage to space. However, some respondents replied in the negative when asked despite having already listed address as a data category. This seemed to indicate a lack of awareness of the potential use of address-linked data as GI. The breakdown of the results was as follows:

- All thirty organisations collected the address but only twenty-nine entered it on the database;
- Nineteen of these used the address exclusively, five used the address and area codes together, and three used it in combination with such codes and National Grid co-ordinate references;
- Only one organisation used area codes exclusively and two used grid referencing alone.

Of those using area coding the majority were using CSO level boundaries. The purpose of the use of these areas was generally the linking of CSO statistics to their own information for analysis purposes.

The question of sensitivity of data proved quite complex. The majority of organisations did not have such a sensitivity ranking (twenty), while one third did. Of the ten that did the basis of the sensitivity was not always privacy of the individual:

- Three stated that they accorded a high degree of sensitivity to all personal data;
- Two ranked data on a customer rather than a data category basis so that certain individuals' records were more sensitive than others;
- Two had a ranking based on sensitive operations (all data used in those operations was highly sensitive regardless of category);
- The remaining three, one had sensitive data while the other two treated all data items equally, but all stated that access was on a need to know basis.

It emerged from the discussions, however, that the data categories most likely to be treated as sensitive by these organisations were financial and health information, two of the most highly sensitive to the Irish public according to the DPC (1998).

Of those who did not have a sensitivity-ranking and who were asked to rank their data, fourteen felt that all categories were of equal sensitivity. Of these, three specified, however, that access to all information was on a need to know basis, indicating clearly the link between this question and Questions 4.3 and 4.4. In two cases the issue was felt to be inapplicable due to the fact that none of the data were particularly sensitive. The remaining four cases specified that "financial details and name are most sensitive followed by address", "information covered by the DPA was most sensitive", "telephone numbers were most sensitive", and "the least sensitive were occupation and former addresses and all others were highly sensitive, respectively.

The linking of data on different individuals within a database was practised by fifteen of the organisations, with a further fourteen not doing so and one organisation to which the question was not applicable. Of the fourteen that did not link data in this way two had plans to do so in the near future. Where linkages were formed almost all were on the basis of family relationship, or the sharing of an address: "family nucleus", "households", "living together" being typical reasons for such linkage.

Question 1.5 involved the ranking of data items collected (from Question 1.1) in order of their importance to the organisation with respect to data analysis and manipulation. In this regard the address proved to the most important category of data, being highly ranked in twenty cases. This was followed in turn by Subject Name, including forename and surname, (eighteen cases), Unique Reference Number (nine cases), Date of Birth (eight cases), and 'Other' (seven cases). Other categories such as financial details and the

Personal Public Service Number were also raised by some organisations but were clearly of concern only to certain organisations. The clear importance of the address, in advance even of subject name in the analysis of personal information clearly shows the importance of the geographic component even in the case of organisations not using GIS.

#### On the spot checks at the home of the subject

Regarding the collection of information the vast majority of organisations collected initial information from the individual in person. This was the case in twenty-six instances, the majority of which were cases of the individual making an application to the organisation and thus filling out a form. Only one organisation used 'surveys exclusively', while seven obtained data from other organisations, two of them exclusively so. Three organisations specified other data sources (one of them as the unique source), namely maps, the electoral roll and other analogue sources.

On the issue of procedures used to check data quality and consistency a wide variety of methods is in place. A number of organisations indicated that the maintenance of quality data is one of the most important issues for them and that the rapid falling off in data quality over time is a serious problem. Fifteen organisations said that the individual data subject was the primary source of such information. In such cases checking with the individual in person at the point of contact was the primary method, with additional contacts being used as an opportunity to find out about any change in circumstances. A small number of respondents indicated that they ultimately "take it on trust" and "accept what [they] are told". The next most important method of checking was the use of software data validation methods (fourteen responses). Such methods ensure that the data integrity criteria of that organisation are met when the data are entered into the system. Typically information that does not fit these criteria is 'flagged' for further examination and in certain cases the whole process of data input is prevented if the difficulty is sufficiently serious. The next most significant forms of checking are checking by another person within the organisation (in the case of sensitive information or of a problem being thrown up by validation software or some other method), mentioned six times, and documentation checks, mentioned eight times.

Other important methods used by organisations in this search for data quality and consistency included:

- The use of double-punching of keyboards, where the same key must be punched twice before it is registered, at data entry
- On the spot checks at the home of the subject
- Double-checking with other agencies
- Audits and checks of the internal consistency or possible duplication of data
- The use of a rating system which ascribes a degree of reliability to each item of information depending on its source and other factors.
- The duplication of all data collection by two separate data collection units with only the information agreed by both being used (used by only one organisation)

In regard to the question of audit trails (Question 1.7) it was found that all organisations placed a very high degree of importance on the possession of such material for the purposes of checking the source of any mistakes, and to enable double-checking in the case of any dispute. Many of the methods used to keep such "paper trails" are legislation driven since for many organisations there are statutory requirements regarding the maintenance of records, the nature of such records, and the duration for which they must be kept. The forthcoming implementation of the European Directive will also have an impact on this material as it extends the data protection principles, and thus subject rights of access and correction to such material.

In terms of the form of maintenance of audit material almost all organisations preserved both manual and digital data, with only one organisation having no such material since their data was supplied from outside and is not changed until fully replaced. The analogue data stored generally consisted of at least the original documentation, and often also further documentation relating to subsequent changes to the database. Some organisations transferred the original documents to microfilm, or to the digital medium by scanning, after a number of years to save on physical storage space. Twenty-four of the organisations preserved both analogue and digital backups, one preserved only analogue backups and a further four preserved only digital backups. These four included two organisations that received their information from outside sources, one which sourced information in other documentation, and one other. Of the twenty-nine organisations to which Question 1.9 was applicable, a great variety of methods of preserving such material was found. Organisation's digital backups were generally done for technical reasons, as a safeguard in case of computer system failure, and thus logic dictated that they were done on a time basis rather than on the basis of the stage of data manipulation. Depending on the importance and changability of the database organisations backed up data on a time scale varying from twice daily to weekly, with a daily backup being most common. These backup materials were then kept for a varying time period before eventually being "purged and overwritten" or merely overwritten. It is important to stress, however, that the maintenance of such material is in most cases merely as a technical safeguard to ensure against the loss of material on the database rather than as audit material in the sense intended by the question. For the purpose of audit most systems were incremental in nature, building up gradually and storing up initial information and adding to it. The majority also had systems in place to register the changes made and the personnel who made them as a comprehensive digital auditing process (see Questions 4.6, 4.7, 4.8).

In regard to the paper records a different regime was in place. In all twenty-three of the twenty-five organisations preserved paper records at input, and twenty-one at update stages. Only eight of the twenty-four directly claimed to maintain records of manipulations in analogue form. In general such material was kept for a number of years, with the shortest-term preservation exceeding one year. A more detailed breakdown is available in Table 7.2 below.

Table 7.2: The Retention of Analogue Documentation		
Retained for an indefinite period	6	
Indefinite Time/Specified No. Years	3 ons 4.3 and 4.4 deal	
One year, then microfilm/scan	2	
1-7 years	3	
7 years	5	
More than 7 years-indefinite	2	
For a certain number of years after end of association	2	

Table 7.2: The Retention of Analogue Documentation

As can be seen from this most organisations have a strong policy of retaining original documents or copies thereof for substantial periods of time. The vast majority of the organisations which maintain such paper trails maintain them for at least seven years, with

a very substantial proportion maintaining at least some documents indefinitely. When it came to disposal of these materials fifteen of the nineteen relevant organisations used shredding, deep burial, or 'secure disposal' (generally on contract to professional organisations). Four organisation representatives were unsure of the method of disposal though felt it would be secure, and one organisation used deep burial.

## 7.3 Data Input and Update

In relation to the issue of data input and update the first question sought to determine the relationship between organisational structure and the processes linking data collection, its input and update. The importance of this question is central to the issues involved in privacy since it determines both the number of people who are exposed to information on any given individual. It also has a bearing on the quality of data: it is better for example if more than one person is responsible since this allows checking of data, as well as making any misuse of or corruption of data difficult for any given individual. The results of this question showed that all of the options suggested to interviewees were of relevance, though certain ones proved more important. The three most important were "same department, different units" with six cases, "different departments, same organisation" which had eight, and "any employee" (seven cases). Most organisations did not draw any distinction between "same department, different units" and "different departments, same organisation", however, and so these results may safely be read as one category. In addition, the "any employee" category, where selected was invariably qualified by "job description" or "need to know" status. In effect this means that although every employee potentially has access, in reality only those who need to do (Questions 4.3 and 4.4 deal specifically with the question of authorisation to access and alter data). In effect this means that this category is also linked to the previous two. This would mean that data were available to people in different sections of the overall organisation in twenty-one Many organisations answered this question by agreeing to a number of the cases. possibilities but as they are hierarchical only the 'top' one is counted for Table 7.3 below. Thus, for example, where "same person", "same unit", and "same department" were all listed, only same department is used as it implies the other categories.

#### Table 7.3: Responses to Question 2.1

Same Person	E 3GHLIKL
Same Unit/Room	3
Same Department, Different Unit	6
Different Department, Same Organisation	8
Any Employee	U 7.M.N.O.P
Outside Agency (with In-House Update)	3
Other Other	G. LK.L.N.O.P. 2

Question 2.2 had two parts which related to the skill of employees at entry level and more importantly the training they received on the job to enable them to deal with personal information. Part (a) of the question concerned the general entry-level skill and the majority of respondents revealed that their entrants' minimum skill level was low- or non-skilled. Twelve of the organisations specified that they had no necessary skills, and a further fifteen that they expected keyboard skills and/or low-level computer knowledge. In one case the question was inapplicable since data was acquired from outside and not altered, and in a further two cases the organisations selected "other" as an option. In these cases the "other" referred to:

- A variety of skills pertinent to that sort of organisation (in the Civil Service) but not computer skills;
- The leaving certificate (meaning that this effectively belongs under "no necessary skills").

It is important to note that these were the minimum requirements of those that would be entering an organisation, and potentially involved in the manipulation of information. All organisations stressed that they received a variety of levels of qualification in their entrants, depending in part on the level at which they entered the company.

Section (b) of this question was in the more significant of the two since it concerned the training received by employees to enable them to deal with personal information. As Table 7.4 illustrates the answers to this question paint quite a complex picture. Each individual organisation is represented by a separate letter (or combination such as AA, AB) of the alphabet.

Software Specific Training Course	A, B,C,D,E,F,G,H,I,J,K,L	12
Data Handling Training	H,L,M	3 the docu
Informal Training from Predecessor/Colleague	A,B,C,D,I,K,L,M,N,O,P	11 <sup>°S Procee</sup>
Other Formal Training	B,C,D,E,G,H,K,L,N,O,P, Q,R,S,T,U,V,W,X,Y,Z	21 sic desci
Other	a their organisations. The vast	mejority of c
All/Most of Above	B,C,H,L,AA,AB,AC	7
Not Applicable	put could not proceed. The SO	<sup>1</sup> was therefo

Table 7.4: Responses to Question 2.2 (b)

Since the possible answers are not at all mutually exclusive, nor do they form some sort of continuum it is impossible to describe the trends revealed as simply as in part (a) which allowed for the selection of the minimum entry requirements. The most commonly chosen options were:

- "Other formal training" (twenty-four);
- "Software specific training course" (fifteen);
- "Informal training from predecessor/colleague" (fourteen).

With the exception of "other formal training" the vast majority of responses are to multiple categories, whereas in this category only fourteen of the twenty-four had also responded to other categories. The organisations that responded that they had "other formal training" had, in the majority of cases, in-house training courses to familiarise workers with their duties and the systems and techniques used. In addition many of these organisations also had a policy of encouraging their employees to acquire other formal qualifications from educational and training institutions, with promotion-prospects being enhanced thereby.

In regard to data input ten had purely manual input of information, only one had totally automatic input, while nineteen had a mixture of both types. In regard to manual input this was generally keyed in from applications, while automatic data input comprised a number of different methods including the use of magnetic cards and the manual input of information into handheld units from which it is directly downloaded onto the system. Questions 2.4 and 2.5 concerned the issue of whether there was some sort of Standard Operating Procedure (whether documented or not), and whether it was possible to find out some details of it. Of the thirty organisations concerned all but four had a documented procedure for data input and update although not surprisingly the documentation was generally confidential. These four all did have Standard Working Procedures that were undocumented according to Question 2.5. While the documentation and the specific procedures were confidential, many organisations did give basic descriptions of the methods used as standard within their organisations. The vast majority of cases had screen driven procedures. When inputting or updating data, therefore, the form filled the screen and once filled in appropriately this would lead on to another screen. If details were entered in an invalid fashion input could not proceed. The SOP was therefore in-built into the actual system, which would not allow it to be violated. whereby each screen successively led one through and imposed the SOP. Seventeen organisations specified this as the mainstay of their SOP. Other methods of enforcing the SOP were "procedures in which people are trained", "software validation systems are in place" and "clerical procedures are set out at all levels".

One organisation raised the issue of address standardisation in this regard. As has been discussed Ireland lacks a national standardised address system, although the An Post/OSI GeoDirectory initiative can be expected to alter this. The organisation that raised the issue found that this lack seriously undermined one aspect of their SOP. As there existed no standard nationally, data had to be entered using the non-standard addresses that were supplied. Although the organisation collected data in numerous contexts, often in relation to the same address, there was no possibility of linking the information using the address and this was felt to seriously undermine the usefulness their analysis and manipulation of personal information. In this context delays in the production of the GeoDirectory were severely criticised.

In regard to Question 2.6 twenty-six of the thirty organisations specified that they had techniques for the checking of accuracy of information during input and update. This has considerable overlap with the previous question since the main SOP mentioned there was the use of screen-driven data input methods. This is the first line of safeguards since it prevents information being entered fully unless it complies with data standards.

Other methods used include the following:

- checking of data by another person, often a supervisor (fifteen cases);
- internal audits and data validation checks (six cases);
- audits alone (two cases);
- validation without audit (four cases);
- 'Other' (four cases).

In any given organisation more than one method was generally in use, a combination of screen-driven input with data validation, for example.

Finally Question 2.7 was designed to determine the frequency of update of information since this is vital to the whole issue of data protection. The value of information decreases rapidly as it goes out of date, and it also becomes potentially damaging to the individual to have information that is not up to date being used. The results were as follows:

- One 'informal, incomplete';
- Six 'optional update', usually customer driven;
- Three 'regular optional' updates;
- Fifteen 'regular obligatory' updates (four 'incomplete', ten 'complete' and one 'either');
- Three 'other';
- One 'not applicable'.

In regard to the second part of the question only nine organisations said that all fields of data were compulsory and needed to be filled. The remaining twenty (one organisation did not have update at all but merely replaced the entire database) said that this was not the case though for the majority of these some were mandatory, while some were optional.

## 7.4 Nature of Data Storage and Analysis Medium

The first two questions of this section concern the nature of the system used to store and analyse data. Question 3.1 asks whether the main system (many of the organisations because of their organisational complexity used more than one system) is an off-the-shelf piece of software, or one which was designed specifically to meet the needs of the organisation. While the division between the two was roughly fifty-fifty this is actually a little deceptive as only three organisations reported that their system was off-the-shelf without adding that it had been modified in-house to meet the needs of their organisation. The result was a three way split between those which were purely off the shelf (three), those which were customised off the shelf (thirteen), and those which were designed to meet organisational requirements (sixteen). Of this latter group some were based on offthe-shelf programs. The most commonly named off-the-shelf systems were Oracle and MS Access, although overall a wide variety of systems were in use, some of which were quite old.

The second question elicited a bit more detail concerning the precise nature of the data storage medium. Not surprisingly perhaps, in view of the widespread use of Oracle and Access the vast majority of the organisations relied most heavily on Relational Databases (twenty in total). No organisation reported using Object-Relational systems and only one reported using object-oriented technology. This organisation, however, reported that its systems were mainly either relational or older hierarchical database designs, and that the object-oriented technology was relatively unimportant to the organisation's activities. Three organisations specifically mentioned that they used spreadsheets, though these also relied most heavily on RDBMS. The second largest category selected was under the heading 'databases' (nine instances), the majority of which were 'hierarchical databases'. Finally three organisations were using other forms of storage such as "flat files" and "stand alone independent records", while another three organisations said that they were using all of the options mentioned (see Table 7.5).

1	
Database	X,X, X, X
	A, B, C, D
RDMS	X, X
the relevant record and a link in another re-	A, D, E, F, G, H and some of the largest
Object-Oriented	D respectively in agmented
Object-Relational	- onlicibile to the organic' growth of IT.
Spreadsheet	E, G, H
Other	F, G, I, J, K
Any/All	X, X
protection by preventing the linking of date	Educred for different purposes, even when

Table 7.5: Replies to Question 3.2\*

\* X refers to an organisation that chose this option only. Where an organisation chose more than one option this is illustrated by giving it another letter

#### need to make their systems Euro and Y2K compliant

Question 3.1 concerns the use of a unique identifier within the system, a key issue in relation to how data are stored and analysed (it is also linked to Questions 1.1 concerning data items and 1.5 concerning the importance of different data items). The importance of the question was not in whether there was an identifier (all organisations were expected to have one) but in its nature. All thirty organisations had an identifier and the majority of these were in the form of assigned unique numbers (twenty-five cases), with a further five using a combination of other categories together to comprise a unique identifier. Thus twenty-four of the twenty-five used a unique number generated within their own systems while one government organisation used the PPS number exclusively. The low level of usage of the PPS number can be attributed to the legislative restrictions on its use described in Chapter Five. However, in at least one case an organisation stated that it was not used because of 'uncertainty about its value as a truly unique number'. This organisation accordingly used its own identifier even when dealing with data containing the PPS number. The remaining five organisations used combinations of "name and date of birth", "name, address and date of birth" and "assigned number and name".

One unexpected item of information to emerge from this question was that many organisations possessed different datasets, each of which possessed its own unique identification system. The result was that personal information on a particular person might be stored under different unique numbers (and even potentially an entirely different numbering system) in different systems. In consequence it is not possible to directly link personal information collected and stored in one database with that in another. Some organisations get over this issue by using separate combination identifiers that enable them to link such records, while others 'flag' a link within the database even though assigning a new number to a new case. In the latter case the keying-in of one identifier will bring up the relevant record and a link to another related record. However, some of the largest organisations contacted did not use such techniques and so had entirely fragmented databases. In many cases this was directly attributable to the 'organic' growth of IT capability in an unplanned fashion over many years with particular departments of the organisation creating their datasets without consulting others. In effect this action prevented organisations getting maximum use from their data but also increased data protection by preventing the linking of data gathered for different purposes, even when legal. In these cases, however, the introduction of new systems that would be more coordinated was generally in progress. A number of organisations appeared to be using the need to make their systems Euro and Y2K compliant as a means to modernise and integrate their systems and enable the linking of previously separate datasets.

Questions 3.4 and 3.5 covered the possibility that the organisations concerned were using GIS or the spatial tools now available for standard databases (see Chapter Two). Only eleven of the organisations had GIS as such either as their main system, or for use on data extracted from the main system. The GIS packages most commonly used were Arcview, Mapinfo and Microstation. However, most representatives of organisations spoken-to were not GIS experts themselves and so could not always name the particular GIS package in use. In one organisation the package in use was a Computer Aided Design package, and thus not technically a GIS according to the narrow definitions of GIS. However, it was being used to specifically spatial work. Two of the organisations that had GIS had not yet fully implemented their GIS but were in the process of doing so. Only one organisation representative responded that the organisation was using more than one GIS package.

Of the remaining nineteen organisations only eight claimed to be using some spatial functionality. None stated, however, that they were using the spatial tools for databases that have recently become available. Instead the spatial analysis consisted of "non-map based" analysis using some of the geographical codes stored as data items with the other data. In effect this involved grouping and classifying individual personal records by geographical area (such as census area) using normal database functionality. While such analysis is crude compared to what can be done using GIS, and while it lacks the visualisation tools of GIS, it is nonetheless powerful. Thus, for example, it would be possible to group customer addresses on the basis of the census area to which they belong. Then, in combination with actual census statistics, geodemographic profiles of customers and the areas in which they live could be developed.

The final question in this section abandoned the issue of GIS and moved in the direction of access to the data, the subject of the next section. The question concerned the physical location of the database and the nature of access to it. The vast majority of respondents (twenty-four) had centrally-held databases with remote access to them over protected networks. In the case of the some of the smaller organisations such access, although 'remote', was all from within the same building. Of the twenty-four organisations two also had other forms of system, namely 'diffuse' and 'centrally-located with central access

only' (in both cases the centrally-held and accessed database was used for highly sensitive information).

Diffuse location applied in four cases, although this was the exclusive database type in only one (two others had both 'diffuse' and 'central with remote access', and one had 'central access'). Central access of a 'centrally located database' applied in a total of six cases, only three of which used this method only.

## 7.5 Data Access and Security Issues

This is perhaps the most important section of the questionnaire with regard to the issue of privacy, as most people would understand it since it concerns directly those who can access information.

## 7.5.1 General Access Issues

The section on general access issues concerned the issues of technical and organisational issues affecting access, the personnel who can access information and those who can update it. It also includes the issue of procedures in place to protect against falsification of information by authorised personnel or others.

The majority of organisations questioned had a minimum of a password and user identifier. Two of the organisations did not need this precaution due to the nature of the dataset in one case, and the limited access to the terminal in the other. The remaining twenty-eight organisations all made use of at least one level of password protection. Quite a number of the larger organisations specified that there was more than one level of such protection. In such cases one password is needed to access the overall system and a second to access individual datasets. Policies in relation to passwords existed in all but one of these twenty-eight organisations. A large proportion (twelve) had regular changes at thirty, 60 or 90-day intervals. A further twelve said that they had a policy of regular enforced change without volunteering a time interval, while one organisation did not have a specific policy. The remaining three organisations' policies were 'changed twice a year', 'varied', and 'frequent but at irregular time intervals' respectively.

A total of nine of the organisations specified that they used encryption methods while five used firewalls. Four of those using firewalls were also using encryption. Three of those using encryption also specified that they used 'other multiple security systems'. These were respectively 'passwords, encryption and scrambler', 'dedicated line and encryption' and 'swipe card access with passwords and encryption. Four organisations also specified that they used 'other' security measures: 'physical security' in two cases, 'call line identification' and 'terminal security'.

A similarly varied situation existed in regard to organisational issues of security, though the most commonly mentioned was the monitoring of access patterns in the form of an audit trail, while four organisations did not feel that such procedures were necessary. Twenty-four organisations specified audit trails as a significant aspect of security. Of these ten also conducted staff checks, while only one organisation conducted staff checks but did not specify that they used audit trails. One organisation was unwilling to answer this question.

Question 4.3 asked who could access information on the organisation's system. Many of those questioned specified that a number of the categories applied. All organisations had a minimum access for those who entered the information and those in the same unit. One organisation had no access beyond this level, two beyond 'intradepartmental' level, fourteen beyond 'cross departmental', and twelve had 'access across organisation'. Only four organisations (all of which had separately specified a level of internal access) specified access for outsiders. In all four cases such access was necessary for the conduct of normal business by the organisation and such access was limited by protocols to necessary organisations. One organisation specified that a variety of such categories would apply, with the degree of access varying according to the particular system in question.

The next part of Question 4.3 made these answers much more clear. It emerged that though read-access might be stated to be 'anybody in organisation' what this actually meant was to 'anybody in the organisation that needed access because of his or her job description'. Only eight did not have some form of restriction to access on this basis. Of the remaining twenty-two, thirteen were predominantly job description, seniority or 'need to know' based. In some of these cases particular data types were also considered more sensitive, but all of these fourteen were united in the fact that job needs were the chief

restricting factor. The remainder had restrictions based on sensitive data, which was predominantly of a financial or medical character. In two cases the information considered most sensitive was actually stored only in conventional files with only information needed for processing purposes being entered on the system.

ideing was the main method of control also mentio

One of the reassuring factors to come from this question was that access was decided in a negative fashion. Thus rather than having blanket access aside from certain sensitive categories, access to any information was limited to those who needed it, decided on an individual basis.

While Question 4.3 dealt with the issue of read-only access, Question 4.4 dealt with writeaccess, the ability to update the database. In this case two of those (eight) organisations that did not place restrictions on read-only access similarly did not have different levels of access for update. This seemed to be due to the relatively straightforward nature of update, which was undertaken by the same unit that initially input information, and the presence of firm procedures for such updates. The remaining twenty-seven all had some such restriction with the majority being based on job description and seniority or grade of employee (twenty-two of the total), and the remaining five confining update to a specific unit within the organisation. Significantly, of the twenty-two who had access restrictions based on job needs, or seniority, seven specified that such limited access was also dependent on the sensitivity of information. In relation to such sensitive information sensitivity was based on individual fields in the database in four cases, on sensitive cases in two, and on the phase of processing in the final case.

The final question dealing with general access issues dealt with the deliberate falsification of information, an issue central to data protection that specifies that data held must be accurate. In regard to this issue a wide variety of protections existed, particularly with regard to personnel and hackers, though many organisations admitted that it was difficult to prevent the data subjects themselves falsifying data if they so chose.

In regard to employees the combination of access restrictions (controlled by password) and the maintenance of comprehensive audit trails (discussed further in relation to Question 4.6) of who had accessed what were the main weapons. Fourteen mentioned auditing as the chief method, while five emphasised access control levels, with three giving the two equal emphasis. The next most important category was consistency checking or doublechecking of work by another usually senior member of staff. This was the chief measure for four organisations, while two organisations gave it joint eminence with auditing, and one with both auditing and access control. The remaining organisation specified that internal disciplinary measures dealt with the problem. In this vein four of those for whom auditing was the main method of control also mentioned IT security, system restrictions and independent verification (in two cases) as other factors. Similarly one organisation that listed access as the major restriction mentioned the employees legal liability for breach of contract in such cases.

The emphasis was different for access from outside. Sixteen organisations had no facility whereby direct access to a database could be obtained from the outside since systems were either completely closed (in thirteen cases), or because there was a dial back requirement (which only worked for approved numbers) or a swipe card system in operation. The next most important categories were internal security and firewalls respectively. In total there were nine of the former (including two who also had no direct dial) and six of the latter, with three of these common to both (one who also had no direct dial). Of the remaining four two mentioned audits and restricted access, one, software protocols and one the inability to modify data online. Other methods that were mentioned by some of those relying chiefly on these methods included the lack of physical access (when there was no direct dial), and the use of swipe cards, encryption and technology within systems, as well as, in one case, the existence of surveillance cameras.

In relation to the question of the data subject falsifying information the issue was somewhat simpler. Since in general the subject has no access to the system (unless they fall under one of the previous two categories) information can only be falsified at the data collection phase. While four organisations admitted that there was little that could be done if a person chose to give false information, and a further seven accept the word of the person, many conducted various double checks, some for purely operational reasons, others because required to do so by law (under Money Laundering Legislation for example). Of the seven that accept the word of the person, three nonetheless had either direct checks in a percentage of cases or had statistical analysis techniques which threw up anomalous data for checking. A large number of organisations otherwise either required certified information (eight), checked a certain portion of persons (three), or verified information with other sources (four). The technique of looking for anomalies was also used by two organisations.

#### In some cases the duration for which such records are kent was benelstool

In regard to the checking of information consistency only three organisations did not do so, while a further one did not feel that the question applied. Of the remainder the specified methods were: system reports and audits, fourteen; software checks, seven; double checking and administrative procedures, six. Non-standard updates required outside verification in all but seven cases. Such verification chiefly had to come in the form of a second signature or authorisation, usually by somebody senior. In other cases the only necessity was the written request of the data subject, while in one case an outside organisation verified changes in partnership with the organisation questioned. Such actions are usually the exception in most of the organisations questioned, however, and generally apply to changes of data which is regarded as sensitive, or as potentially having a serious impact either on the subject or the organisation.

#### 7.5.2 Internal Access

In relation to the internal accessing of the database the questions concerned the maintenance of an audit trail (already raised as a major security element by many of the interviewees), procedures to monitor unusual accessing, and the possibility of the removal of information in digital or analogue formats.

Question 4.6 asked whether there was a record of who accessed information and the purpose for which it was accessed, as well as the duration for which such a record was kept. Twenty-two of the interviewees had such a system of 'audit trail' or 'logging records' which produced regular (generally daily or weekly) 'system reports' for checking. Of the remainder one organisation was unwilling to answer the question on security grounds while the remaining seven did not have such systems. However, one of these seven was building such a capability into their system and another did have short-term (two days) recording of access though the policy was that access was open 'subject to the constraints mentioned earlier in regard to "need to know". Aside from this example most audit trails were kept for much longer duration's with three months being the shortest term (one case). Other terms included: 'last update' in cases where update meant major reconstruction of the database (2 cases), six months or the last permanent backup (one case), one year (one), two years for some datasets and indefinite for others (one case). As can be seen thus the vast majority of those holding an audit trail maintain it indefinitely or at least for many years.

In some cases the duration for which such records are kept was legislatively determined but in most it was a matter of internal rectitude. The form of the records entailed recording the login identity of those accessing particular information, particularly when such accessing involved the update of information. Many of the organisations stressed that this audit function acted in conjunction with the allocation of individual access privileges. Thus while it is theoretically impossible to access information for which one does not have a work-based need, and particularly to alter it, records of all such accessing were nonetheless widely held and analysed regularly in search of anomalies.

The next question dealt with procedures for detecting such unusual access, an issue mentioned by many interviewees in the course of answering Question 4.6. Again one interviewee did not wish to answer on security grounds. The key issues which were looked for were: attempting to access an unauthorised area, unusual work patterns in terms of areas accessed or the times when accessed, unusual volumes of work in certain areas (in particular sudden jumps in usage), password problems, and unauthorised attempts to change the database. One interviewee stated that the system architecture was the major protection and that attempts to evade this would be the major thing being looked for. One interviewee did admit, however, that if a person authorised to access that area carried out something untoward it would be very difficult to detect. Another organisation, however, which declared itself very sensitive to issues of fraud, stated that the division of labour within the organisation would make it almost impossible for an individual acting alone to conduct fraud. A number of organisations also mentioned unusual staff behaviour as a key issue which would warn management to check their audit logs. A particular example that was raised was reluctance to take regular leave entitlements. This would cause worry since such behaviour could mean that the individual is afraid their activities would be detected by their replacement.

The final question in this section concerned the downloading of and potential removal of information from the premises. Twenty-nine had some degree of ability to print out information. By contrast nineteen organisations allowed download to tape or disk (outside of regular backups), and fifteen allowed download to other systems or other media (generally a subset of those allowing download to tape or disk).

The circumstances in which such downloads were permitted varied. In regard to paper printouts the main reasons were for internal analysis and other work purposes, or alternatively when necessary to provide information either to the data subject or others where required by law (under the Freedom of Information Act or Data Protection Act for example). In many such cases the ability to printout was carefully monitored (in some cases from only one printer which was easily observable) or could be done with authorisation only. A number of organisations also had procedures in place that audited printouts, logging who had printed them. Any printouts that contained personal information were be shredded.

By contrast downloads onto tape, disk or other media were usually authorised only for higher grades of employee and in certain circumstances. Downloads to tape or disk were also permitted by some organisations for supply to outside organisations or sub-offices where this was appropriate (see discussion of questions 4.12 to 4.15 in Section 6.5.3). In regard to both types of download the chief purpose was to permit authorised higher level workers to conduct their tasks, usually analysis tasks working with statistical aggregate data. In a small number of cases such downloads were allowed to permit outside consultants (under strict legal contract) to conduct tests and technical fixes for the system.

The removal of material from the premises was permitted in fourteen cases only, usually in the case of management removing material on a laptop to conduct work at home. Once again this was based on job requirements and authorisation and limited to a very few personnel. Other circumstances where this was permitted included external office moves, transfer on information to those bodies entitled to it, and in situations where there was a legal requirement. In regard to printouts the additional circumstance existed of provision of the information to the data subject as has been mentioned.

The final part of this question regarded the safeguards against the unauthorised removal of such material. In this case the chief obstacles to removal were: the size of files and the practical difficulty of removing them, the audit trail which would identify potential individuals who had removed it, and the legal and disciplinary consequences of such action which would be a violation of the contract and of the law. Other safeguards included (in some cases) the impossibility of downloading personal information, physical security (security personnel and the need to use swipe cards to access areas, for example) and the presence of cameras, and the limitation of access to, or ability to download sensitive information. In many cases a combination of impracticality, logging, limited access, and the disciplinary consequences provided a high degree of protection. It was

acknowledged by a number of interviewees, however, that should an employee be determined to ignore the negative consequences, and be able to download an inconspicuous section of the database there was little that could be done since "you can't search everybody's briefcase on the way out". In such cases the best that could be done would be the disciplinary procedures undertaken after the fact when the breach was discovered.

# 7.5.3 External Access

With regard to the question of external access to information it was found that in general such access was relatively low. Where access to information did exist it did not tend to be in the form of direct access, but rather in the form of provision of information, usually under stringent control.

In regard to the provision of services over the Internet only two organisations provided such services, with a further two in the process of developing such services. This was despite the fact that most of the organisations questioned did have websites that were only being used to provide information regarding the nature of their operations. In the case of the organisations which had or were developing such services the nature of the service was to enable individuals to gain information on their own interactions with the organisation, and to undertake secure transactions with the organisation. The particular technical details of such operations are of a somewhat sensitive nature, but it is clear that the organisations in question use firewalls and encryption to establish a secure login and authentication of the identity of the individual. In addition there are limits set to transactions undertaken over the Internet.

In regard to the sharing of data with outside organisations a two thirds majority of organisations did share such information. It should be noted, however, that at least two of the ten organisations which replied in the negative do in fact give information to other organisations though such information is sold (the use of the word 'share' may thus have been misleading).

Of the private sector bodies which share information the majority do so with other private sector bodies, chiefly other similar institutions (five cases), though one organisation specified that it also supplies information to 'other service providers' in the private sector,

and another that it provided information to other bodies (chiefly state) 'only when legally obliged', while another provided data to the police when required. Two other private sector bodies provide their data on a sale or rent basis to 'anybody who will pay'.

In regard to public sector information there is somewhat more sharing. Thirteen organisations share information with certain government departments for certain operational purposes, usually statute driven. Four organisations similarly provide information to Semi-State bodies, and seven to the police or other official investigative bodies. Two public bodies also specified that they share information with other similar bodies, and a further two with other public bodies (specifically Health Boards). Three public bodies also share some information with financial institutions, chiefly in connection with payments. A number of other organisations both private and public also volunteered that they share other information more widely provided it has been aggregated for statistical use.

Where such data exchanges take place they are predominantly by means of transfer across the network without the outsider having actual access (ten cases), and by tape, CD or disk being sent by courier (fourteen cases). Only seven commonly give such information over the telephone, while three organisations provided data in printout format. Three organisations selected the option 'direct access' but subsequent elaboration revealed that in such cases access was read-only.

Where networking is in place to other institutions a plethora of safeguards are operated. These include passwords (five), encryption (four), personal accounts (two), smartcards (one), leased lines (four), call back (one), firewalls and address authentication (one), and agreed protocols with direct line (one). A number of organisations with such networking only allow access to statistical information.

As will be clear from the above there is little if any direct access. One organisation has direct full access since their information is public; three have access for specific cases (in one of these this is only in the event of an outside specialist needing to fix the system). Finally two organisations selected 'other'. In both cases there was networking but no direct access; in such cases the two systems interacted, one sending an enquiry which generated an automatic reply transferred over the network without any access being granted.

162

In regard to email all of the organisations had email systems, though in some cases limited to a very small number of staff. Only two organisations had internal email only though nine of the remainder had only a limited number of external accounts (internally everybody was connected). The chief method of protection was the password, which was used in all cases. Additional protections included firewalling and the existence of external accounts only on stand-alone machines not connected to the company system (three). Other protections included the necessity of logging on to the system first and thus establishing an audit trail, limited access to connected PCs or terminals, and the fact that in certain organisations external accounts were limited to management.

The policing of email was of considerable importance to a number of organisations that expressed concern over potential legal problems in the event of misuse, particularly in the absence of clear legal precedent or legislation. Five organisations had a skeleton policy or were developing one while two had a personnel policy document that had to be signed by employees. Six had some degree of monitoring of content, usually by IT security, and in one case copies of everything were maintained at another site. One organisation also had a specific ban on the acceptance of attachments, and a requirement that mails be virus checked. In the majority of cases, however, the policy seems to have been mainly concerned with the usage levels, and the volume of email storage with a requirement for regular clearouts of memory.

Email accounts were only transferable in three of the organisations. This was only done where an email account was passed to another's supervision during an absence, following the departure of an employee, or in the case of group email accounts.

In regard to the response to requests for information by telephone twenty-seven had a policy. Of the remaining three two did not give out such information, and the third did not feel the information was very sensitive. Six organisations would only give out such information in written form to those entitled to have it or with written permission. Sixteen have internally- or legally established protocols that must be adhered to in order to establish identity and entitlement, in which staff who will deal with such queries are trained. Two organisations used call back to identify the person, two require referral to a member of management, and two others have a policy of refusing except in exceptional circumstances.

Only two of the financial institutions surveyed used automated telephone banking. Both had sophisticated techniques to ensure security, consisting of a digital id and password, and secure lines.

Question 4.21 reveals that the most important public bodies in terms of sharing information in the public sector are finance, the central statistics office and the Department of Social Welfare.

## 7.6 Data Protection

At the time the survey was undertaken the Data Protection Act had been in force for ten years. The organisations involved in the survey showed a high degree of awareness of data protection. In addition it was found, perhaps surprisingly that most organisations expressed approval of the Act, and that few found it a serious impediment to their operations. Only a small number of organisations said that they belonged to the IDMA, the only organisation to have produced a Data Protection Code of Practice recognised by law, although many belonged to other organisations which did not have codes of practice of the sort envisaged in the 1988 Act.

## Table 7.4: Data Protection Compliance

	Yes	No	N/A
Required to Register under Act	28	2	-
Registered under Act	28	2	A on the
Procedures to Comply with Act	28	2	anisations
Membership of Representative Body	18	3	9

The first part of this section of the questionnaire concerns the requirement to register and procedures taken to comply with the requirements of the Act. Of the organisations surveyed the vast majority fitted at least one of the categories required to register, and some fitted more than one (generally at least one of the categories of data controller required to register, in addition to the category of data processor). These same organisations had all registered. As can be seen from Table 7.6 all of the twenty-eight

organisations required to register had done so. Many of them revealed that they had more than one registration, in one case ten.

The third question of this section was also concerned directly with compliance with the Act and asked not only whether there were specific measures in place to ensure such compliance, but also encouraged the respondents to volunteer what such practices might actually be. As can be seen from Table 7.6, all twenty-eight organisations had such procedures in place. The majority of specific answers to this question involved the appointment of a Data Protection Officer (sixteen), as envisaged by the Act. This was closely followed in terms of frequency by the existence of in-house data protection manuals and operational procedures (nine), and regular circularisation of employees to ensure their awareness of the terms of the Act (seven). Other measures mentioned included the incorporation of the issue as part of staff training (three), regular reviews of the terms of registration (four), various procedures involving third parties, usually the data subject (six). One organisation had internal auditing in control of compliance and another had a legal team who had responsibility for implementing the Act. A further two (government) organisations specifically mentioned that their own governing Acts in large measure controlled what they could and could not reveal and thus the DPA was only of partial relevance. Only one organisation mentioned regular contact with the DPC's office as one of their strategies. Registration reviews, however, often involve such contact, and in those organisations that had a DPO his/her job involves such contact when in doubt as to the appropriate action to take.

The second part of Section Five concerned the issue of the impact of the DPA on the activities of an organisation. Perhaps surprisingly the vast majority of organisations questioned had little problem with the operation of the Act. In the Irish context twenty found the Act 'easy to comply with', three stated that it was 'awkward', and five that it 'curtailed activities somewhat'. Nobody felt that the Act curtailed their organisation's activities in Ireland seriously.

In terms of foreign activities the number who felt the question irrelevant to their activities jumped from two to thirteen. These either did not conduct international business involving personal data, or, if they did, only transferred aggregate statistical information. Of the remainder twelve found compliance with the Act 'easy', and two 'awkward', while one said that it 'curtails somewhat', and one that it 'curtails seriously'. This final organisation

found that this category was actually sufficiently "not strongly worded" and that the Act had very serious implications for international activities outside the EU. On the other side of the debate, however, it was pointed out by one financial body that by breaking down legal barriers within the EU the Act (and associated ones Europe-wide) "breaks down barriers between organisations" and thus "protects international business".

The comments made concerning the Act reflect the overall picture of ease of compliance. Many organisations, while acknowledging that the Act had necessitated some adjustment initially, felt that it was actually positive in many respects, or else that it was largely neutral since either for competitive or other organisational reasons data tended to be kept confidential anyway. While all organisations had a high degree of awareness of the Act and of its provisions, many felt it to merely be something that accorded with their normal practice. In this context one respondent said that though there was some extra work involved the Act had a two-way effect of protecting "the individual and the institution".

There was a minority of respondents who, while broadly supportive of the Act, did have some criticisms. At least three organisations admitted that they disagreed with the DPC over certain issues relating to their operations. The result was inevitably the curtailing of the organisation's acts in that arena, resulting in the loss of competitive advantage, or efficiency. In other less serious cases organisations admitted that the Act "doesn't help", or that it "curtails peripheral activities". In other words certain activities which that organisations might like to undertake were rendered out of bounds by the legislation and the DPC's interpretation of it. One final point raised in organisational perspective, certain areas of the organisation did have more work to do due to the need to respond to customer requests. In addition three organisations specifically mentioned the provision of the EU Directive extending protection to analogue files, which will potentially have a significant effect on the cost and manpower involved in data protection for organisations.

The final question of this section was designed chiefly to find out which organisations belonged to representative bodies that had Codes of Practice. Since only one body, the IDMA, has fully implemented such a code after four years of consultation with members and the DPC (Moss, 1998), however, the question turned out not to be as relevant as might have been expected. Nonetheless seventeen organisations did belong to such organisations, while three did not and nine felt the question irrelevant. Of the seventeen
organisations that belonged to such bodies, the majority belonged to more than one. These included many such organisations, both national and international, although the IDMA was mentioned in only three cases.

# 7.7 Conclusion

While certain types of Geographical Information like maps or satellite images are intuitively understood to be such the type of Geographical Information dealt with in this survey has been quite different. It is nonetheless GI because of the ubiquity of a geographical reference, in most cases the address. More importantly the other information which is linked to this address is of a highly personal nature. The recent release of products which geocode individual Irish addresses make the use of such information as GI easier than ever before, while the data itself is chiefly held in systems which are based on relational databases, the same model used by most GIS systems.

Furthermore this information is widely accessed though the sharing of it between organisations is limited. While security measures within the organisations questioned seem robust, it is clear that concern for confidentiality rather than data protection was the cause, though compliance with data protection is high. The fact that most organisations found that data protection was advantageous to their own operations and confidentiality once implemented is perhaps the main reason. The need to protect commercially valuable information in the case of the private sector, and the traditional culture of secrecy within the civil service seem to be much more important than any concern for personal rights. At least one interviewee admitted that in his private capacity he was very concerned for privacy, but that in his professional capacity concern for privacy could be an obstacle to the efficient operation of his organisation.

In regard to the input, update, accuracy and currency of data considerable efforts are made to ensure high standards are maintained. Once again, however, this appears to be a matter of organisational efficiency rather than any particular concern with these issues as defined under data protection legislation. Information which has been allowed to become outdated, or which has been inaccurately entered or updated would lead to inefficiency of operations. Thus the maintenance of high standards of information integrity are vital to most organisations, and the need to adhere to data protection principles seems to merely encourage this further. In the next chapter these findings will be discussed in the context of the content of previous chapters to examine the degree to which this information fits into the history of GI's use as an instrument of power, and the potential use of this power over the individual in view of the legal situation in Ireland in the late 1990s.

## 8.1 Introduction

In previous chapters a number of issues have been cause. These include the links between the use of GI and the exercise of power, both historically and in the present; the increased power that modern methods of manyalation give to the use of GI, the ethical use of information and the importance of proview and its measurable variant interpretations of the importance of information in the exercise of power and its measurable variant interpretations of the constraints on the use of information in the exercise of power and the level restriction of privacy and results of a survey of thirty large or provide the college score and end of a personal nature in Ireland.

The purpose of this chapter is a second second second second for ingen in second secon

in modern society the latternal of the second secon

Traditionally GI was used to according to the second secon

# **Chapter Eight**

# **Discussion of Results**

8.1 Introduction

In previous chapters a number of issues have been raised. These include the links between the use of GI and the exercise of power, both historically and in the present; the increased power that modern methods of manipulation give to the use of GI; the ethical use of information and the importance of privacy and its meaning; various interpretations of the importance of information in the exercise of power; and the legal protection of privacy and constraints on the use of information in Ireland. Finally the last chapter discussed the results of a survey of thirty large organisations that collect, store and use GI of a personal nature in Ireland.

The purpose of this chapter is to integrate these various issues and findings. In so doing it will create a picture of the current status of privacy and related data protection issues in Ireland with regard to such data. Further it is hoped that this will shed light on the nature of the relationship between the individual and such organisations.

In modern society the Information Revolution has, if anything, increased the power of information by making it easier to manipulate, and by privatising it as a commodity. Information has become the basis of many industries, some of them the fastest growing in the world, as well as coming to underpin the activities of many if not all of the traditional industries. Information infrastructure is the basis of the modern world economy.

Traditionally GI was used as an instrument of power by many institutions for many purposes, significant among them the state and military. Part of the development of Information Technology over the last decades has been in the area of GI manipulation and analysis, resulting in new methods of GI manipulation making it more powerful than before.

# 8.2 Privacy of GI in Ireland

In regard to the specific question of GI in Ireland a twofold study was undertaken involving a study of legal protection of privacy and a questionnaire survey of organisations to determine their operational methods of ensuring privacy and data protection. Although the entire questionnaire was of relevance to the issues, differences in the focus of the questions are evident. The parts of the questionnaire of central importance are Questions 1.1, 1.2, 1.5, and Section Three since these indicate the type of information collected and the nature of storage which in turn affects the ease with which it is used in geographical analysis.

What these questions reveal is a very comprehensive collection of personal data being held by these organisations. The basic administrative data collected by the majority of organisations included the name and address. Additional categories of information commonly collected included the date of birth and PPS number. These categories of information in combination with an internally supplied reference number seem to be the core information used to administer the database and ensure unique records for each individual. The ancillary information which was added to this is perhaps more significant in terms of personal privacy since it is the information used to determine the behaviour of the organisation in regard to the individual. As such this information varied from organisation to organisation but the most commonly included categories were occupation, income, family relationships, medical details, telephone number, insurance and financial details, property ownership and religion.

All of these categories constitute quite sensitive personal information. Religion and health details are two of the types of information (with race, political and other beliefs, and details of sexual life) identified as being especially sensitive and requiring special legal protection according to the Council of Europe Convention on Data Protection (1981). More significantly from an Irish perspective financial information is held to be the most sensitive type of digitally held information by most Irish people according to a recent survey by the Data Protection Commissioner (DPC, 1998). In terms of concern financial details were closely followed by: health, PPS number, and telephone number (DPC, 1998). According to the results of the survey it is precisely these sensitive items of information that are most likely to be collected and used. Despite this the majority of those questioned

did not have a sensitivity ranking for their information, though those that did ranked health and financial details as most sensitive. Others merely ranked certain individuals' records as more sensitive than others did.

In regard to the geographic aspect of the information collected the majority of information used the address as a geographic link though a significant number also used either an area code or grid reference. This information was typically stored in a relational database system, the most common being Oracle and Access. This is highly significant given the fact that many GIS packages, including the market leader ARC/INFO, use a relational database model. This similarity of underlying data model facilitates the transfer of information from this type of storage into GIS packages for analysis.

While only eleven of the organisations were using GIS packages as such, a further eight were using the normal abilities of relational databases to carry out some spatial analysis using geographic area codes. This is quite significant since the recent release of the GeoDirectory address database effectively means that in future address-based data can be given a precise geocoding. Since eleven of the organisations already use GIS and a further eight are sufficiently interested in the benefits of geographic analysis to attempt it in conventional databases without specific geographic tools it is likely that such analysis will become more important in the coming years. The recent release of spatial tools for Oracle and Access, in combination with this tendency to conduct spatial analysis, further increases the likelihood of ever increasing use of geographic analysis of personal information. While such personal information might not always traditionally have been regarded as geographical by organisations it is likely to be so in the future.

The importance of this discussion for privacy should be relatively self-evident. Large volumes of information are currently being collected about individuals in the population in the course of normal business by organisations from a variety of different sectors (both public and private). Such information is of a geographical nature as well as of a highly sensitive personal nature, and is increasingly open to geographic as well as other analysis. At the same time the nature of modern life, and the importance of the institutions concerned, means that it is almost impossible to avoid volunteering this information. To do so would of necessity prevent an individual interacting with normal society in a meaningful way since that person could have no dealings with the state or any of the major

171

institutions which regulate daily life, in effect making the individual an outcast in an Information Society.

In effect therefore the option of information privacy (through non-disclosure) does not exist in the modern world. This is not a new trend. Many of the organisations questioned from the Central Statistics Office through to the financial institutions were collecting significant amounts of personal information before the advent of the computer, although perhaps in some cases on a smaller scale. The difference is essentially in the technology and what it allows. Previously such information was collected for a single purpose and filed. Although it could be used for other purposes and combined with other information this involved a great deal of work in manually extracting information and cross-tabulating it. The use of computing power changes this. It enables the accessing of information from a variety of sources or files, and its combination with relative ease. Such access is relatively trouble-free as, in a networked organisation, it can be achieved without leaving one's desk. The information thus accessed combined in new ways to create new information and analysed for a variety of purposes.

Thus, although information privacy has been being eroded for some time, the development of new technology, added to the inclusion of virtually all members of the population in databases takes this erosion to a new level. More significantly still, the distinction between the manipulation possible of such information stored in paper files, and that possible in digital form makes the level of privacy much lower. Whereas formerly records were stored in a filing cabinet and had to be searched for, and any correlation with other information had to be made manually, now such access and manipulation is possible to anybody with appropriate clearance (provided systems are well designed and are mutually interoperable). Although in the past privacy might technically have been infringed by the process of data collection, the method of storage meant that very few people would see the information, and even then only on rare occasions. In effect a certain residual privacy protection existed due to the difficulty of dealing with manual files. The modern situation is quite different since not only is the information collected in the first place but also all the practical obstacles to access and use can effectively be removed through the use of IT.

The purpose of the concept of data protection and the resulting legislation and codes of practise is to attempt to redress this balance. It is important to note, however, that though data protection is related to privacy it is not the same. While the preamble to EU

Directive, and Section Two (Protection of Privacy of Individuals with Regard to Personal Data) of the Irish Data Protection Act, 1988 both specifically mention the protection of privacy, data protection is only really necessary because of the erosion of privacy. In effect what data protection attempts to ensure is that information which would be regarded as private by an individual, but which has to be revealed, is treated confidentially by the recipient. A second strand of data protection is designed to ensure that information is of a sufficient quality to ensure that the interests of the individual are not adversely affected by the use of inadequate data.

## 8.3 Implementation of the Data Protection Principles in Ireland

The essence of data protection is contained in the data protection principles which are set out in the Council of Europe Convention on Data Protection, itself the basis of the various national data protection statutes in Europe. These principles are also enshrined in the Irish Data Protection Act, 1988, and are the basis of good data protection practice and of enforcement according the Data Protection Commissioner (1988). The Principles are as follows:

#### Quality of Data:

- Fairly Obtained and for a Specified Legal Purpose;
- Adequate and Relevant to Purpose, but not Excessive;
- Accurate and Up to Date;
- Kept only for as long as necessary.
- Special Data to be Given Safeguards in Domestic Law:
  - Race;
  - Political, Religious and other Beliefs;
  - Health and Sexual Life;
- Appropriate Security Measures:
  - Against Damage, Loss or unauthorised access or alteration.
- Subject Rights:
  - To establish the existence of data;
  - To know what is in such records;
  - To have such records amended if inaccurate;
  - To have such records deleted if appropriate;

- To redress in the event that their rights are not respected (Council of Europe, 1981).

In their more concise form the principles can be held to consist mainly of those listed under data quality, appropriate security measures and subject rights. These principles provide a comprehensive range of rights to the individual and impose corresponding duties to the 'data controller' or 'data processor'

This clearly shows that data protection is a question of the balancing of commercial and organisational needs of data users with those of the data subject to privacy and to respect for information given on trust. It is clear that the individual (or data subject) is obliged to surrender information of a personal nature subject to certain constraints (legality, fair obtaining, and relevance among others). As a balance to this the principles seek to ensure that such information is not used to the detriment of the individual, or for unspecified purposes, and that the information is maintained as confidentially as possible and is accurate.

While technically only the Section of the questionnaire on data collection directly impacts on privacy in the pure sense, the rest of the questionnaire impacts on the wider concern with data protection. Thus the extent of the data, and whether 'special' categories of information are held is dealt with in the Section on data collection since this overlaps to a significant extent with the question of privacy itself. The issue of accuracy arises in Sections One, Two and Four, while access and security issues arise in the Sections Two and Four. The issue of subject rights to know and have rectified any information held is indirectly covered by Section Five since this section deals with actual data protection legislation and its impact on the organisation.

## 8.3.1 Data Protection and Survey Results

# Table 8.1: Data Protection Principles Relating to Data Acquisition and Standards

	•	Fairly Obtained		
in		s regard as they		

- Specified Legal Purpose
- Adequate and Relevant to purpose but not Excessive
- Accurate and Up to Date
- Kept only for as long as necessary

In regard to the principles relating to data quality listed in Table 8.1 above, a number of conclusions can be drawn. The requirements for a specified legal purpose, and that the information is adequate to that purpose, are dealt with indirectly by Section Five of the questionnaire. From this Section it is clear that there is a high degree of awareness of the DPA among the organisations questioned, and that twenty-eight of the organisations had registered as required, while the remaining two did not need to do so under the terms of the 1988 Act itself.

The Register contains details of the purpose for which data are collected, and the types of data collected. Since the Commissioner is both responsible for enforcing the Act, and for administering the Register, it can be surmised that registered data are both legal and relevant. The fact that the vast majority of organisations acquired their information directly from the individual, who was thus aware of collection and gave his/her consent means that the necessity of fair obtaining is met. In the case of organisations that obtained information from other organisations the legal requirements of the Act require that the individual be aware that information may be passed to another organisation.

The questions of accuracy and of retention of information only for as long as necessary are more complex and are dealt with in greater detail by the questionnaire. In regard to accuracy the evident benefit to the organisations, raised by a number of them as an issue, of the accuracy and timeliness of data was more significant as a factor than their obligations under the DPA. Nonetheless the effect remains the fulfilment of this principle, regardless of the motivating factor. A number of methods of ensuring accuracy were used, the main one of which was checking with the data subject at 'point of contact' and afterwards. Other important checks included documentation checks and software and audit consistency checks, as well as various other methods such as checks with other agencies. At the stage of data collection and initial input, as well as for later update the use of personal contact with the subject to check details is most significant for data protection purposes since it involves subject knowledge, and consultation. The retention of documents, backups, and particularly initial application forms are also important factors in this regard as they ensure that the individual is protected by potential recourse to original (non-digital) documents. The other methods of checking data accuracy (such as double-checking by a supervisor, or the use of software validation) are more important for organisational purposes (such as the avoidance of fraud and the maintenance of data quality at a high level) rather than for the protection of the individual.

#### Table 8.2: Data Protection Principles and Security

Just as organisations placed substantial significance on accuracy at the data collection stage subsequent input and update also involved both safeguards designed to protect the individual and the organisation. In many cases such safeguards would be simultaneously advantageous to both. All of the organisations placed a strong emphasis on the level of training of staff in the operation of their software and the procedures used. All of the organisations had a standard operating procedure (fully documented in twenty-six of the thirty cases) for update and input with which their staff were familiar. The use of screen driven data inputting and standard formats ensured that any major mistakes in input are immediately flagged and must be rectified before proceeding. Additional checks such as those by supervisors and auditing procedures were further guarantees against mistakes that could lead to inaccuracies. The frequency of update is also significant in this regard and as in other cases the majority of organisations specified that this was a priority, once again because of the liability of dealing with out of date data.

The principle of keeping data only for as long as necessary was a closely related issue. Ensuring accuracy necessitates the maintenance of adequate backups, and the requirement to be accurate means that organisations must keep such material in case of disputes about the source of any inaccuracy. There is thus some potential for material to be maintained for longer than might be necessary. Although the answers varied it transpired that backup and archive material was kept for a variety of time periods both in digital and paper format. Organisations governed by statute, or in sectors subject to legislative regulation. were subject to legal requirements to maintain such records for specified lengths of time. Even in the case of organisations not subject to such provisions, however, practical considerations meant that the minimum time period for such storage was one year in the case of analogue records. In contrast digital material was largely kept for technical reasons and thus was more ephemeral, being regularly overwritten to conserve storage space. The overall picture was of a situation where manual material was kept for a number of years depending on the legislation governing the activity concerned. In some cases this period was arbitrarily set while in others such material had to be held for the duration of the relationship with the individual. By contrast the digital material by being constantly overwritten ran almost no risk of being maintained for longer than necessary. In this case once again the operational needs of the organisations largely coincided with the interests of individuals.

176

Table 8.2: Data	a Protection Principles and Security
access to datas	Appropriate Security Measures Must be in Place:
measures and t	- Against Damage
	- Against Loss
In terms of ove	- Against Unauthorised Access
the integrity an	- Against Unauthorised Alteration
access to those	data. Password and user identification protection seemed to be a minimum

The question of security measures and the issue of access featured in between one third and half of the questionnaire. Section Four, by far the longest Section of the questionnaire, dealt specifically with the question of access both in terms of reading and of altering data, and of security measures. The issue of alterations to data was also indirectly dealt with by Questions 1.8 and 1.9 which concerned audit trails, and the later questions of Section Two on update and accuracy.

#### organisations themselves

The overall picture that emerges from these questions is once again of a serendipitous coincidence between data protection principles (Table 8.2 above) and organisational needs. A further issue that emerged through the course of many interviews, particularly with some of the largest institutions, was that databases were often fragmented. Thus different sections of organisations often held information on the same individual for different reasons without ever linking it. The often piecemeal development of IT resources in organisations over the course of many years means that many of the organisations have disparate systems in different departments, each dealing with different types of data. The majority of such systems are not connected at all and even where export is possible from one to another it is often done on a one-off basis. Obviously this has had a substantial effect in regard to the accessibility of data, confining access to those with authorisation within a particular section of the organisation. This is a situation that is rapidly changing, however. The need for greater efficiency and the tendency to centralise IT planning have led towards the introduction of unified systems. When coupled with the impetus and need to update systems due to worries about the Y2K problem and to have systems that can cope with the single European currency there has been considerable pressure to modernise such systems. All of the organisations that stated that they had such fragmented systems had plans of modernisation and integration in place. In effect the introduction of the single European currency and fears caused by the Millennium Bug were providing a timetable for such modernisation plans. The result is that even those organisations that had such fragmented systems will by the end of 1999 be in a position where there is much wider access to datasets within their organisations. In this context the use of various security measures and the assignment of different access levels becomes even more important.

In terms of overall security measures all organisations showed a high level of concern for the integrity and quality of their data, both from the point of view of internal and external access to those data. Password and user identification protection seemed to be a minimum on all systems, in many cases involving the use of a sequence of passwords to get into any database. While some systems did not have any external access others used firewalls, leased-lines, dial back systems and encryption to protect external connections. In all cases where information was officially accessible to outside organisations (as opposed to suboffices of the institution in question) across a network such organisations did not have direct access. Thus even with the protections afforded by leased lines, firewalls and so on there was still no direct access (even on a read only basis) permitted except within the organisations themselves.

Further to these technical measures other security measures were also in place including staff checks and usually highly developed internal auditing systems. Such systems for internal audit record access to and alterations of data and highlight atypical activities such as attempts to access unauthorised material, unusual access times and unusual volumes of traffic. Typically reports were generated by such auditing departments on a regular basis and checked for such abnormal activity. In addition to such security measures the use of physical security measures was particularly important, especially in those organisations where the databases could only be accessed from within the organisation, and in some cases within certain parts of the organisation. Such physical security included security guards on entrances, CCTV systems, and the use of ID badges within buildings to signal one's right to be present. In some cases such ID badges doubled as swipe cards preventing access to unauthorised areas. In certain institutions it was also necessary to use such a swipe card (in combination with more ordinary measures such as passwords) to access one's individual computer terminal. In this case access is even more severely restricted, and audit controls are even tighter.

On a less general level the question of access, and of any resultant alteration of data, was divided into two categories in the questionnaire: access by employees and access by outsiders. In the case of the latter those security measures detailed in the previous

paragraph form the bulwark against unauthorised access and alteration of or damage to data. In the case of the individual who is the data subject, however, less technical measures such as documentation checks form the major protection<sup>1</sup>.

The question of access within organisations was dealt with extensively in Section Four of the questionnaire. The overall picture was of organisational structures that specified particular access clearances for each individual. Though access was in many cases from anyplace within an organisation (apart from those organisations that had fragmented systems as described earlier), the degree of access available was limited. Significantly the descriptions most often used of this limitation were 'job description based' and 'need to know based'. This individual-specific access existed on two levels: access to view data, and access to alter data. The latter was even more restricted than the former, and often limited to certain grades of employee. This seems to indicate a high degree of precaution being taken against the possibility of unauthorised or damaging alterations to data. Additional factors in this case would be the necessity in certain organisations to gain authorisation for unusual alterations to a dataset, or for alterations to sensitive aspects of the information. The technical security measures that prevent outside access that is not authorised also operate in the realm of internal access: namely passwords and other identification systems and internal audit trails. Thus each access leaves its signature which can be used to trace the person who made an alteration which later proves controversial. Once again in such cases it is concern for organisational needs which is key. In interviews with the public sector it was repeatedly stated that the traditional 'need to know' ethos still had a strong hold on organisations and dominated thinking when it came to access. Similarly in private companies the commercial advantage inherent in customer data was acknowledged to be a key factor in access restrictions.

Some organisational representatives did, however, outline potential cases where unauthorised access to and alteration of data could conceivably take place. One such case was where somebody left his or her terminal while logged on, and somebody with access to the same area used this lapse. A number of organisations did, however, specifically mention that on-screen messages reminding employees not to do so were organisation policy. Another potentially possible situation mentioned was where an employee who had recently left the organisation managed to gain access to the building (access to the system only being possible - aside perhaps from expert hackers - from terminals within the

<sup>&</sup>lt;sup>1</sup> Falsification of information by the individual him/herself is not a data protection but a fraud issue.

building). Such a former employee could be sufficiently skilled and knowledgeable to gain access and possibly make alterations to the database, and, not being an employee, could leave a false trail potentially pointing to somebody else. Such extreme actions seemed unlikely, however. The size and architecture of datasets and difficulty of reproduction of data, meanwhile, seemed likely to preclude unauthorised access to material removed from the premises. Similarly in the case of attempting to alter data the sensitivity of at least some of the organisations to potential fraud would mean that more than one employee would have to be involved in any attempt since the security measures were so tight and checking so constant.

One unexpected result of the survey was that public and private sector organisations appeared to give equal protection to their data. The relative safety of information in the care of public and private sector organisations has been the subject of some debate. Although in the 1970s, when the technology was expensive, the main worry was that 'Big Brother' government would amass vast databanks and eliminate the concept of privacy, in more recent years the increasing collection of data by private sector organisations has raised fears that privacy would be invaded for profit. In this context the fact that government has been collecting such data for decades without fears of 'Big Brother' being justified has led to some measure of trust of government. In addition the fact that government organisations are often governed by their own legislation in addition to general legislation (such as the DPA) means that there is a greater level of trust that government will take care of data. The absence of a profit motive for government is also a factor in this trust. Private sector organisations, since they profit from their data, are frequently viewed as less trustworthy.

However, the survey revealed few differences in the importance placed on data protection issues between the two sectors. The difference that existed was in emphasis, and intention. Thus, government has a tradition of secrecy that has only recently been overturned by the FOIA, whereas private sector bodies have a tradition of confidentiality. This tradition is based on two pillars: the profit motive, and the confidence of customers. Thus the profit to be made from the use of, and in some cases the sale of, personal information leads to a very high premium being placed on security. Those companies that sell or rent their data generally engage their customers in a legal contract to guarantee non-disclosure: once proprietary information becomes public it no longer has monetary value. The issue of confidence is also of considerable importance to private sector organisations, as any scandal concerning abuses would have a deleterious impact on the company's public standing. This could prevent customers from volunteering information in future. Finally it is undoubtedly the case that the Data Protection Act (1988) has had an impact on all of the organisations holding sensitive information, or other information that required registration. Its introduction led to a revision of procedures in all organisations (which most organisations found advantageous) to ensure compliance. It is significant that the Act applies equally to public and private sector organisations (unlike the US Privacy Act) and therefore has had the effect of ensuring that both sectors are compliant with the same standards.

Overall thus the picture which emerges is one of tightly policed access to information. Even where access is widespread within an organisation it is often confined to access to the most basic information at low levels of seniority, with the more detailed or sensitive information only readable by a limited number of employees. The same holds true for 'write access' which is even more limited, and where safeguards are common for types of information regarded as sensitive. In regard to damage of data it is as much in the interests of the institutions concerned that their data be of the highest possible quality as it is of the individual. Thus the vast majority of organisations maintained regular digital backups of their entire databases. Such backups were made on a variety of timescales from weekly through to three and six monthly. In most cases such material was stored off-site in secure locations, or, if on-site, in fireproof safes. Such backups were intended to allow the return to normal business speedily in the event of the corruption of databases, or of their destruction, by natural events such as fire, or by computer virus or other such technological attack. In addition to these digital backups of material the legally-required maintenance of paper and microfiche copies of original materials provides for the more laborious reconstruction of databases in the event it is needed. The maintenance of such material also makes it potentially possible to correct defects in the digital record if discovered, or to resolve contradictions between different records, for example. As has been noted previously the emphasis in almost all organisations on security had little to do with concern for the individual or for data protection legislation. Although the organisations appeared to take their responsibilities under such legislation seriously their main motivations were self-interest, institutional traditions of secrecy, and commercial advantage.

# 8.4 The Irish Legislative Context

One of the things most evident from the survey is the fact that concern for privacy and data protection issues is low in the organisations questioned. One individual remarked that as an individual he felt strongly about such civil libertarian issues as personal privacy but that as a professional it was his duty to care more about the purpose of his organisation. Thus, though there may be concern for privacy in organisations, it is subordinate to organisational needs. In the case of the organisation in question the constraints of the data protection legislation were causing some problems. Though the organisation in question did not find the Data Protection Act irksome according to the answers to questions 5.4 and 5.5 it became clear that the Act was having a negative impact on the organisation. This was due to the fact that the Act impacts not only on already existing activities, but also on potential activities that could be in contravention if allowed. In such a case a negative judgement from the Data Protection Commissioner can cause the abandonment of a proposed policy on the grounds that it would infringe currently existing levels of data protection. The only remedy for such a situation is the passing of enabling legislation by the Oireachtas to permit the activity in question, not an option open to any but major civil service organisations. Even in such cases the intervention of the Data Protection Commissioner during the passage of legislation through the legislative process can prevent or mitigate the effect the legislation as was the case with the Social Welfare (Amendment) Act of 1998. In this case the intervention of the Data Protection Commissioner prevented the full implementation of all those initiatives desired by the various Departments in the Integrated Social Services System Report (Government of Ireland, 1996).

In this context a number of the findings of the study of the Irish legal situation become quite important, and potentially disturbing. The interview process led to meetings with individuals with a variety of job titles. These included Data Protection Officers, IT employees including Heads of IT, and in the public sector, Freedom of Information Officers. Although Data Protection Officers gave data protection high level of prominence as a factor influencing their treatment of data, the other professionals gave other factors precedence.

Depending on the perspective of the individual and the nature of the organisation concerned these chiefly fell into three categories:

Commercial advantage in the private sector;

• A tradition of secrecy in the public sector (despite the introduction of the FOIA);

• And in regard to both public and private sectors the importance of security.

With the exception of employees whose specific job was data protection, the emphasis was thus on other issues, although the interests being served included data protection.

In this context the issues discussed in Chapter Five take on a new complexion. In that chapter the various legal protections of privacy and those laws relating directly to information technology in Ireland were discussed. While Ireland has adopted a number of initiatives to deal with the information revolution itself, privacy was less of an issue. The situation as it stands is that privacy is only protected in a fragmentary fashion and not at all comprehensively. While certain articles of the constitution protect the privacy of the family (a particular type of what the Law Reform Commission describes as privacy of the person) and privacy of property (the first of the four categories of privacy as defined by the Law Reform Commission (1996)), there is no overall right to privacy in the Constitution. While such a right is expressed in the UDHR and ECHR to which Ireland is a signatory, Ireland is one of the few signatories of the latter to fail to ratify it into national law.

In domestic legislation, similarly, privacy is only fragmentarily dealt with. Privacy of property is well protected by legislation as well as being a clearly defined constitutional right. Of the remaining three categories of privacy, aspects of privacy of the person and "the interest in freedom from surveillance and from the interception of one's communications" (LRC, 1996b: 11) are dealt with to some extent by a variety of diverse statutes of varying ages (LRC, 1996a). The final category of privacy, privacy in the information context, is legislated for in the Data Protection Act, and other legislation that deals with personal information, chiefly the Freedom of Information Act. The overall picture is, however, of a fragmented legislative and legal approach to privacy. Certain aspects of what could be described as the 'right of privacy' are legally protected, some through explicit legal provisions and others through interpretation of law relating to other issues (such as the rights of the family under the constitution, for example). As has been described by some of the legal commentators on the issue of privacy discussed in Chapter Three it is something which only gains legal protection through statutes protecting other rights. Though such commentators were referring to the situation in the United States it would appear that a similar situation exists in Ireland. Unlike the United States with its comprehensive Bill of Rights, however, into which case law has read some privacy protection, Ireland has a much less comprehensive list of rights in the constitution. As has been seen case law has only read the most minimal privacy protection into these laws. Various statutes add to the protection of privacy. Thus a very similar situation exists to US law. The question of whether this is due to the subordinate nature of privacy to other rights, to not being a right itself, as described by Prosser (1960) and Thomson (1975), or whether it is simply due to the complexity of the right to privacy is difficult to decide in relation to Ireland. While the question itself belongs to jurisprudential debate, and may perhaps never be resolved as such, it is clear that in Ireland there is some feeling that privacy as a right does exist but is insufficiently catered for by Irish law.

The position of the Law Reform Commission, the body established by statute in 1975 to recommend changes in Irish legislation, is clearly that privacy is important. Their 1996 consultation paper limits itself for practical reasons to one area of privacy, as they define it, though this is clearly envisaged as a first stage in their examination of the need for law reform in regard to privacy (LRC, 1996a). This area of interception of communication is chosen due to the importance of this consideration in view of technological change (LRC, 1996a). However, the Commission makes it clear that concern for privacy in general is 'justified' (LRC, 1996a: 2). They also state that this concern is at least in part justified by technological developments which enable both the state and private sector to amass large amounts of information without the awareness of the individual. Such information can "be acquired and used to the detriment not only of the individual concerned but also of society at large" (LRC, 1996a: 2). In addition they add that the law is often slow to adjust to such dangers, and that "in some areas, there is little or no protection" (LRC, 1996a: 3). Thus the body charged with law reform in Ireland not only holds that privacy is actually a right which needs protection, but also that current developments endanger privacy. They also point out in their 18th Report that the Consultation was "a response to the growing concern.... at the lack of legal protection for privacy" (LRC, 1996b: 11)<sup>2</sup>. It is moreover, clear that the Commission intended this Consultation Paper and Report to be a starting point in their examination of the need for law reform to enable privacy protection in general (LRC, 1996a: Section 1.8).

The clear implication of this discussion of the right of privacy in Ireland is that it is a right which is not clearly defined in law and is fragmented in its protection, though agreed to be in need of such protection by the body charged with law reform. Starting from this perspective it becomes clear that the legislation enacted with regard to information

<sup>&</sup>lt;sup>2</sup> The Commission recommended the creation of a number of torts and offences in regard to surveillance (LRC, 1996b: 11, 12).

regarding the person, and to "privacy in the information context" (LRC, 1996a: 3), is unusual in its scope and comprehensiveness.

The Data Protection Act of 1988 enacts the provisions of the European Convention including the data protection principles discussed earlier. In addition it establishes a duty of registration on those who possess or use personal information, and empowers a Commissioner to oversee this process and act as an ombudsman to deal with and arbitrate complaints. Unlike some similar legislation, however, such as the initial Data Protection Act (1984) in the United Kingdom, the duty of registration is not universal. Instead only those holding certain types of sensitive personal information (see Chapter Six) are obliged to register. This omission seems to be sensible since the British Data Protection Registrar was unable to enforce compliance to such an extent that non-compliance was estimated at approximately 100,000 in 1994 (House of Commons Committee of Public Accounts, 1994). This was despite an increase of over 20,000 to 188,766 in the year to June 1994 (Data Protection Registrar, 1994). Since the Data Protection Commissioner's budget is so limited that he cannot afford to undertake educational work (DPC, 1997) enforcing universal registration would merely make the legislation unworkable. The fact that compulsory registration is restricted to only certain types of personal data and certain types of data controller means that it is precisely those areas of sensitivity as defined by the European Convention, with the addition of financial data which are the major categories covered. This means that the Data Protection Commissioner's duties are particularly concentrated on the most sensitive information, though the main provisions of the Act itself (such as the data protection principles) apply to all personal data held.

Despite the more limited register than that held in the United Kingdom the Act thus provides comprehensive protection and adheres very closely to the Convention. The law is thus in close harmony with other European jurisdictions. Once the European Directive (1995) is enacted into Irish law the degree of coherence with Europe will increase. So too will the degree of protection in Ireland since this Directive incorporates a number of additional refinements worked out by various European legislatures over the course of a decade of data protection, as well as incorporating protection of manual records.

The Irish Freedom of Information Act (1997) is quite a recent innovation, which has been hailed as finally stripping much of the veil of secrecy which shrouded Irish government operations for so long. As well as granting general freedom of information to public records and documents (under certain restrictions) it also forms a substantial reinforcement

to the DPA since it also gives individuals rights of access to information held concerning them. This information extends not only to digital information, and to straightforward records in paper form, but also to information as to why decisions concerning them were made. This not only aids the democratic process by making decision-making more transparent but also grants power to the individual. Under such legislation the individual's right to know what is held about him/her gives them some power in their dealings with government. It additionally supplements data protection legislation by extending one part of the rights under data protection to manual records in public hands, before the European Directive was enforced. The second aspect of privacy protection in regard to data in this Act is also significant. Section 28 of the Act provides for the refusal to grant access to personal information if it does not refer to the person requesting the information without the written permission of the subject. The exceptions include:

- Situations where the information is effectively public anyway;
- Disclosure is vital to the health or life of somebody;
- Certain health or medical criteria are met (Subsections 3, 4);
- The public interest is better served by granting the request than by protecting the privacy of the individual;
- It is beneficial to the individual data subject;
- In certain cases when the individual is dead;
- Applicants are parents or legal guardians.

The decision in such cases is left entirely up to the discretion of the head of the public body in question. While this Section of the Act is one of many that dilute the effect the Act could have in achieving the open government that is its aim, it is a valuable protection of privacy. However, the fact that the decision is entirely in the hands of the 'head' in such cases gives such persons a large measure of power to decide on how far privacy protection should extend. This is particularly the case with regard to the clause that "in the opinion of the head concerned, on balance-the public interest that the request should be granted outweighs the public interest that the right to privacy of the individual to whom the individual relates should be upheld" (FOIA, 1997: 39 - Section 28-6-a). The freedom accorded under the legislation to the 'head' to decide on the balance between the public interest and the right of the individual could potentially create inconsistencies in the protection of privacy. It is to be hoped that civil service procedure will clarify this matter to maintain consistency of treatment by public bodies.

The overall picture that emerges from any analysis of the legal situation is that privacy is not a very clearly developed concept in Irish law. While the right to privacy is explicitly recognised as a concept in some legislation (such as the FOIA and DPA), and by the Law Reform Commission, it does not exist in any comprehensive sense. Similarly to the US Bill of Rights the Irish constitution sets out a variety of rights which it guarantees its citizens that does not include privacy as such. Unlike the US where a strong right to privacy has been derived by judgements from at least three of the other rights, Ireland has only produced a few case law precedents reflecting on privacy, and these are fragmented just as is the case with privacy-related legislation.

in the 'MarketPlace' Households' part of the pro

The most comprehensive Act of parliament designed to protect an aspect of privacy of the ordinary individual is the Data Protection Act. This has its origins, as has been seen in Chapter Five, in European legal agreements, rather than domestic concern for privacy in the information society. Indeed the only other specifically computer related legislation, the Criminal Damage Act (1991), is flawed enough to suggest that the Irish government does not treat the area of regulation of the computer industry and computer use very seriously. It has also been suggested by legal experts that the origins of the Data Protection legislation are commercial rather than rights-based (McMahon and Binchy, 1990). Though the authors do not specifically explain this contention it can be surmised that the damage to Irish-based companies that would be caused by Irish failure to harmonise its legislation with other European countries is what is meant. The potential that public confidence would have been low and that people might refuse to volunteer information when needed is also a lesser possibility. In regard to Freedom of Information the situation is similar. For a long time the country had a very secretive civil service protected by the Official Secrets Act. Considerable efforts needed to be exerted to pass the FOIA, and despite this it was substantially watered down during its passage from Bill to Act.

# 8.5 A Comparison of Data Protection for GI in Ireland and the US

The case of Lotus MarketPlace was discussed earlier in Chapter Two. This case not only shows the way in which pressure can alter the actions of a major corporation, and an early

example of the use of the Internet for such purposes (Gurak, 1997), it was also an example of the collection a large database of sensitive personal GI. The name of the product emphasises the importance of the geographical element through stressing the term 'Place' just as much as 'Market'. The most significant thing about the collection of this information and its compilation into a saleable CD-ROM is that though the product was withdrawn it was entirely legal to create it and similar databases are held by many companies (Onsrud, 1994). While such databases do not tend to contain names this information can be derived through linking the database with other information sources such as a digital version of the phone directory. Table 8.3 shows the information available in the 'MarketPlace: Households' part of the product

Table 8.3: Perso	nal Data Held	in Lotus	MarketPlace
------------------	---------------	----------	-------------

Names	Marital Status
Addresses	Shopping Preferences ('for over 100 products')
Gender	Estimated Income Levels
Age	cases. One result is that by 1995 "80 percent of America

(Source: Spinello, 1997)

The main legislation that affects such things in the United States is very different from that in Europe. There is no equivalent to data protection legislation. The US has chosen to allow industry self-regulation in such matters for the private sector. This is a factor that has caused friction with the EU as EU Directive 95/46/EC will thus prohibit information flows from EU states to the US as it lacks suitable protection. While there is no directly corresponding legislation to data protection the Privacy Act of 1974 does impose limitations on the use of federal data on individuals. The Act was introduced to prevent 'data trawling' by federal agencies seeking to match different items of information to discern inconsistencies that could point to illegal activity (Onsrud *et al.*, 1994). The limitations imposed are broadly the same as the data protection principles espoused in Europe such as relevancy, consent, subject access and the right to amendment (Mason, 1995). Thus there is effectively a two-tier system in the US whereby the Federal Government is constrained by the equivalent of data protection while the private sector is not.

The United States equivalent of the Irish FOIA is Freedom of Information legislation introduced in 1966. This legislation though much older has broadly similar aims and

general operation. One difference is, however, in the degree to which freedom of information operates. While there are restrictions (the act was amended in 1974 to define such exemptions) the act "establishes a presumption that records in the possession of executive-branch agencies and departments are accessible" and requires "government to provide the fullest possible disclosure of information requested by the public" (Mason, 1995: 247, 248). Similar freedom of information legislation has also been passed by many state legislatures. The contrast with the Irish case is quite noticeable. While the US law is over thirty years old the Irish Act only came into operation in 1998 (although enacted in 1997). Similarly the degree of openness appears to be quite different: the Irish law has been said to be much less than was hoped. This has many impacts. One of particular relevance to those using GI is that while American government GI is available for the cost of reproduction Irish (and British) GI is copyrighted and costly. From the point of view of privacy, however, the more restrictive Irish legislation does have a positive impact. Whereas in the US it is possible to obtain personal information from government agencies, as evidenced by the list in Table 8.4, this is specifically ruled out in the Irish case except for certain very limited cases. One result is that by 1995 "80 percent of Americans believed they had lost all control over personal information" (Strum et al., 1998: 196).

Source	Information		
Drivers Licence Information	Name, address, height, weight		
Photo	Scanned image		
Census Bureau	ZIP+4 address location		
Local Government	Cadastral, taxation & facilities records		
Retail Outlets	Scanned bar-code purchases		
Commercial Sector	Social security number		
Other Databases	Magazine subscriptions, gasoline purchases, and other purchases.		

Table 8.4: Perso	al Information	Legally	Available	e in	USA
------------------	----------------	---------	-----------	------	-----

Source: Onsrud, 1994.

The contrasting combinations of US Privacy Act and FOIA and Irish Data Protection Act and FOIA are very significant in regard to the question of privacy and the examples raised above. Although the US has been the world leader in IT, and most developments that occurred there do occur here, the examples of Lotus and Equifax would be illegal here. The contrast could not be greater. While the US has a similar protection against the 'Big Brother' state from the Privacy Act as Ireland does through the DPA, there is no similar regulation of other bodies, which can collect and collate any information available. The FOIA aids this process by allowing them to include government as well as private sector information. By contrast in Ireland information can only be obtained from other organisations if such organisations have informed the subject and obtained permission for the transfer, regardless of whether organisations are public or private sector. In addition the Irish FOIA specifically prohibits the giving out of private information. Thus the collation of the types of databases described above would be completely illegal in Ireland. In addition the particular cases of credit referencing and direct marketing data are specifically addressed in the Act. These agencies are among those specifically required to register and thus come under the scrutiny of the Commissioner.

information in order to function efficiently. By extension in such

The difference in the degree of protection thus is enormous and is an indication that whatever the shortcomings of Irish law, and that regardless of the tardiness of implementation of new law, Ireland has quite a high degree of legal protection of private data from misuse in comparison to many other jurisdictions.

## 8.6 Privacy and Power

Three major theories of power were examined in Chapter Four, each of which concentrated chiefly on the use of information as an instrument of power. While they differed in focus they all assumed that information was such an instrument, and that it had through time served various interests. The theoretical ideas of Schiller and Giddens approached the problem from the perspective of the exercise of power from the top down. In contrast Foucault's ideas of Panopticism and Confession focused on the actual mechanics of the operation of power at an individual level, as well as suggesting that power was not exercised in a completely top down fashion.

Although Schiller and Giddens differ largely on their respective emphasis of state and capital as the institution exercising power, both see the use of information as being a method of imposition of control in the interests of the institution concerned. Schiller, and other commentators such as Chomsky, concentrates on the use of information (in all its forms) as a servant of capital. They are thus concerned with the flow of information to people as well as from them and highlight issues such as information deprivation and the role of the media in controlling people's access to information. They also suggest that the capital accumulation of personal information is an element in the maintenance of capitalist hegemony. Giddens focus on the state is, by contrast, highly focused on the issue of surveillance and the gathering of individual information. This he largely sees as a part of a wider process of state consolidation of power and of the development of a capacity for violence. In order to survive in a world of competing states each one must possess similar abilities. This necessitates highly organised bureaucratic states with a strong emphasis on the collection of records on individuals to permit efficiency of organisation. The focus of these two theoretical stances is different. One stresses the use of information about individuals as a tool of capitalism, ensuring its hegemony, and operating in part through the (capitalist) state. The other stresses the organised modern bureaucratic state's need for information in order to function efficiently. By extension in such a society corporate interests are also served by the collection of information to increase their operational efficiency. The two thus provide explanations of the reasons for the collection of personal information that differ in focus: on the one hand capitalism and on the other the nationstate.

The two do have common ground, however:

- Both acknowledge the great importance of personal information and its collection to the exercise of power;
- Both agree that there is a close relationship between the nation-state and capitalism;
- Both see the control of personal information as being important both to the efficiency of operation of state and private sector, and important in influencing the behaviour of the individual.

Foucault takes a different approach to the issue. His focus is on the individual under scrutiny.

According to his work there are two related methods by which information is extracted and used to exert power over the individual:

• The panoptic methodology involves placing the individual into a situation where they are watched, or potentially watched and know it; in effect they are in a situation where personal information is collected by the watcher;

• The confessional methodology uses the historically developed willingness to reveal information on the part of the individual to collect such information.

These two sources of personal information operate within a network of power relations. According to Foucault power is not a top-down process but operates at every level of interaction within society. Power is thus a network of interactions. This means that though it tends to serve dominant interests, and though interactions tend to be unequally balanced, there is some potential for resistance. It also means, however, that the individual participates in the exercise of power through this network. Thus, in the case of Irish GI collection by state and private sector bodies the individual theoretically participates in his/her insertion into a panoptic mechanism of surveillance by actively 'confessing' information to the organisations concerned. In consequence, the individual is fully aware of the fact that information is being collected and must therefore behave accordingly, if necessary modifying behaviour, and thus becomes the object of manipulation, the object of power. This theory of how power operates on the individual through the extraction of information is very important to this study of privacy since it is the removal of privacy that allows it. It is also in agreement with one of the chief theories regarding the importance of privacy. This theory values privacy precisely because it removes the individual from social scrutiny and thus enables autonomy and freedom, including the freedom to develop and express non-conformist thought and behaviour patterns.

## 8.6.1 Power and the Privacy of GI

potential to give different answers to diff

Ireland is a chiefly capitalist nation-state in which both public and private sector are involved in the collection of personal information, with this tendency increasing as information technology becomes more pervasive. Therefore, to some degree the contentions of both Schiller and Giddens can be seen to be true. Capitalist organisations do collect personal information, and use it to increase their efficiency and thus increase profits. The state also has a role to play in facilitating capital in Ireland as is evidenced among other things by its implementation of the Data Protection Act, 1988 in response to commercial rather than privacy concerns (McMahon and Binchy, 1990). It is also clear that the state is perhaps still one of the largest collectors of information and that this information is largely collected for bureaucratic needs, chiefly efficiency of operation of government. In this context both Schiller's and Giddens' ideas do reflect reality. The mechanism of collection of information can clearly be interpreted in the light of Foucault's confessional ideas since the source of the information is the data subject him/herself in all but four cases. It is also clear that one potential effect of this collection of information is the creation of a panoptic mindset. The information that is known to any given authority is known to the individual and the individual must thus ensure appropriate behaviour, or risk censure which could involve negative impacts such as the withdrawal of service by the institution. This is often the purpose of the collection of information in the first place as in the case of fraud prevention. This is accomplished either through having enough information on the individual to cause them to avoid such unapproved practices or sufficient information to warn the institution in advance of its likelihood.

There are ways in which these modes of operation of power are curbed, however. The first is the legislative curbs on the use of such data, equally binding on public and private sector. The second is the voluntary curbs imposed by the organisations themselves for internal organisational purposes. These combine to limit the power uses of information. In addition the fact that information is in general collected not simply to manipulate behaviour but to serve internal administrative needs is significant. Also important is the fact that though a great deal of information is collected it is not shared, for legal and other reasons. This in effect means that a fully panoptic mechanism cannot operate: though information may be constantly collected, and though 'visibility' may be very great the potential to give different answers to different institutions still exists. In effect, unlike the Panopticon where true information is given whether this is desired or not, the ability to lie prevents this from happening with regard to confessed information.

Despite these curbs on the power of information through legislative and other administrative concerns, the potential power of personal GI is great. One of the key characteristics of the Panopticon itself was its "analytical arrangement of space" (Foucault, 1979: 203). The same is true with panopticism in general: it is a "type of location of bodies in space" (Foucault, 1979: 205).

Thus GI can be seen to be central to the operation of Foucault's power model which is in its essence based on the recording of geographical information regarding the individual. The power of modern digital GI has already been discussed in some detail but it is important to note this clear connection between the recording of personal GI and this particular theory. In effect this draws together GI, privacy and power as concepts. The recording and collation of personal GI is not only a potential invasion of privacy, but is also a method of exerting power over the person. Knowing that the information is being collected, and knowing that it is being shared can create a situation in which the individual's behaviour is altered to avoid drawing adverse attention from what is in effect an observer. In this context the great power of modern GI to link information of a personal nature on the basis of a spatial characteristic is of central importance. Under normal circumstances a database can link personal data from a variety of sources. In general the only potential problem in accomplishing this is the selection of the item of data with which to conduct the linkage. Common names, for example, may be duplicated many times even within the same locality, while the potential to use different versions of the same name is also a problem. The solution in most cases is the use of a unique identifying number such as the PPS number that refers to only one individual. However, the use of the address is also a very reliable method of matching records.

In addition such a geocoded address can be used, not only to link a person's information, but also to perform spatial analysis, and to effectively pin the individual's details to the map. In effect personal GI thus allow the 'location of bodies in space' for those possessing the data in the same way as architecture does for the warder in the Panopticon. One difference is, however, that the warder in the prison, although unseen occupies the same space whereas the analyst may remain not only anonymous but also distant in space. Foucault describes the ideal situation where power can operate as being where the individual is 'visible' and 'individualised', and where power is also 'visible but unverifiable'. In terms of these principles of the panoptic mechanism, the potential is for the agent using the GI to be completely unverifiable through the use of technological means. However, the data protection principle of access means that the operation of power, in terms of the way in which information is held and used, is open to the individual. If the individual chooses to s/he can exercise a legal right to know what information is held and why, and if it is not accurate and up to date, or if it is more than is necessary to carry out the 'legal' function for which they were collected. Data protection legislation is thus central to the redressing of the power balance in favour of the individual, and permitting him/her to verify whether, and how, personal information is being used against his/her interests.

In regard to the other principles of the panoptic mechanism and personal GI there is a strong element of congruence. When personal GI is collected the data protection

legislation ensures that it is visibly collected under the 'fair obtaining' principle. By being collected it in turn renders its subject 'visible' to the gaze of the organisation which has collected it. There is also an element of individualisation involved since the collection of information in the Information Society is individual and records are maintained individually. Although a person may take refuge in the general population, their record is always individual by definition, and anything attached to it will only ever relate to them. This serves to isolate the individual to some degree as it is impossible to completely hide in the population.

In effect, thus, personal GI, in combination with the technology to manipulate it does create the possibility of a spatial panopticon (Curry, 1994). In effect the main element preventing this is the data protection legislation which swings the balance of power back to some degree in favour of the individual, although implemented as much to protect business as the individual.

However, as has been seen, there is a strong body of opinion in Irish civil service circles that feels that in the interests of greater efficiency the linking of information within the civil service should be possible without the need to inform the subject. This would rely on the expanded use of the PPS number and the social services card, and also on the direct transfer of information within an integrated social services system. In effect the result would be to make verification more difficult. Although data protection legislation would still mean a right of access for the individual the suppression of the fair obtaining principle would mean that the individual would not be aware of what data were held where and by whom. This knowledge would of necessity make the exercise of the 'access right' difficult. In addition the possibility that information would be being used for a purpose unsuspected by the individual at the time of supplying the information would be far greater.

A final point of relevance is to note that GI is not collected in isolation. In the current Information Society the collection of information has become an end in itself, since such information is a valuable commodity. Inevitably the collection and use of personal GI is only one aspect of the overall collection of personal information. The Law Reform Commission notes, for example, the increasing use of surveillance cameras in public areas (LRC, 1998). The use of cookies on the Internet to 'track' the movements of people in cyberspace has recently become a worry for privacy advocates, and also echoes the collection of information on activities in real space (through Geographical Information). Thus, although the use of personal GI in Ireland appears to be well regulated by law and practice, it is only one type of information in a wider Information Society. The existence of such diverse types of observation both through personal data and more direct methods such as the use of CCTV in effect can create the effect of the Panopticon using information. To do this it is not necessary that the information actually be linked together. It is sufficient that it is collected and used. Even if diverse power interests are using information separately the effect on the ordinary person is one of pervasive observation.

However, since one of the chief characteristics of the Information Society is the integration of diverse types of information, such varied information may be linked, ultimately creating more unified surveillance. It is possible for personal GI to be linked with other information and thus cause a privacy or data protection problem, even when none was caused by the information when held separately. In regard to the question of the use of information to exert power over the individual this could create a far more effective Information Panopticon than that created by more fragmented means. In effect the panoptic mechanism of surveillance through information would then be far more closely analogous to the original Panopticon itself. If, for example, it were possible to link personal GI to even some of the following, the real world could act just as effectively as a mechanism of observation and discipline as the backlit cells in the Panopticon:

- Other personal information held in databases;
- The intercepted contents of email;
- Internet use determined from cookies;
- Movements recorded by tracking a mobile phone signal;
- Movements recorded from digital analysis of surveillance camera images;
- Intercepted telephone calls.

The importance of such issues can be gauged from the controversy generated by the US government's insistence on the use of the Clipper Chip which would allow law enforcement agencies access to all encrypted private messages on the Internet (Gurak, 1997). Although such a scenario of information linkage may seem far-fetched, the basis of the power of IT is in its ability to generate, link and use information which can then potentially be used if access is gained to it. For example, the Law Reform Commission in listing the currently available surveillance technology describe "an interactive link between surveillance technology and computerised data banks (CCTV surveillance networks). This

will potentially allow for automatic tracking of the movements of individuals" (LRC, 1998: 6). In effect this allows the direct creation of personal GI on the movements of an individual from surveillance camera footage recorded digitally and subjected to 'Face Recognition' software. There is, thus, also a potential that methods of observation that are traditionally considered non-digital, and non-GI could become both.

8.7 Conclusions

GI and related analysis technology forms one element in a broader range of technological developments that potentially threaten privacy. Privacy is, however, a difficult concept to define and therefore difficult to protect legally. Ireland lacks comprehensive protection although it does have a data protection statute that is comparable to any in Europe, and through it achieves a high level of protection of privacy with respect to GI. However, this Act had its genesis outside of Ireland and the government, as well as attempting to undermine its operation, has been slow to enact its replacement. However, a number of factors have combined to supplement the operation of the Act as a means of protection of privacy including traditions of secrecy and confidentiality in the organisations that collect GI, and fragmentation of the storage and use of such GI for technical reasons. The combination of practice, law and this fragmentation has meant that up until this time privacy in relation to GI has been well protected, in comparison to the United States, for example. However, recent technical and data developments both within Ireland and in the wider fields of GI and IT are likely to undermine this situation. In addition the integration of GI into the wider IT community provides the potential to link GI with other forms of information and thus to compromise privacy further. In effect it is possible to monitor the activities and movements of an individual with relative ease. This has several consequences not only for the given individual, but also for society.

Two of the most important characteristics of privacy are, according to the literature, its centrality to self-development of the individual personality and its importance to the exercise of freedom in a democratic society. One of the features of modern democracies is, according to Strum *et al.* (1998), their freedom from the 'social shame', which is used in other societies to force people to conform with social norms, because of privacy. The potential of the digital revolution to effectively return the element of social shame is of necessity a matter of some concern. Even more importantly the fact that such social pressure will be exerted from afar by unseen observers raises the potential that modern

diminishment of privacy will even more powerfully affect the individual than the social shame of peer observation in traditional societies. An important difference is the inability of the observed to observe the observer in turn and subject him/her to similar pressure. In effect modern technology alters this power balance in favour of the observer, potentially creating what Foucault calls the 'disciplinary mechanism'. One important characteristic of data protection and other privacy legislation is that it limits the degree to which this can happen. In effect such legislation redresses the balance somewhat by giving the individual the right to examine the activities of the organisation that collects and uses personal data, and the right to force such an organisation to delete information if it is not lawfully used.

The final chapter will summarise the findings of this study, and make recommendations for future research and further study.

Although privacy is a right which is much debated there is general agreement that it represents something fundamentally important to barries hit. Concerns at the effect on privacy of developments in IT, which had being the smassing of large databases of private information led to a variety of keyblactic dispersion. From the 1974 Privacy Act in the USA, to Directive 95-to EC of the European Communication. Such legislative responses strive to strike a balance between the mode (non-arrive and otherwise) of information users and the wishes and rights of the response of antice private.

In regard to the related serves of onlyant and data planation, two impacts of the digital fevelution on GI are particularly in posture.

- It has increased its practical power by many embors of magnitude by enabling the analysis and combination of detected the level of the individual address, and thus effectively of the individual
- In addition it has made the use of GI potentially more detrocratic since recent developments integrating GI technology into the wider realm of IT make spatial analysis available to the wider comments of computer users.

Chapter Nine Conclusions and Recommendations 9.1 Background

Privacy has been an area of ethical and legal concern in regard to computers since the early 1970s. At that time concern was chiefly focused on the collection, use and linking of government data by intrusive public bodies. As technology changed in the following decades, the potential to infringe privacy has expanded beyond the realms of large public sector organisations with substantial resources, and is now available to many organisations provided they have the data, a relatively insignificant obstacle given the current levels of information collection.

Although privacy is a right which is much debated there is general agreement that it represents something fundamentally important to human life. Concerns at the effect on privacy of developments in IT, particularly the amassing of large databases of private information led to a variety of legislative responses, from the 1974 Privacy Act in the USA, to Directive 95/46/EC of the European Commission. Such legislative responses strive to strike a balance between the needs (economic and otherwise) of information users and the wishes and rights of the subjects of such information.

In regard to the related issues of privacy and data protection, two impacts of the digital revolution on GI are particularly important:

- It has increased its practical power by many orders of magnitude by enabling the . analysis and combination of data at the level of the individual address, and thus effectively of the individual.
- In addition it has made the use of GI potentially more democratic since recent developments integrating GI technology into the wider realm of IT make spatial analysis available to the wider community of computer users.

One effect of these developments has been the increased potential for digital GI to be used to infringe privacy. Though personal data has long been collected on an individual basis linked to address, this has not been easily subjected to analysis as GI in the past. New developments in the geocoding of addresses, coupled with the wider availability of data and the spatial tools available for normal databases, have made such individual addresses amenable to sophisticated analysis as GI. Thus information collected and stored in conventional databases must now be seen as GI if it includes an address. Therefore almost any personal information is GI since almost all collection of GI includes the recording of an address. The combination of these two factors, the use of specialist spatial analysis with the ability to use almost any personal information stored on computer, takes the potential to infringe privacy to a new level.

It is against this background that this study examined the issues of privacy, surveillance and data protection, the connections between information and power, and the position in Ireland with regard to privacy and GI. The interview survey method was used to determine the practical impacts of these concepts in Irish organisations.

# 9.2 Summary of Findings

This study had it s practical focus in the examination of the state of play in Ireland in the late twentieth century with regard to digital GI from a legal and practical point of view. However, the study also looked at complex issues such as the importance of privacy for free democratic societies and the potential use of surveillance and the observation of individuals as a method of regulating their behaviour to obtain docile compliance with whatever was desired by those conducting such observation. As such the study has two sets of results, those focused solely and narrowly on the particular Irish situation, and those which examine the important debates and ideas surrounding the privacy issue.

# **Findings: the Irish Situation**

In the purely Irish context it was found that although legal protection of privacy reflected the wider debate in being weak and fragmented the law of Data Protection was strong and comparable to other such legislation due to it s non-native origins in the Council of Europe. This outside origin and the delay in implementation of Directive 95/46/EC, coupled with civil service attempts to lessen the effectiveness of the DPA, particularly in regard to the question of the PPS number, are a matter of concern since they appear to suggest that civil rights in the information age are of secondary importance to the Irish government compared to the organisational needs of government and business.

At the same time a number of changes in the Irish technological milieu are creating far greater potential for digital information, and particularly GI, to be used to infringe privacy and to monitor the individual. Such developments include specifically Irish GI-focused developments such as the development of national geo-coded address databases, wider technological change with regard to GI bringing it into the arena of 'ordinary' digital information not requiring specialist software, and the integration of systems and in some cases sharing of data for organisational purposes.

Such changes underline the fact that although privacy was found to be relatively well protected up until now in regard to Irish information this was largely due to a combination of serendipity (fragmented systems) and organisational needs (for secrecy and commercial advantage), rather than to the action of the DPA and concern for civil rights. These developments also come against a background of information being collected in ever-increasing amounts by a greater variety of organisations, and of increasing internationalisation of information flows which make it potentially more difficult for the under-funded DPC to police the actions of those holding data on Irish citizens.

#### Findings: Privacy, Surveillance, Information and Power

Although the exact nature of privacy is contested and it s very existence as a separate entity is denied by some commentators, it s importance is nonetheless widely acknowledged, particularly in democratic societies. Its status as a right under the UDHR, despite the lack of a clear definition, means that it s existence and common human importance is acknowledged by all signatory states and thus giving it an effective independent existence regardless of disagreements concerning its exact nature and methods of protecting it. In relation to the specific privacy impacts of IT concern has been substantial and has led to the enactment of legislation (mentioned above), particularly in Europe, to counteract the ill effects of IT while permitting the continued collection of private information.

Theorists have focused on issues of information and power of concern to many, particularly in light of changing information practices in the Information Society. The

work of such theorists as Giddens and Schiller focuses on the power of information, economically and politically and on the way in which this power is wielded by two respective power blocs: state and capital. Foucault in contrast focuses more on the mechanism by which power is exercised over the individual through the use, or appearance of use, of information concerning him/her. In the panoptic prison constant observation was the means by which information was 'gathered' or made to seem to be gathered. Such information concerned the behaviour of the prisoner and could be used in the prison regime to bring punishment if such behaviour were not that which was desired by the prison regime. The effect was that observation or its simulation resulted in the disciplining of the prisoner (or person in other institutions such as the factory) who avoided such actions as would draw censure from the observer.

As the modern world has become more and more information-focused it has come to resemble the panoptic mechanism in its wider sense, as described by Foucault (1979), existing in institutions of society. The modern Information Society is one of both direct observation, such as that practised in the Panopticon, and of indirect observation through the collection and analysis of information. This latter is facilitated by the confessional mechanism, described by Foucault (1990) as another aid to discipline, which encourages people to openly volunteer information and thus enables the collection of such information without the necessity of obtaining it forcefully. Both methods derive their effectiveness from their openness. Neither involves any direct coercion or imposition on the individual, instead placing the individual into the network of power that operates around, on and also through him/her.

The combination of the two techniques is by no means unique to the Information Society and examples of the use of such combinations of direct observation and information recording and analysis are to be found in both *Discipline and Punish* and *The History of Sexuality*. While the latter work provides descriptions of the use of volunteered information in institutions where direct observation was also a tool, the case of the plague town in the former provides the most clear example of an early Information Society. In this situation total control of the populace was achieved by a constant direct monitoring of their physical whereabouts and activities, combined with comprehensive collecting and recording of information on each individual. This was only possible in a pre-digital age in an extreme situation (epidemic), where people were confined to their homes and thus both largely individualised and easily monitored. The Information Society involves the routine
collection and analysis of information on individuals, as well as their routine observation. This could potentially result in the creation of a truly spatial panoptic mechanism in the world outside the enclosed institution, without the necessity of a disaster such as plague to prompt it.

### 9.3 Conclusions

In contrast to the plague town and other earlier models of the disciplinary mechanism the Information Society is one of individualism, where confession is part of the culture, and the surrender of information is necessary to social participation. Technology, meanwhile, makes the recording and analysis of information on an individual basis relatively trivial, while also allowing considerable and growing levels of direct observation, particularly outside of protected private spaces such as the home (although this can also be monitored). The particular techniques associated with geographical analysis make it a relatively trivial matter to link and analyse individual information to build up highly-detailed, constantly-updated characterisations of people and their activities in space. Such characterisations may also potentially be linked with the results of more direct observation, also carried out through the medium of digital recording devices.

In the face of such developments jurisdictions such as Ireland have enacted legislation to ensure a certain minimum protection for personal information held digitally. However, the Irish study revealed quite clearly that the protection of privacy owed more to organisational needs than to legislation. In addition, it is clear that while such legislation may be useful and effective its underlying motive may be something other than the desire to protect individual rights and freedoms, such as the desire to protect business interests in this case. Even where such legislation exists moreover, its effectiveness may be curtailed as in the Irish case by a lack of awareness among the public, while the actual power of national legislation to protect the individual in a world of international flows of large volumes of information is questionable.

The potential to create a complete disciplinary society now exists or is coming into existence, and personal GI is a keystone of this process. At the moment observation functions widely, generally being conducted for the purposes of organisational efficiency in dealing with the public. This stems partly from the desire to ensure that an organisation

takes no risks in beginning to deal with a member of the public, and partly to encourage good behaviour later. While the gaze is not quite as unceasing as in the Panopticon (people possess a greater degree of freedom from observation when in the home, for example, than on the street, but even there information may be collected quite frequently), nor is that gaze embodied in watchers all working for one institution, the gaze is becoming a normal fact of life. Whether the fragmentation of the gaze will have an effect in allowing space to individuals for non-compliance, or whether a whole series of sub-gazes will impose discipline (perhaps with sometimes contradictory results) on people, remains to be seen. It will depend on public perception of the way in which information is used: if it is felt that information is shared it may well have the same unified disciplinary impact as the gaze from the central tower of the panopticon.

One further important issue raised by Foucault's work is the nature of resistance within a disciplinary network of forces. As was mentioned above, the individual is central to the operation of power in this model. Foucault (1979) makes it clear that although the individual is at a disadvantage in this network of power relations, it is not the hopeless situation prevalent in the top-down models associated with state or capital imposition of discipline. For Foucault the disciplinary network allows the watchers to be watched also, and also presumes that, although there may be an effective status quo, there is always room for resistance to the disciplinary imperative. The network of power is thus also a network of struggle where the individual may be weaker than other actors in the network, but has the ability to resist and thus to force changes in the network.

In the context of these ideas data protection legislation takes on new significance since it may well be a concession to such forces of resistance and the fear that they would damage international trade. As a concession, moreover, it is of great significance since it gives the right of access to the information held to the weakest individual in the network, allowing the observation of the observer's actions at least as they impact on the individual being observed. In addition, the terms of data protection legislation which prevent unauthorised sharing of information prevent the gaze from becoming truly panoptic: rather than one central tower it is as though there are many smaller towers each populated by people watching for slightly different things.

Thus two central factors can be seen to be crucial to future developments: public attitudes and the actual purposes of the more powerful information collectors and users. The importance of the former is based on the continuing necessity that a lot of information be collected from willing data subjects while the latter will determine whether efforts will be made to unite the gaze of the various observers.

# 9.4 Recommendations and Further Research

#### 9.4.1 Recommendations

#### The Irish Situation

In regard to the situation currently existing in Ireland a number of simple recommendations could serve to substantially improve substantially improve the protection of privacy and to clarify the specific dangers facing the privacy of Irish people.

- The implementation of the European Data Protection Directive, substantially overdue at time of writing, should be effected as soon as possible. In regard to data protection the strengthening of the DPC's office through the provision of better funding is also to be desired. One of the most fundamental problems of the current system is that it requires public knowledge of the Act to stimulate complaints and thus lead to investigations. However, the lack of funding for the DPC has resulted in a very low priority being given to education which has had a detrimental effect on public awareness of the Act as demonstrated by the Commissioner's survey in 1997 (DPC, 1998).
- The development of a comprehensive law of privacy defining the nature of privacy and its importance for Ireland also seems vital as a supplement to the action of data protection legislation. In an era of rapid technological change even technology-based law may quickly become outdated and fail to meet the needs of the moment. In such cases where data protection legislation is found to be inadequate a clear legislative commitment to and support of privacy would provide a framework for the guidance of legal decisions in the absence of legislation or precedent covering a particular case.
- The development of a code of practice by the GI industry in Ireland, overseen by IRLOGI, would not only raise ethical and privacy awareness within the industry and provide clear standards, but also would be beneficial to the industry through its effect of encouraging public trust.
- Most importantly of all, however, it is vital that Irish public awareness of the issues needs to be raised. This extends to knowledge of rights under the DPA, and of the

types of information which are being collected and used, and the purposes for which they are being used, as well as by whom. Without such awareness the DPA itself is useless since it relies on individual knowledge of rights, and on individual complaints. In addition, it is impossible to exercise any attempt to resist attempts to discipline without understanding how the disciplinary mechanism works, and what it is attempting to achieve.

#### General Recommendations

Outside of the purely Irish situation the same challenges are facing people with regard to protecting their privacy and thus their independence of action. In this regard the only recommendation which can have validity is that people be aware of the threats to their privacy and of attempts to enclose them in a disciplinary mechanism, and do all that is possible to protect their privacy and neutralise such discipline.

It is clear from the work of Foucault that the perceptions of those under observation are vital to the working of a disciplinary mechanism. This is particularly the case in the current situation where a substantial amount of observation is conducted indirectly through the linking of information which is either volunteered or indirectly granted (as is the case with the tracking of Internet activity, for example). Such activity depends on favourable or indifferent public attitudes, or on ignorance of what exactly is being collected and why, coupled with a culture of confession, to allow it to occur.

Practical general recommendations for those who wish to avoid a disciplinary society naturally arise from these points:

- The strengthening as much as practical of data protection legislation in all jurisdictions and the formation of international agreements to prevent the removal of information to protection-less states merely to avoid breaking the law in the relevant jurisdiction. The EU Directive on Data Protection takes this approach.
- The education of the public in the exact nature of data protection, where it exists, and the rights granted to them under it. This should be coupled with a commitment to strong data protection enforcement bodies with an active mandate to investigate cases and situations, rather than having to wait for complaints. Public education should also comprehensively inform them of the power of the technology and the uses to which even seemingly innocent information can be put.

Recommendations applicable on a personal level concern the willingness with which people abandon privacy, and the culture of confession. People should be far more vigilant and suspicious in regard to the surrender of personal information. While it is almost impossible to live in modern society while maintaining an information blackout, the culture of confession to which people tend to belong enables organisations to collect information with ease. This in turn has the potential to stifle resistance to discipline since the individual is collaborating to more firmly entrench him/herself in the disciplinary network. However, the fact of being part of the network gives the individual the power to resist the imposition of discipline and to exercise individual power to alter it. To do this, however, it is vital that the individual be informed and that he/she maintain as tight a control as possible over personal information.

Sensible precautions to be taken by any individual include:

- making oneself aware of the data protection legislation if it exists
- determining the nature and extent of information held on oneself and the information which is potentially added to the 'volunteered' information within an organisation's system, and the new information which can potentially be derived by manipulation
  - the avoidance of voluntarily giving out information except when vital the protection of information one holds in a digital medium oneself, and of communications across networks through the use of secure encryption

In addition, attempts to achieve such goals as the introduction of national identity card schemes and universal identification numbers need to be carefully considered and justified. Where such schemes are introduced they should only be accepted after clear and informed public debate and clear decisions need to be made regarding who has the right to use them.

9.4.2 Recommendations for Further Research

One of the primary problems with the research conducted in this study was it s focus on the security and organisational aspects of information storage and use in Ireland. While such issues are vital to the issues of privacy and data protection in Ireland or any other jurisdiction, there are other issues of even more importance, particularly in view of the issues raised in Chapters Three and Four.

As mentioned above, public willingness to permit information collection is vital to the Information Society. The potential to use information to create a disciplinary mechanism depends on the possession of such information and the ability to constantly update it. If the disciplinary mechanism is to be truly effective such information cannot be collected by force but must be volunteered so that the mechanism can maintain the lightness which is its chief characteristic according to Foucault (1979). A vital area of future research, therefore, is that of the perception and knowledge of ordinary individuals of the information revolution, and of their reactions to the collection and use of information concerning themselves. Such research could be relatively easily pursued using a questionnaire survey, structured interview or focus groups depending on the aspects of the issue to be studied. Simple questionnaire survey to a large sample group, for example, would enable the discovery of the basic attitudes and understanding of the population at large. This could be followed up by more detailed examination of the issues raised using focus groups which could include, among others, civil liberties activists, computer specialists and lawyers.

In conducting such a survey some of the important issues to be examined are:

- groups the willingness of people to donate information and whether any information is less likely to be surrendered than other information;
  - the types of information felt to be most sensitive and whether they are more closely guarded in consequence;
  - public understanding of the ways in which such information can be used and the potential to create linkages between data sets;
  - public awareness (or lack thereof) of the potential to incrementally build up highly detailed databases through the compilation and analysis of (often trivial) information from different sources, and of the potential for publicly available, state collected data to enable this;
  - public knowledge of individual rights under data protection, without which such legislation can not function.

Similarly research needs to be done on the attitudes of the collectors and manipulators of data. The Irish study undertaken revealed some hints that Irish organisations did not place

a high priority on such issues as privacy and were much more motivated by concerns for profit and efficiency. However, the study was not designed primarily to directly ascertain this information (although designed to leave latitude for such information to be revealed). What the study revealed of the attitudes of organisations, and in particular their overall lack of concern with individual rights and focus on organisational goals, means that the actual aims of organisations involved in the maintenance of databases need to be known. In particular it is vital to know what kinds of manipulation such information would undergo, organisational attitudes to privacy, and to what degree organisations wish to link their information to other datasets and why. Because of the sensitivity of such a survey and the potential for organisations to be caused public relations damage it would not be an easy study to undertake and many organisations can be expected to refuse to co-operate. However, the experience of the Irish study of the security of information, where such information was volunteered by a substantial number of interviewees, suggests that such a study is possible if sensitively conducted, although participation rates may be low, and organisations with something to hide will naturally refuse to co-operate. However, it is felt that such research could be conducted successfully judging by the willingness of some professionals to talk openly about these issues in the study conducted during this thesis. For such a study to be successful it would need to operate under a strict guarantee of anonymity, and owing to the uncertain nature of the topic concerned, which would be unamenable to questionnaire survey techniques, would best be undertaken using focus groups.

209

## BIBLIOGRAPHY

(Please note that URLs may change through time.)

#### Routledg

Ahlstrom, D. (1999) "Flashes of Brilliance That Can Change it All". *The Irish Times*, Jan. 4 1999. <a href="http://www.irish-times.com/irish-times/paper/1999/0104/fea10.htm">http://www.irish-times.com/irish-times/paper/1999/0104/fea10.htm</a>

Aldenderfer, M. and Maschner, H., eds., (1996) Anthropology, Space, and Geographic Information Systems. UK: Oxford University Press.

Alexander, P. and Gill R., eds. (1984) Utopias. London: Gerald Duckworth & Co. Ltd.

Allen, A. (1998) Exposed. *The Washington Post*, Feb. 8 1998: <http://washingtonpost.com/wp-srv/WPlate/1998-02/08/0021-020898-idx.htm>

Allen J. (1976) "Lands of Myth, Waters of Wonder: The Place of the Imagination in the History of Geographical Exploration". Lowenthal, D. and Bowden M., eds. *Geographies of the Mind: Essays in Historical Geography*. New York: Oxford University Press; 41-61.

Alpert, S. and Haynes, K. (1994) "Privacy and the Intersection of Geographical Information and Intelligent Transportation Systems". In Onsrud, H., ed., (1995) *Proceedings of the Conference on Law and Information Policy for Spatial Databases: Tempe, Arizona:* October 29-31 1994. <a href="http://www.spatial.maine.edu/tempe/tempe94.html">http://www.spatial.maine.edu/tempe/tempe94.html</a>

Als, G. (1994) "Propositions on Statistical Confidentiality". *Proceedings of the International Seminar on Statistical Confidentiality*, November 1994. Luxembourg: Office for Official Publications of the European Communities (1995), 47-51.

Ameghino, J. (1998) "Access Eye in Sky for Blind". *The Irish Times*, Feb. 9 1998. < http://www.irish-times.com/irish-times/paper/1998/0209/cmp4.htm>

Anderson, C. (1997) "Survey Electronic Commerce: In Search of a Perfect Market". *The Economist* (Net Edition), May 10 1997. <a href="http://www.economist.com/editorial/freeforall/14-9-97/index">http://www.economist.com/editorial/freeforall/14-9-97/index</a> survey.html>

Anderson, K. and Gale, F. (1992) Inventing Places: studies in cultural geography. Melbourne, Australia: Longman, Cheshire. - [New York]: Wiley, Halsted Press.

Andrews, J. (1975) *A paper landscape: the Ordnance Survey in nineteenth-century Ireland*. Oxford: Clarendon Press.

Andrews, J. (1994) *Meaning, Knowledge and Power in the Map Philosophy of J.B. Harley.* Dublin: Trinity Papers in Geography, No. 6. Department of Geography, Trinity College.

Andrews, J. (1997) Shapes of Ireland: maps and their makers 1564-1839. Dublin: Geography Publications.

Annan, K. (1998) < http://www.unhcr.ch/html/stms/sg971020.htm>

Annas, J. (1989) An Introduction to Plato's Republic. UK: Oxford University Press.

An Post and Ordnance Survey (Ireland) (1997) GeoDirectory - Geocoded National Address Directory. Presented at GIS Ireland 97, Malahide Dublin.

Appleby, H. (1998) Personal Communication.

Appleyard (1998) "God's Own Country". The Sunday Times Magazine, May 3 1998, 42-57.

Arendt, H. (1958) The human condition. [Chicago]: University of Chicago Press.

Armstrong, K. (1994) A History of God (From Abraham to the present: the 4000 year Quest for God). UK: Mandarin.

Armytage, W. (1984) "Utopias: the technological and educational dimension". Alexander, P. and Gill R., eds. *Utopias*. London: Gerald Duckworth & Co. Ltd, 85-94.

Aronowitz, S.; Martinsons, B.; Menser, M. and Rich, J. (1996) *Technoscience and Cyberculture*. New York: Routledge.

Arthur, W. (1997) How Fast is Technology Evolving? *Scientific American*, Feb. (1997. <a href="http://www.sciam.com/0297/issue/0297wonders.htm">http://www.sciam.com/0297/issue/0297wonders.htm</a>

Aspen Institute (1995) An Information Bill of Rights and Responsibilities. <a href="http://www.aspeninst.org/dir/current/IBRR2.html">http://www.aspeninst.org/dir/current/IBRR2.html</a>

Associated Press (1998a) "FTC Requests Laws on Net Privacy". USA Today, June 5 1998. <a href="http://www.usatoday.com/life/cyber/tech/ctc875.htm">http://www.usatoday.com/life/cyber/tech/ctc875.htm</a>

Associated Press (1998b) "Lawmakers: Cyber Terrorism is a Worry". USA Today, June 11 1998. <a href="http://www.usatoday.com/life/cyber/tech/ctc917.htm">http://www.usatoday.com/life/cyber/tech/ctc917.htm</a>

Athanasiou, T. (1989) "Artificial Intelligence, wishful thinking and war". Levidow, L. and Robins, K., eds. *Cyborg Worlds: The Military Information Society*. London: Free Association Books; 113-133.

Bachelard, G. (1969) The Poetics of Space (translated by Maria Jolas). Boston: Beacon P.

Baddeley, S. (1997) "Governmentality". In Loader, B. The Governance of Cyberspace: Politics, Technology and Global Restructuring. London: Routledge, 64-96.

Balls, R. (1998a) "Act Will Allow Citizens Access to Personal Data". *The Irish Times*, Apr. 22 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0422/hom43.html">http://www.irish-times.com/irish-times/paper/1998/0422/hom43.html</a>

Balls, R. (1998b) "NUJ Wants Proposed Access Fees to be Dropped". *The Irish Times*, Apr. 22 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0422/hom40.html">http://www.irish-times.com/irish-times/paper/1998/0422/hom40.html</a>

Balls, R. (1998c) "Safeguards Urged with Amsterdam Treaty". *The Irish Times*, Sep. 7 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0907/hom19.htm">http://www.irish-times.com/irish-times/paper/1998/0907/hom19.htm</a>

Barber, B. (1995) "The Making of McWorld (Interview of Benjamin R. Barber)". New Perspectives Quarterly, Fall 1995, 13-17.

Barna, T. and Duncan, J. (1991) Writing Worlds: Discourse, Text and Metaphor in the Representation of Landscape. London: Routledge.

Barnes, M., ed., (1981) Information and society: a collection of papers presented at meetings of the B.S.A. Libraries and Information Study Group, 1978-1980. Leeds: School of Librarianship, Leeds Polytechic.

Barr, R. (1996a) "GIS: The Ethical Dimension". Mapping Awareness 10 (1), 15.

Barr, R. (1996b) "They Know Who You Are; They Know Where You Live". *Mapping Awareness* 10 (10), December 1996, 30-32.

Barr, R. (1997) "On the Noble Art of Fixing Elections". Mapping Awareness 11 (3), 21-23.

Barr, S. (1998a) "Pentagon Faulted on Year 2000 Reports". *The Washington Post*, June 12 1998. <a href="http://washingtonpost.com/wp-srv/WPlate/1998-06/12/0671-061298-idx.htm">http://washingtonpost.com/wp-srv/WPlate/1998-06/12/0671-061298-idx.htm</a>

Barr, S. (1998b) "SEC: Year 200 Reports Fall Short". *The Washington Post*, June 111 1998. <a href="http://washingtonpost.com/wp-srv/WPlate/1998-06/11/1811-061198-idx.htm">http://washingtonpost.com/wp-srv/WPlate/1998-06/11/1811-061198-idx.htm</a>

Barrie, C. (1998) "Microsoft gets CandW Brush-Off". The Guardian, Mar. 11 1998. <a href="http://reports.guardian.co.uk/papers/19980310-21.htm">http://reports.guardian.co.uk/papers/19980310-21.htm</a>

Barron, D. (1978) "People, not computers". Young, J., ed. Privacy. Chichester [etc.]: Wiley, 319-328.

Barry, A. (1996) "Who Gets to Play? Art, Access and the Margin". Dovey, J., ed. Fractal Dreams. London: Lawrence & Wishart, 136-153.

BBC (1997) "Spy in the Sky". The Net, Feb. 24 1997. < http://www.bbc.co.uk/the-net/creation/1/item1.html>

Beaumont, J. (1991) "GIS and marketing analysis". Maguire, D., Goodchild, M. and Rhind, D., eds. (1991) *Geographical information systems: principles and applications (2 vols.)*. UK: Longman Scientific & Technical, vol. 2, 139-151.

Benn, S. (1971) "Privacy, Freedom, and Respect for Persons". Reprinted in Schoeman, F., *Philosophical Dimensions of Privacy*. UK: Cambridge University Press, 223-244.

Bensman, J. and Lilienfeld, Robert (1979) Between public and private: the lost boundaries of the self. New York: Free Press. - London: Collier Macmillan.

Bergfeld, J. (1996) "The impact of the EC Data Protection Directive on Dutch Data Protection Law", 1996 (1) The Journal of Information, Law and Technology (JILT). <a href="http://elj.warwick.ac.uk/elj/jilt/dp/ldutch/">http://elj.warwick.ac.uk/elj/jilt/dp/ldutch/</a>

Berland, J. (1996) "Mapping Space: Imaging Technologies and the Planetary Body". In Aronowitz, et al. *Technoscience and Cyberculture*. New York: Routledge, 123-137.

Berndt, R. and Berndt, C. (1989) The speaking land. UK: Penguin.

Bernhardsen, T. (1999) Geographic information systems: an introduction (2nd ed.). New York. - Chichester: Wiley.

Billington, R. (1970). Westward Expansion: A History of the American Frontier. USA: Macmillan Company.

Bimber, B. (1994) "Three Faces of Technological Determinism". In Smith, M. and Marx, L. *Does Technology Drive History? The Dilemma of Technological Determinism*. Cambridge, Massachusetts: The MIT Press, 79-100.

Bishop D. (1995) "Access to Digital Data in US Federal Agencies". The AGI Sourcebook for Geographic Information Systems. London: AGI, 93-99.

Black, J. (1997) Maps and history: constructing images of the past. New Haven, London: Yale University Press.

Blakemore, M. and Harley, J. (1980) "Concepts in the History of Cartography: A Review and Perspective". *Cartographica* 17(4).

Blakemore, M. and Rybaczuk, K. (1993) "Information Supply, Availability, and Costs, Ethics and Freedom. Challenges for 'Open' Europe". *Mapping Awareness* and GIS in Europe 7(1), Jan/Feb 1993, 20-23.

Bloustein, E. (1964) "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser". Reprinted in Schoeman, F., *Philosophical Dimensions of Privacy*. UK: Cambridge University Press, 156-202.

Blume, H. (1995) "Digital Refusnik". Wired Magazine, May 1995, 84-85.

Blume, P. (1996) "Implementation of the European Data Protection Directive: The View from Denmark", 1996(1) *The Journal of Information, Law and Technology (JILT).* <a href="http://elj.warwick.ac.uk/jilt/dp/1Danish/">http://elj.warwick.ac.uk/jilt/dp/1Danish/</a>

Blume, P. (1998) "The Citizen's Data Protection". 1998 (1) The Journal of Infomation, Law and Technology (JILT). <a href="http://elj.warwick.ac.uk/jilt/infosoc/98\_1blum/blume.htm/">http://elj.warwick.ac.uk/jilt/infosoc/98\_1blum/blume.htm</a>

Board, C. (1981) "Cartographic Communication". *Cartographica:* Monograph 27: Maps in Modern Geography - Geographical Perspectives on the New Cartography, 18(2), Summer 1981, 42-78.

Bogard, W. (1996) The Simulation of Surveillance: Hypercontrol in Telematic Societies. UK: Cambridge University Press.

Boggan, S. and Buncombe, A. (1998) "Murdoch's 'Angel of Death' Descends". *The Independent*, Mar. 6 1998. <a href="http://www.independent.co.uk/stories/A0603803.htm">http://www.independent.co.uk/stories/A0603803.htm</a>

Boling, P. (1996) Privacy: the politics of intimate life. New York: Cornell University Press.

Bonham-Carter, G. (1994) Geographic information systems for geoscientists: modelling with GIS. Kidlington: Pergamon.

Borges, J. (1981) A Universal History of Infamy (translated by Norman Thomas di Giovanni). Harmondsworth: Penguin.

Borges, J. (1981) "Of Exactitude in Science". In Borges, J., A Universal History of Infamy. Harmondsworth: Penguin.

Boud, R. (1989) "Episodes in Cartographic Patronage: The Scottish Agricultural Society and the Coal District Maps 1834-1847". *Cartographica* 26(3and4), Autumn and Winter 1989, 59-88.

Bowden, M. (1976) "The Great American Desert in the American Mind: The Historiography of a Geographical Notion". Lowenthal, D. and Bowden M., eds. *Geographies of the Mind: Essays in Historical Geography*. New York: Oxford University Press; 119-147.

Bracken, I. (1994) "A surface model approach to the representation of population-related social indicators". Fotheringham, A., Rogerson, P., eds. (1994) *Spatial analysis and GIS*. London: Taylor & Francis, 247-255.

Brand, M. (1996) Eurogi and the European Geographic Information Infrastructure (EGII). Presented at: GIS Ireland '96, Dublin; October 1996.

Branscomb, A. (1991) "Common Law for the Electronic Frontier". Scientific American, Sept. 1991, 112-115.

Branson, A. (1998) "House Panel Passes Net 'Tax Freedom' Bill". *The Washington Post*, May 14 1998. <a href="http://washingtonpost.com/wp-srv/digest/daily/may98/15/nettax.htm">http://washingtonpost.com/wp-srv/digest/daily/may98/15/nettax.htm</a>

Breen, S. (1996) "Unionists Happy with ID Cards but not with Crest". *The Irish Times*, Aug. 23 1996. <a href="http://www.irish-times.com/irish%2Dtimes/paper/1996/0823/hom23.htm">http://www.irish-times.com/irish%2Dtimes/paper/1996/0823/hom23.htm</a>

Breslin, L. (1996) *The information society: Irish feast or Irish famine?* Dublin: European Movement in association with Telecom Éireann.

Brosnan, M. (1998) Technophobia: the psychological impact of information technology. London : Routledge.

Broughton, J. (1996) "The Bomb's-Eye View: Smart Weapons and Military TV". In Aronowitz, et al. *Technoscience and Cyberculture*. New York: Routledge, 139-165.

Brown, L. (1979) The story of maps. New York: Dover Publications [etc.]. - London: Constable.

Brown, P. (1991) "Exploring geodemographics". Masser, I. and Blakemore, M., eds., *Handling geographical information: methodology and potential applications*. UK: Longman Scientific & Technical, 221-258.

Brown, R. (1969) The Normans and the Norman Conquest. London: Constable.

Browning, J. (1995) "Just Use It". Wired Magazine, May 1995, 37.

Brownlie, I. (1992) Basic Documents on Human Rights. Oxford: Clarendon Press.

Bryson, B. (1990) Mother Tongue: The English Language. UK: Penguin Books.

Buchanan, H. (1996) Impact of European Standards in Geographic Information. Presented at: GIS Ireland '96, Dublin; October 1996.

Bulmer, M. (1982) "How safe is the census? Some reflections on legal safeguards for social research". Raab, Charles D., ed., *Data protection and privacy: proceedings of a conference*. London: Social Research Association, 13-20.

Burnett, A. (1985) "Propaganda Cartography". In Pepper, D. and Jenkins, A., eds., *The Geography of Peace and War*. UK: Basil Blackwell Ltd..

Burns, R. (1998) Using New Technologies to Enhance Human Communications. <a href="http://www.cybercon98.org/wcm/burns.htm">http://www.cybercon98.org/wcm/burns.htm</a>

Burrough P. (1986) Principles of geographical information systems for land resources assessment. Oxford: Clarendon.

Burrough, P. and Longhorn, R. (1998) European Geographic Information Infrastructures. Presented at GIS Ireland 98, Malahide, Dublin.

Burrough, P. and McDonnell, R. (1998). Principles of Geographical Information Systems. Oxford: Oxford University Press.

Butler, S. (1996) Erewhon . UK: Wordsworth Classics.

Byrne, R. and McCutcheon, J. (1986) *The Irish Legal System: cases and materials*. Abingdon, Oxon: Professional Books.

Cairncross, F. (1997) "Survey Telecommunications: A Connected World". *The Economist* (Net Edition), Sept. 13 1997. <a href="http://www.economist.com/editorial/freeforall/21-9-97/index\_survey.html">http://www.economist.com/editorial/freeforall/21-9-97/index\_survey.html</a>

Callinicos, A. (1989) Against Postmodernism: a Marxist Critique. Cambridge: Polity Press.

Callingham, M. (1997) "Can Strangers Find a Common Creed?" *Mapping Awareness* 11(2), Mar. 1997, 14-15.

Calvert, C., Murray, K. and Smith, N. (1997) "New technology and its impact on the framework for the world". Rhind, D., ed., *Framework for the world*. Cambridge: GeoInformation International, 133-159.

Campbell, D. (1998) "Hiding from the Spies in the Sky". *The Guardian Online*, June 4 1998. <a href="http://go2.guardian.co.uk/theweb/896882097-spy.htm">http://go2.guardian.co.uk/theweb/896882097-spy.htm</a>

Carroll, J. (1998) "Father's Email on Child's Murder Leads to Charges". *The Irish Times*, May 2 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0502/wor15.htm">http://www.irish-times.com/irish-times/paper/1998/0502/wor15.htm</a>

Carter, D. (1997) "Digital Democracy' or 'Information Aristocracy'? Economic Regeneration and the Information Economy". In Loader, B., ed., *The Governance of Cyberspace: Politics, Technology and Global Restructuring*. London: Routledge, 136-152.

Caruso, D. (1998) Digital Literacy: Important or Insignificant? <a href="http://www.cybercon98.org/wcm/caruso.htm">http://www.cybercon98.org/wcm/caruso.htm</a>

Casey, E. (1997) The Fate of Place: a philosophical history. Berkeley, London: University of California Press.

Casey, J. (1992) Constitutional Law in Ireland (2nd ed.). London: Sweet and Maxwell.

Cassell, P., ed. (1993) The Giddens Reader. UK: The Macmillan Press.

Castaneda, R. (1998) "A Case to Test the Limits of Press Freedom". *The Washington Post*, Apr. 27, (1998. <a href="http://washingtonpost.com/wp-srv/frompost/april98/matthews27.htm">http://washingtonpost.com/wp-srv/frompost/april98/matthews27.htm</a>

Castells, M. (1996) The Rise of the Network Society. UK: Blackwell Publishers.

Cate, F. (1997) Privacy in the information age. Washington, D.C.: Brookings Institution Press.

Central Statistics Office (1996) Census of Population of Ireland, 1996 - Form A (Specimen). Dublin: CSO.

Chaliand, G. and Ragean, J.-P. (1986) Strategic Atlas: World Geopolitics. Harmondsworth: Penguin.

Chandrasekaran, R. (1998a) "Doors Fling Open to Public Records". *The Washington Post*, March 9, (1998: <a href="http://washingtonpost.com/wp-srv/frompost/march98/privacy9.htm">http://washingtonpost.com/wp-srv/frompost/march98/privacy9.htm</a>

Chandrasekaran, R. (1998b) "Year 200 'Bug' to Cost Firms \$50 Billion". *The Washington Post*, Apr. 29; 1998. <a href="http://washingtonpost.com/wp-srv/washtech/features/y2k042998.htm">http://washingtonpost.com/wp-srv/washtech/features/y2k042998.htm</a>

Chandrasekaran, R. (1998c) "Microsoft to Delay Software, Start Talks". *The Washington Post*, May 15 1998. <a href="http://washingtonpost.com/wp-srv/business/longterm/microsoft/micro.htm">http://washingtonpost.com/wp-srv/business/longterm/microsoft/micro.htm</a>

Chatwin, B. (1979) In Patagonia. London: Pan Books.

Chatwin, B. (1987) The Songlines. London: Picador.

Chesterton, C. (1919) A History of the United States. London: Chatto and Windus.

Cho, G. (1998) Geographical Information Systems and the Law; Mapping the Legal frontiers. Chichester: Wiley.

Chomsky, N. (1972) Problems of Knowledge and Freedom. London: Fontana.

Chomsky, N. (1973a) For Reasons of State. London: Fontana.

Chomsky, N. (1973b) The Backroom Boys. London: Fontana.

Chomsky, N. (1987) "Propaganda States: Orwell's and Ours". *Propaganda Review* 1, Winter 1987-88.. <a href="http://wwwdsp.ucd.ie/~daragh/articles/a\_psao.html">http://wwwdsp.ucd.ie/~daragh/articles/a\_psao.html</a>

Chomsky, N. (1989) Necessary Illusions : thought control in democratic societies. London: Pluto.

Chomsky, N., (1992a) Chronicles of Dissent (interviews with David Barsamian). Monroe: Common Courage. - Stirling: AK Press.

Chomsky, N. (1992b) Deterring Democracy. London: Vintage.

Chorley, R. (1973) Directions in Geography. London: Methuen.

Chorley, R. (1973) "Ethics and Logic in Geography". In Chorley, R. Directions in Geography, 317-331.

Chrisman, N. (1997) Exploring Geographic Information Systems. New York: Wiley.

Churchill, W. (1968) Marlborough: His life and times (four volumes). New York: Charles Scribner's Sons.

Clince, S. (1995) Information Technology in Central Government. Presented at IRLOGI GIS Workshop, TCD, June 14 1995.

Clark, R. (1990) Data Protection Law in Ireland. Dublin: Round Hall Press.

Clark, R. (1996) "Data Protection in Ireland", 1996(1) The Journal of Information, Law and Technology (JILT). <a href="http://eli.warwick.ac.uk/elj/jilt/dp/leire/">http://eli.warwick.ac.uk/elj/jilt/dp/leire/</a>

Clark, R. and Smyth, S. (1997) Intellectual Property Law in Ireland. Dublin: Butterworths.

Clark, T. (1998) "BofA Gives Customers Smart Cards". News.Com. <a href="http://www.News.Com/News/Item/0,4,21550,00.html">http://www.News.Com/News/Item/0,4,21550,00.html</a>

Cleary, C. (1998a) "DPP to get File on Phone Fraud of £100.000". *The Irish Times*, Jun. 12 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0612/hom13.htm">http://www.irish-times.com/irish-times/paper/1998/0612/hom13.htm</a>

Cleary, C. (1998b) "Report Claims Evidence of Paedophiles on Web". *The Irish Times*, Mar. 23 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0323/fro3.html">http://www.irish-times.com/irish-times/paper/1998/0323/fro3.html</a>

Cleary, C. (1999) "Sex Offenders to be Forced to Sign on Register". *The Irish Times*, Feb. 19 1998. <a href="http://www.irish-times/irish-times/paper/1999/0219/hom7.htm">http://www.irish-times/irish-times/paper/1999/0219/hom7.htm</a>

CNN (1998) "FBI Charges 14 in Cyberspace Betting Scheme". CNN, Mar. 5 1998. <a href="http://CNNSI.com/more/news/1998/03/05/internet\_gambling/">http://CNNSI.com/more/news/1998/03/05/internet\_gambling/</a>

Coghlan, D. (1998) "Healy-Rae Transforms Map". *The Irish Times*, Nov. 18 1998. < http://www.irish-times/irish-times/paper/1998/1118/hom5.htm>

Cohen, S. (1985) Visions of Social Control : crime, punishment and classification. Cambridge: Polity Press. - Oxford: Blackwell.

Collins, L. and Lapierre, D. (1997). Freedom at Midnight. London: Harper Collins.

Committee of Public Accounts (1994) Twenty-ninth Report: Data Controls and Safeguards. London: HMSO.

Committee on Government Information (1990) Data Protection, Computers, and Changing Information Practices: A Hearing before the Government Information, Justice, and Agriculture Subcommittee of the Committee on Government Operations - House of Representatives. Washington: US Government Printing Office.

Committee on Government Operations of the House of Representatives (1982) Hearing before a Subcommittee of the Committee: Government Provision of Information Services in Competition with the Private Sector. Washington: US Government Printing Office.

Committee on Government Operations of the House of Representatives (1990) Computer Matching and Privacy Protection Amendments of 1990. Report of Mr. Convers from the Committee on Government Operations. Washington: US Government Printing Office.

Committee on Government Operations of the House of Representatives (1991) Hearing before the Government Information, Justice, and Agriculture Subcommittee of the Committee: Data Protection, Computers, and Changing Information Practices. Washington: US Government Printing Office.

Connected.org (1998) *Privacy: A Fragile Boundary between Private and Public Spheres.* <a href="http://www.connected.org/rights/privacy.htm">http://www.connected.org/rights/privacy.htm</a>

Connor, S. (1997) Postmodernist Culture: an introduction to theories of the contemporary (2nd ed.). Oxford: Blackwell.

Conrad, D. (1995) *Privacy and Security in the Information Age*. <a href="http://www.freenet.org/staff/conrad/privacy.html">http://www.freenet.org/staff/conrad/privacy.html</a>

Conrad, J. (1995) Heart of Darkness (with The Congo Diary). London: Penguin.

Coppock, C. and Rhind, D. (1991) "The history of GIS". Maguire, D., Goodchild, M. and Rhind, D., eds., *Geographical information systems: principles and applications (2 vols.)*. UK: Longman Scientific & Technical, vol. 1, 21-43.

Corcoran, E. (1998a) "Ads to Target Encryption Curbs". *The Washington Post*, Mar. 4 1998. <a href="http://washingtonpost.com/wp-srv/tech/target.htm">http://washingtonpost.com/wp-srv/tech/target.htm</a>>

Corcoran, E. (1998b) "Facing the Problems of Prank Messages: Bogus E-Mail a Growing Issue on the Net". *The Washington Post*, Mar. 21 1998. <a href="http://washingtonpost.com/wp-srv/WPlate/1998-03/21/0161-032198-idx.htm">http://washingtonpost.com/wp-srv/WPlate/1998-03/21/0161-032198-idx.htm</a>

Corcoran, E. (1998c) "U.S. Software Company Poses Challenge to Encryption Curbs". *The Washington Post*, Mar. 21 1998. <a href="http://washingtonpost.com/wp-srv/WPlate/1998-03/21/0171-032198-idx.htm">http://washingtonpost.com/wp-srv/WPlate/1998-03/21/0171-032198-idx.htm</a>

Cosmedia (1998) Surviving the Internet Legal Minefield: A Brief Guide to the Legal Perils of the Internet. Dublin: Cosmedia.

Council of Europe (1950) Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights). <a href="http://www.coe.fr/eng/legaltxt/5e.htm">http://www.coe.fr/eng/legaltxt/5e.htm</a>

Council of Europe (1981) Council of Europe Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data. <a href="http://www.coe.fr/eng/legaltxt/108e.htm">http://www.coe.fr/eng/legaltxt/108e.htm</a>

Council of Europe (1985) Recommendation N° R (85) 20 Of The Committee Of Ministers To Member States on the protection of personal data used for the purposes of direct marketing (25 October 1985). <a href="http://www.coe.fr/DataProtection/rec/r(85)20e.htm">http://www.coe.fr/DataProtection/rec/r(85)20e.htm</a>

Council of Europe (1986) Recommendation N° R(86) 1 Of The Committee Of Ministers To Member States on the protection of personal data used for social security purposes (23 January 1986). <a href="http://www.coe.fr/DataProtection/rec/r(86)1e.htm">http://www.coe.fr/DataProtection/rec/r(86)1e.htm</a>

Council of Europe (1987) Recommendation N° R(87) 15 Of The Committee Of Ministers To Member States regulating the use of personal data in the police sector (17 September 1987). <a href="http://www.coe.fr/DataProtection/rec/r(87)15e.htm">http://www.coe.fr/DataProtection/rec/r(87)15e.htm</a>

Council of Europe (1990) Data Protection and the Media. < http://www.coe.fr/DataProtection/emedia.htm>

Council of Europe (1991a) Recommendation N° R (91) 10 Of The Committee Of Ministers To Member States on the communication to third parties of personal data held by public bodies (9 September 1991). <http://www.coe.fr/DataProtection/rec/r(91)10e.htm>

Council of Europe (1991b) The Introduction and Use of Personal Identification Numbers: the data protection issues. Strasbourg: Council of Europe.

Council of Europe (1999) Recommendation No.R (99) 5 Of The Committee Of Ministers To Member States For The Protection Of Privacy On The Internet: Guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways. <http://www.coe.fr/DataProtection/elignes.htm>

Council of Europe: Directorate of Legal Affairs - Committee of Experts on Data Protection (1989) *New Technologies : a challenge to privacy protection?* (study prepared by the Committee of Experts on Data Protection under the authority of the European Committee on Legal Co-operation. Strasbourg: Council of Europe.

Cox, R. (1995a) The European Umbrella Organisation for Geographic Information (EUROGI). Presented at IRLOGI GIS Workshop, TCD, June 14 1995.

Cox, R. (1995b) The European Geographic Information Infrastructure / GI2000 Document, A Summary. Presented at IRLOGI GIS Workshop, TCD, June 14 1995.

Cox, R. (1995c) *The Irish Organisation for Geographic Information (IRLOGI)*. Presented at IRLOGI GIS Workshop, TCD, June 14 1995.

Cox, R. (1998) Personal Communication.

Craib, I. (1992a) Anthony Giddens. London: Routledge.

Craib, I. (1992b) Modern Social Theory: from Parsons to Habermas. :New York, London: Harvester Wheatsheaf.

Craib, I. (1997) Classical Social Theory. UK: Oxford University Press.

Cresson, E. (1995) "Roots and Wings: Remaining European in the Information Age" (Adapted from Talk to Multimedia Forum in Tokyo). *New Perspectives Quarterly*, Fall 1995, 26-28.

Crnobrnja, M. (1996) The Yugoslav Drama (revised edition). London: I. B. Tauris. 1 (1) 10-14

Crone, G. (1978) Maps and their Makers: an introduction to the history of cartography. Folkestone: Dawson.

Cullen, P. (1997) "Poisoned Chalice of Human Rights". *The Irish Times* World Review, 1997. <a href="http://www.irish-times.com/irish-times/paper/wldreview97/wrev22.htm">http://www.irish-times.com/irish-times/paper/wldreview97/wrev22.htm</a>

Cullen, P. (1998) " 'No end in sight' to senseless war". *The Irish Times*, June 10 1998. <a href="http://www.ireland.com/newspaper/world/1998/0610/wor4.htm">http://www.ireland.com/newspaper/world/1998/0610/wor4.htm</a>

Cunningham, F. (1998) "Nothing to Lose by Re-Examining Marx". *The Irish Times*, Mar. 21 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0321/wor8.htm">http://www.irish-times.com/irish-times/paper/1998/0321/wor8.htm</a>

Cunningham, M. (1996) "Address Unknown". The Irish Times, Mar. 4 1996. <a href="http://www.irish-times.com/irish%2Dtimes/paper/1996/0304/cmp4.htm">http://www.irish-times.com/irish%2Dtimes/paper/1996/0304/cmp4.htm</a>

Cunningham, M. (1997) "Cookies: The Paparazzi of the Internet". *The Irish Times*, Sept. 8 1997. <a href="http://wwww.irish-times.com/irish%2Dtimes/paper/1997/0908/cmp3.htm">http://wwww.irish-times.com/irish%2Dtimes/paper/1997/0908/cmp3.htm</a>

Cunningham, M. (1998a) "Nua Ways of Doing Business". The Irish Times, Mar. 16 1998. < http://www.irish-times.com/irish-times/paper/1998/0316/cmp1.htm>

Cunningham, M. (1998b) "Post Modern Ironies". *The Irish Times*, Apr. 6 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0406/cmp2.htm">http://www.irish-times/paper/1998/0406/cmp2.htm</a>

Cunningham, M. (1998c) "Why I Really Hate Computers". *The Irish Times*, Apr. 27 1998. <a href="http://www.irish-times/irish-times/paper/1998/0427/cmp1.htm">http://www.irish-times/paper/1998/0427/cmp1.htm</a>

Cunningham, M. and Ó Marcaigh, F. (1999) "The Times They've Been a Changin". *The Irish Times*, Feb. 22 1999. <a href="http://www.irish-times/irish-times/paper/1999/0222/cmp1.htm">http://www.irish-times/irish-times/irish-times/paper/1999/0222/cmp1.htm</a>

Curry, M. (1994) "In Plain and Open View: Geographic Information Systems and the Problem of Privacy". In Onsrud, H., ed., (1995) *Proceedings of the Conference on Law and Information Policy for Spatial Databases: Tempe, Arizona:* October 29-31 1994. <a href="http://www.spatial.maine.edu/tempe/tempe94.html">http://www.spatial.maine.edu/tempe/tempe94.html</a>

Curry, M. (1998) Digital places: living with geographic information technologies. London. - New York: Routledge.

Cusack, J. (1996) "Law to Protect Against Bugging Urged". *The Irish Times*, Oct. 24 1996. <a href="http://www.irish-times.com/irish%2Dtimes/paper/1996/1024/hom22.htm">http://www.irish-times.com/irish%2Dtimes/paper/1996/1024/hom22.htm</a>

Cusack, J. (1998a) "Garda Tests New Criminal Intelligence Network". *The Irish Times*, Dec. 7 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/1207/hom10.htm">http://www.irish-times.com/irish-times/paper/1998/1207/hom10.htm</a>

Cusack, J. (1998b) "Surveillance Cameras May be Used to Discipline Gardai". *The Irish Times*, June 10 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0610/fro2.htm">http://www.irish-times.com/irish-times/paper/1998/0610/fro2.htm</a>

Dahlbom, B. and Mathiassen, L. (1993) Computers in Context: the philosophy and practice of systems design. Cambridge, MA. - Oxford: NCC Blackwell.

Dainith, J. (1997) Biographical Dictionary of Quotations (Revised Edition). UK: Bloomsbury Reference.

Dalenius, T. (1982) "Privacy and statistics: Some potential research topics". Raab, C., ed., Data protection and privacy: proceedings of a conference. London: Social Research Association, 26-30.

Dandeker, C. (1990) Surveillance, Power and Modernity: bureaucracy and discipline from 1700 to the present day. Cambridge: Polity Press.

Dangermond, J. (1993) "Sharing Government's Digital Information with the Public". GIS Law 1 (3), 19-21.

Dansby, B. (1996) "Publishing Land Records on the Internet". GIS Law 3 (3), Fall 1996, 1-3.

Dansby, H. (1993) "Public Records and Governmental Liability - Part II". GIS Law 1 (3), 10-14.

Dapor, M. (1991) "Civil Liberties in Cyberspace". Scientific American, Sept. 1991, 116-120.

Data Protection Commissioner (1988) Guide to the Data Protection Act 1988. Dublin: Data Protection Commissioner.

Data Protection Commissioner (1989a) Annual Report of the Data Protection Commissioner 1988. Dublin: Data Protection Commissioner.

Data Protection Commissioner (1989b) Data Protection Act 1988: applications for registration - guidance notes. Dublin: Data Protection Commissioner.

Data Protection Commissioner (1990) Annual Report of the Data Protection Commissioner 1989. Dublin: Data Protection Commissioner.

Data Protection Commissioner (1991) Annual Report of the Data Protection Commissioner 1990. Dublin: Data Protection Commissioner.

Data Protection Commissioner (1992) Annual Report of the Data Protection Commissioner 1991. Dublin: Data Protection Commissioner.

Data Protection Commissioner (1993) Annual Report of the Data Protection Commissioner 1992. Dublin: Data Protection Commissioner.

Data Protection Commissioner (1994) Annual Report of the Data Protection Commissioner 1993. Dublin: Data Protection Commissioner.

Data Protection Commissioner (1995) Annual Report of the Data Protection Commissioner 1994. Dublin: Data Protection Commissioner.

Data Protection Commissioner (1996) Annual Report of the Data Protection Commissioner 1995. Dublin: Data Protection Commissioner.

Data Protection Commissioner (1997) Annual Report of the Data Protection Commissioner 1996. Dublin: Data Protection Commissioner.

Data Protection Commissioner (1998) Annual Report of the Data Protection Commissioner 1997. Dublin: Data Protection Commissioner.

Data Protection Registrar (1994) The Tenth Report of the Data Protection Registrar. London: HMSO.

Davies, S. (1995) "Welcome Home Big Brother". Wired Magazine, May 1995, 58-63 and 110.

Davies, S. (1997) "10 Reasons Why Public CCTV Schemes are Bad." *Privacy International*, Apr. 28 1997. <a href="http://merlin.legend.org.uk/~brs/cctv/tenreasons.htm">http://merlin.legend.org.uk/~brs/cctv/tenreasons.htm</a>

Davis, J. and Kanellos, M. (1998) "Cyberhomes on the Horizon?" News. Com, Apr. 30 1998. <a href="http://www.News.Com/News/Item/0,4,21673,00.html">http://www.News.Com/News/Item/0,4,21673,00.html</a>

De Blij, H. (1973) Systematic Political Geography. USA: John Wiley and Sons, Inc..

De Bréandún, D. (1996) "Bill to Give Dail Committee Power to Review Secrecy Laws". *The Irish Times*, Jan. 8 1996. <a href="http://www.irish-times.com/irish-times/paper/1996/0108/hom8.htm">http://www.irish-times.com/irish-times/paper/1996/0108/hom8.htm</a>

De Bruine, R. (1999) Report of the Consultation Meeting Regarding GI2000. <http://www2.echo.lu/gi/en/meetings/gi200015399.html>

De Buitléir, M. (1995a) National Geographic Information Issues. Presented at IRLOGI GIS Workshop, TCD, June 14 1995.

De Buitléir, M. (1995b) "The Irish Dilemma". Mapping Awareness 9 (1), Feb. 1995, 20-22.

De Landa, M. (1996) "Markets and Antimarkets in the World Economy". In Aronowitz, et al. *Technoscience and Cyberculture*. New York: Routledge, 181-194.

DeMers, M. (1997) Fundamentals of geographic information systems. New York, Chichester: Wiley.

De Sant'Anna, A. (1996) "Libraries, Social Inequality, and the Challenge of the Twenty-First Century". Daedalus (Journal of the American Academy of Arts and Sciences) 125(4), Fall 1996, 267-281.

Delanty, G. (1995) Inventing Europe: idea, identity, reality. Basingstoke: Macmillan.

Deleuze, G. (1988) Foucault (translated and edited by Sean Hand). London: Athlone.

Delos, A. (1992) "Principles of Implementation at EEC Level". *Proceedings of the International Seminar on Statistical Confidentiality, September 1992, Dublin.* Luxembourg: Office des Publications Officielles des Communautés Européennes (1993), 157-163.

Denning, D. (1997) "The Future of Cryptography". In Loader, B. The Governance of Cyberspace: Politics, Technology and Global Restructuring. London: Routledge, 175-189.

Department of Agriculture and Food (1998a) 1998 EU Area Aid Application - Form AA98. Dublin: Department of Agriculture and Food.

Department of Agriculture and Food (1998b) Land Parcel Identification Systems (LPIS) - 1998 Update. Dublin: Department of Agriculture and Food.

Department of Justice, Equality and Law Reform (1997) Consultation Paper on Transposition into Irish Law (of EU Directive EC 95/46/EC). <a href="http://www.irlgov.ie/justice/Publications/Law/consultation.htm">http://www.irlgov.ie/justice/Publications/Law/consultation.htm</a>

Department of Justice, Equality and Law Reform (Working Group on the Illegal and Harmful Use of the Internet) (1998) Illegal and Harmful Uses of the Internet: First Report of the Working Group (chairperson: John Haskins). Dublin: Stationary Office. <a href="http://www.irlgov.ie/justice/Publications/internet%20submissions/intrep.pdf">http://www.irlgov.ie/justice/Publications/internet%20submissions/interp.pdf</a>

Department of Social Welfare (Chairman: Sullivan, E.) (1996) Interdepartmental Report on the Development of an "Integrated Social Services System". Dublin: Stationary Office.

Department of the Environment (Chorley, R., ed.) (1987) Handling geographic information / report to the Secretary of State for the Environment of the Committee of Enquiry into the Handling of Geographic Information - Chairman, Lord Chorley. London: HMSO.

Department of the Environment (1988) Handling geographic information: the Government's response to the report of the Committee of Enquiry chaired by Lord Chorley. London: HMSO.

Dertouzos, M. (1997) "Cyberview: What Will Really Be". *Scientific American*, July 1997. <a href="http://www.sciam.com/0797issue/0797profile.htm">http://www.sciam.com/0797issue/0797profile.htm</a>

Desramaux, L. (1992) "Confidentiality and Privacy: How a Statistical Agency Meets New Challenges Created by New Times". *Proceedings of the International Seminar on Statistical Confidentiality, September 1992, Dublin.* Luxembourg: Office des Publications Officielles des Communautés Européennes (1993), 123-130.

Dial, O. and Goldberg, E. (1975) Privacy, security and computers: guidelines for municipal and other public information systems. London: Praeger.

Difazio, W. (1996) "Technoscience and the Labor Process". In Aronowitz, et al. *Technoscience and Cyberculture*. New York: Routledge, 195-203.

Diffie, W. and Landau, S. (1998) *Privacy on the Line: The Politics of Wiretapping and Encryption*. USA: The MIT Press.

Dikshit, R. (1997) Developments in Political Geography: A Century of Progress. New Delhi, London: Sage Publications Ltd..

Dikshit, R. (1997) "The Nation-State-Territory Relationship as the Central Organising Principle of Political Geography". In Dikshit, R., *Developments in Political Geography: A Century of Progress*. New Delhi, London: Sage Publications Ltd., 55-105.

Dixon, C. and Leach, B. (1979a) Concepts and Techniques in Modern Geography No. 17: Sampling Methods for Geographical Research. UK: Geo Abstracts.

Dixon, C. and Leach, B. (1979b) Concepts and Techniques in Modern Geography No. 18: Questionnaires and interviews in Geographical Research. UK: Geo Abstracts.

Dommering, E. (1991) Protecting Works of Fact: copyright, freedom of expression, and information law. Deventer - Boston: Kluwer Law and Taxation Publishers.

Donnelly, K. (1998) "ID Cards on Way for All: Citizens Face 'Tag' from Childhood". *The Evening Herald*, Feb. 12 1998, 1-2.

Donnelly, R. (1998) "Blair Sets Up Army of 20,000 'Bug Busters'". *The Irish Times*, Mar. 31 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0331/wor9.htm">http://www.irish-times.com/irish-times/paper/1998/0331/wor9.htm</a>

Donovan, K. (1998) "Striking Back at Big Brother". The Irish Times, Apr. 7 1998. < http://www.irish-times.com/irish-times/paper/1998/0407/fea2.htm>

Dorman, L., Lin, P. and Tow, A. (1997) *Digital Privacy: The Ethics of Encryption.* <a href="http://rescomp.stanford.edu/~pweston/privacy.html">http://rescomp.stanford.edu/~pweston/privacy.html</a>

Douglas, N. (1997) "State-formation, Nation-building and Plural societies". In Dikshit, R., Developments in Political Geography: A Century of Progress. New Delhi, London: Sage Publications Ltd., 105-147.

Dovey, J., ed. (1996) Fractal Dreams: new media in social context. London: Lawrence & Wishart.

Doyle, R. (1997) "By the Numbers: Access to the Internet". *Scientific American*, July 1997. <a href="http://www.sciam.com/0797issue/0797scicit3.htm">http://www.sciam.com/0797issue/0797scicit3.htm</a>

Dreyfus, H. and Rabinow, P. (1982) Michel Foucault: beyond structuralism and hermeneutics. Brighton: Harvester.

Dudycha, D. (1981) "The Impact of Computer Cartography". In *Cartographica*: Monograph 27: Maps in Modern Geography - Geographical Perspectives on the New Cartography, 18(2), Summer 1981, 117-150.

Duncan, G. and Mukherjee, S. (1992) "Confidentiality Protection in Statistical Databases: A Disclosure Limitation Approach". *Proceedings of the International Seminar on Statistical Confidentiality, September 1992, Dublin.* Luxembourg: Office des Publications Officielles des Communautés Européennes (1993), 307-315.

Dunne, M. and Bonazzi, T. (1995) Citizenship and Rights in Multicultural Societies. UK: Keele University Press.

Duvall, M. (1998) "Magaziner: Industry Efforts to Protect Online Privacy Falling Short". ZDNet, Apr. 30 1998. <a href="http://www.zdnet.com/zdnn/content/inwÓ0430/311688.htm">http://www.zdnet.com/zdnn/content/inwÓ0430/311688.htm</a>

Dworkin, G. (1978) "Privacy and the Law". Young, J., ed. Privacy. Chichester [etc.]: Wiley, 113-136.

Dymon, U. (1989) "Do We Really Know Our Map Users?" Cartographica 26(3and4), Autumn and Winter 1989, 49-58.

Dyson, E. (1998) "Second Sight: Divergent Myths of Governing the Net". *The Guardian Online*, Mar. 19 1998. <a href="http://go2guardian.co.uk/theweb/890236357-second.html">http://go2guardian.co.uk/theweb/890236357-second.html</a>

Eastern Health Board (1998) Cardlink (Information Sheet). Ireland: EHB.

Edge, D. (1995) "The Social Shaping of Technology". In Heap, N. et al., eds., Information Technology and Society: A Reader. London: Sage Publications, 11-32.

Edson, E. (1997) Mapping Time and Space: how medieval mapmakers viewed their world. London: British Library.

Edwards, P. (1989) "The Closed World: Systems discourse, military policy and post-World War II US historical consciousness". Levidow, L. and Robins, K., eds. *Cyborg Worlds: The Military Information Society*. London: Free Association Books; 135-158.

Egenhofer, M. and Golledge, R., eds. (1998) Spatial and temporal reasoning in geographic information systems. New York, Oxford: Oxford University Press.

Eisenberg, A. (1997a) "Cyber View: Where the Money Is". *Scientific American*, Mar. 1997. <a href="http://www.sciam.com/0397issue/0397cyber.htm">http://www.sciam.com/0397issue/0397cyber.htm</a>

Eisenberg, A. (1997b) "Disliking the Internet". *Scientific American*, June 1997. <a href="http://www.sciam.com/0697issue/0697cyber.htm">http://www.sciam.com/0697issue/0697cyber.htm</a>

Eisenberg, A. (1998) "Confidentially Yours: A Novel Security Scheme Sidesteps U.S. Data Encryption Regulations". *Scientific American*, June 1998. <a href="http://www.sciam.com/1998/0698issue/0698techbus4.htm">http://www.sciam.com/1998/0698issue/0698techbus4.htm</a>

Electronic Frontier Foundation (1996) Your Constitutional Rights have been Sacrificed for Political Expediency: EFF Statement on 1996 Telecommunications Regulation Bill. <a href="http://www.eff.org/pub/Alerts/cda\_020296\_eff.statement">http://www.eff.org/pub/Alerts/cda\_020296\_eff.statement</a>

Eliade, M. (1959) *The Sacred and the Profane: the nature of religion* (translated by Willard R. Trask). New York: Harcourt Brace Jovanovich.

Elmer-Dewitt, P. (1995) "On A Screen Near You: Cyberporn". *Time* 146(1), Jul. 3 1995. <a href="http://pathfinder.com/~PEHjxgYAL5Dw647X/time/magazine/domestic/1995/950703/950703.cover.html">http://pathfinder.com/~PEHjxgYAL5Dw647X/time/magazine/domestic/1995/950703/950703.cover.html</a>

Engelage, C. (1992) "Statistical Confidentiality in the Context of Community Statistics: The Legal Framework". *Proceedings of the International Seminar on Statistical Confidentiality, September 1992, Dublin.* Luxembourg: Office des Publications Officielles des Communautés Européennes (1993), 151-156.

Engelage, C. (1994) "The Draft Data Protection Directive - No Reason to Panic". *Proceedings of the International Seminar on Statistical Confidentiality*, November 1994. Luxembourg: Office for Official Publications of the European Communities (1995), 23-32.

Environmental Systems Research Institute (1993) Understanding GIS: the ARC/INFO method (Rev. 6 for workstations). Harlow: Longman Scientific & Technical.

EPIC (1997) What Can You Do? Controlling Personal Information. <a href="http://epic.org/privacy/consumer/action.html">http://epic.org/privacy/consumer/action.html</a>

Ernst, M. and Schwartz, A. (1962) Privacy: the right to be let alone. New York: Macmillan.

EU Commission (1995) GI2000: Towards a European Geographic Information Infrastructure (EGII): A Discussion Document for Consultation with the European GI Community. Brussels: European Commission, DG XIII.

EU Commission (1997a) Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector. <a href="http://www2.echo.lu/legal/en/dataprot/protection.html">http://www2.echo.lu/legal/en/dataprot/protection.html</a>

EU Commission (1997b) "Towards a European policy framework for Geographic Information: a working document". Rhind, D., ed., *Framework for the world*. Cambridge: GeoInformation International, 202-205.

EU Commission (1998a) *Technical Briefing for Journalists on Data Protection – EU/US Dialogue*. European Commission: DG XV. <a href="http://europa.eu.int/comm/dg15/en/media/dataprot/backinfo/euus.htm">http://europa.eu.int/comm/dg15/en/media/dataprot/backinfo/euus.htm</a>

EU Commission (1998b) Geographic Information in Europe: A Discussion Document. European Commission: DGXIII <a href="http://www2.echo.lu/gi/en/gi2000/discussion98.html">http://www2.echo.lu/gi/en/gi2000/discussion98.html</a>

EU Commission (1999) Status of Implementation of Directive 95/46/EC. European Commission: DG XV. <a href="http://europa.eu.int/comm/dg15/en/media/dataprot/law/impl.htm">http://europa.eu.int/comm/dg15/en/media/dataprot/law/impl.htm</a>

EU Commission, DG XIII (1998) Cardlink 2 Project Fact Sheet. <a href="http://www2.echo.lu/telematics/health/cardlink2.htm">http://www2.echo.lu/telematics/health/cardlink2.htm</a>

EU Parliament and Council (1995) Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. <a href="http://www2.echo.lu/legal/en/dataprot/directiv/directiv.html">http://www2.echo.lu/legal/en/dataprot/directiv/directiv.html</a>

EU Parliament and Council (1996) Directive 96/57/EC of the European Parliament and of the Council on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, in Particular in the Integrated Services Digital Network ISDN) and in the Public Digital Mobile Networks. <a href="http://www2.echo.lu/legal/en/dataprot/isdn/isdn.html">http://www2.echo.lu/legal/en/dataprot/isdn/isdn.html</a>

European Information Industry Association (1996) Access to Government Information-Proposal: A Draft Directive for a Commercial Right of Access to Public Sector Databases. London: European Information Industry Association.

European Union (1998) Treaty of Amsterdam amending the Treaty on European Union, the Treaties Establishing the European Communities and certain related Acts. <http://ue.eu.int/Amsterdam/en/amsteroc/en.htm>

Evans, E. (1998) "Y2K Raises Contract Issues". *The Irish Times*, June 15 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0615/cmp3.htm">http://www.irish-times.com/irish-times/paper/1998/0615/cmp3.htm</a>

Fancher, C. (1996) "Smart Cards". *Scientific American*, August 1996. <a href="http://www.sciam.com/0896issue/0896fancher.htm">http://www.sciam.com/0896issue/0896fancher.htm</a>

Farnsworth Riche, M. (1998) Communication, Politics, and the Census. Presented at One Number Census Workshop, Leeds UK, May 12-13 1998.

Farrell, M. (1997) "Ireland Out of Step on European Rights Law". *The Irish Times*, Dec. 29 1997. <a href="http://www.irish-times.com/irish-times/paper/1997/1229/hom18.htm">http://www.irish-times.com/irish-times/paper/1997/1229/hom18.htm</a>

Farringdon, H. (1989) Strategic Geography: NATO, the Warsaw Pact and the superpowers (2nd ed.). London: Routledge.

Faughan, E. (1999) "Substantial Bill includes a Rich Mix of Measures". *The Irish Times* (Business This Week), Feb. 12 1999, 3.

Feinberg, S. (1992) "Conflicts Between the Needs for Access to Statistical Information and Demands for Confidentiality". *Proceedings of the International Seminar on Statistical Confidentiality, September 1992, Dublin.* Luxembourg: Office des Publications Officielles des Communautés Européennes (1993), 33-47.

Finnis, J. (1983) Fundamentals of ethics. Oxford: Clarendon.

Fischer, M., Scholten, H. and Unwin, D., eds. (1996) Spatial analytical perspectives on GIS. London: Taylor & Francis.

Fischer, M., Scholten, H. and Unwin, D. (1996) "Geographic Information Systems, spatial data analysis and spatial modelling: an introduction". Fischer, M., Scholten, H. and Unwin, D., eds., *Spatial analytical perspectives on GIS*. London: Taylor & Francis, 3-19.

Fisher P., Dykes, J. and Wood, J. (1993) "Map Design and Visualization". *The Cartographic Journal* 30, Dec. 1993, 136-142.

Flaherty, D. (1979) *Privacy and government data banks: an international perspective*. London: Mansell Information Publishing.

Flaherty, D. (1994) "Privacy Protection in Geographic Information Systems: Alternative Protection Scenarios". In Onsrud, H., ed., (1995) Proceedings of the Conference on Law and Information Policy for Spatial Databases: Tempe, Arizona: October 29-31 1994. <http://www.spatial.maine.edu/tempe/tempe94.html>

Flaherty, D., Donohue, T. and Harte, P., eds. (1984) Privacy and data protection: an international bibliography. London: Mansell.

Flanagan, P. (1996) "Big Brother has 'Access to All Areas'". The Irish Independent, July 4 1996, 12.

Flew, A. (1984) A Dictionary of Philosophy. UK: Pan Books.

Foley, M. (1998a) "Information Watchdog to End Culture of Secrecy". *The Irish Times*, June 11 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0611/hom33.htm">http://www.irish-times/paper/1998/0611/hom33.htm</a>

Foley, M. (1998b) "Ireland Out of Line with European Partners". *The Irish Times*, Jan. 31 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0131/>">http://www.irish-times.com/irish-times/paper/1998/0131/></a>

Foley, M. (1998c) "Ireland Urged to Adopt European Accord on Rights". *The Irish Times*, Jun. 15 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0615/hom8.htm">http://www.irish-times.com/irish-times/paper/1998/0615/hom8.htm</a>

Foley, M. (1998d) "Welcome to the Byte-Size Scandal". *The Irish Times*, Feb. 2, 1998. < http://www.irish-times.com/irish-times/paper/1998/0202/cmp2.html>

Foley, M. (1998e) "Well, What Do You Know?" *The Irish Times*, Apr. 7 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0407/fea1.htm">http://www.irish-times.com/irish-times/paper/1998/0407/fea1.htm</a>

Forde, M. (1987) Constitutional law of Ireland. Cork, Dublin: Mercier Press.

Forrest, R., Henderson, J. and Williams, P. (1982) Urban Political Economy and Social Theory: critical essays in urban studies. Aldershot: Gower.

Fotheringham, A. and Rogerson, P., eds. (1994) Spatial analysis and GIS. London: Taylor & Francis.

Foucault, M. (1977) "Confinement, Psychiatry, Prison". In Foucault, M., *Politics, philosophy, culture: interviews and other writings, 1977-1984* (translated by Alan Sheridan and others). New York, London: Routledge, 178-210.

Foucault, M. (1978) "On Power". In Foucault, M., Politics, philosophy, culture: interviews and other writings, 1977-1984 (translated by Alan Sheridan and others). New York, London: Routledge, 96-109.

Foucault, M. (1979) *Discipline and punish: the birth of the prison* (translated by Alan Sheridan). Harmondsworth: Penguin.

Foucault, M. (1980a) *Power/Knowledge: Selected Interviews and Other Writings 1972-1977* (translated by Colin Gordon et al.). Brighton: Harvester Press.

Foucault, M. (1980b) "Body/Power". In Foucault, M., *Power/Knowledge: Selected Interviews and Other Writings 1972-1977* (translated by Colin Gordon et al.). Brighton: Harvester Press, 55-62.

Foucault, M. (1980c) "Prison Talk". In Foucault, M., Power/Knowledge: Selected Interviews and Other Writings 1972-1977 (translated by Colin Gordon et al.). Brighton: Harvester Press, 37-54.

Foucault, M. (1980d) "Questions on Geography". In Foucault, M., *Power/Knowledge: Selected Interviews and Other Writings 1972-1977* (translated by Colin Gordon et al.). Brighton: Harvester Press, 63-77.

Foucault, M. (1980e) "The Confession of the Flesh". In Foucault, M., *Power/Knowledge: Selected Interviews and Other Writings 1972-1977* (translated by Colin Gordon et al.). Brighton: Harvester Press, 194-228.

Foucault, M. (1980f) "The Eye of Power". In Foucault, M., Power/Knowledge: Selected Interviews and Other Writings 1972-1977 (translated by Colin Gordon et al.). Brighton: Harvester Press, 146-165.

Foucault, M. (1980g) "Truth and Power". In Foucault, M., Power/Knowledge: Selected Interviews and Other Writings 1972-1977 (translated by Colin Gordon et al.). Brighton: Harvester Press, 109-133.

Foucault, M. (1986) The Foucault Reader. Harmondsworth: Penguin.

Foucault, M. (1988) Politics, philosophy, culture: interviews and other writings, 1977-1984 (translated by Alan Sheridan and others). New York, London: Routledge.

Foucault, M. (1989) The order of things: an archaeology of the human sciences. London: Routledge.

Foucault, M. (1990) The History of Sexuality: Volume 1: An Introduction (translated by Robert Hurley). Harmondsworth: Penguin.

Foucault, M. (1997) *Ethics: subjectivity and truth* (translated by Robert Hurley and others). London: Allen Lane.

Fox, B. (1998) "I Never Sent That ...". New Scientist, Mar. 28, 1998, 18-19.

Fox, C. (1983) Information and Misinformation: an investigation of the notions of information, misinformation, informing, and misinforming. Westport (Conn.), London: Greenwood.

Fox-Clinch, J. (1997) "Crime and the Digital Dragnet". Mapping Awareness 11(2), 22-24.

Frawley, K. (1992) "A 'green' vision: the evolution of Australian environmentalism". Anderson, K. and Gale, F., eds. *Inventing places: studies in cultural geography*. Melbourne, Australia: Longman Cheshire. - New York: Wiley, Halsted Press, 215-234.

Fried, C. (1968) "Privacy [A Moral Analysis]". Reprinted in Schoeman, F., *Philosophical Dimensions of Privacy*. UK: Cambridge University Press, 203-222.

Fried, I. (1998) "Cookies That Tell the World Your Fortune". *The Independent*, June 9 1998. <a href="http://www.independent.co.uk/net/980519ne/story5.htm">http://www.independent.co.uk/net/980519ne/story5.htm</a>

Friel, B. (1981) Translations. London: Faber.

Frissen, P. (1997) "The Virtual State: Postmodernisation, Informatisation and Public Administration". In Loader, B. *The Governance of Cyberspace: Politics, Technology and Global Restructuring*. London: Routledge, 111-125.

Gates, B., Myhrvold, N. and Rinearson, P. (1995) The Road Ahead. London: Viking.

Gates, B. and Hemingway, C. (1999) Business @ the speed of thought: using a digital nervous system. London : Penguin.

Gates, D. and Groves R. (1992) "Data Protection: Do Respondents, Data Collectors and Users Agree on its Meaning?" *Proceedings of the International Seminar on Statistical Confidentiality, September 1992, Dublin.* Luxembourg: Office des Publications Officielles des Communautés Européennes (1993), 49-59.

Gatrell, A. (1991) "Concepts of Space and Geographical Data". Maguire, D., Goodchild, M. and Rhind, D., eds. (1991) *Geographical information systems: principles and applications (2 vols.)*. UK: Longman Scientific & Technical, vol. 1, 119-134.

Gavison, R. (1980) "Privacy and the Limits of Law". Reprinted in Schoeman, F., *Philosophical Dimensions of Privacy*. UK: Cambridge University Press, 346-402.

Gellman, R. (1995) "Public Reporter System Risks Privacy". *The National Law Journal*, Oct. 2 1995. <a href="http://library.ljextra.com/risk.html">http://library.ljextra.com/risk.html</a>

General Medical Services (Payments) Board (1997a) Financial and Statistical Analysis of Claims and Payments - 1996. Dublin: GMS Board.

General Medical Services (Payments) Board (1997b) Report for the Year Ended 31st December 1996. Dublin: GMS Board.

Gerbner, G., Mowlana, H. and Schiller, H., eds. (1996) Invisible crises: what conglomerate control of media means for America and the world. Oxford, Boulder, Colo.: Westview.

Gerstein, R. (1970) "Privacy and Self-Incrimination". Reprinted in Schoeman, F., Philosophical Dimensions of Privacy. UK: Cambridge University Press, 245-264.

Gerstein, R. (1978) "Intimacy and Privacy". Reprinted in Schoeman, F., *Philosophical Dimensions of Privacy*. UK: Cambridge University Press, 265-271.

Gewirth, A. (1998) "Epistemology of Human Rights". Pojman, L., ed. *Ethical theory: classical and contemporary readings* (3rd ed.). Belmont, Calif., London: Wadsworth, 720-732.

Gibbs, W. (1997) "Taking Computers to Task". *Scientific American*, Jul. 1997. <a href="http://www.sciam.com/0797issue/0797trends.htm">http://www.sciam.com/0797issue/0797trends.htm</a>

Gibbs, W. (1998) "The Web Learns to Read". Scientific American, June 1998. <a href="http://www.sciam.com/1998/0698issue/0698cyber.htm">http://www.sciam.com/1998/0698issue/0698cyber.htm</a>

Giddens, A. (1984) The Constitution of Society: outline of the theory of structuration. Cambridge: Polity.

Giddens, A. (1985) The Nation-State and Violence: Volume Two of a Contemporary Critique of Historical Materialism. Cambridge, Polity Press.

Giddens, A. (1991) The Consequences of Modernity. UK: Polity Press.

Giddens, A. (1993a) "Administrative Power and the Nation-State". Cassell, P., ed. *The Giddens Reader*. UK: The Macmillan Press, 257-266.

Giddens, A. (1993b) "The Nation-State and Military Power". Cassell, P., ed. *The Giddens Reader*. UK: The Macmillan Press, 266-283.

Giddens, A. (1993c) "A Critique of Foucault". Cassell, P., ed. The Giddens Reader. UK: The Macmillan Press, 228-235.

Gill, K., ed. (1996) Information society: new media, ethics, and postmodernism. London, New York: Springer.

GIS Law (1996) "The Supreme Court Considers Impact of Errors in Computer Data on Admissibility of Evidence". GIS Law 3(3), Fall 1996, 10-11.

Glave, J. (1998) "SynCrypt Promises Pain-Free Crypto". *Wired News*, Apr. 6 1998. <a href="http://www.wired.com/news/news/technology/story/11484.htm">http://www.wired.com/news/news/technology/story/11484.htm</a>

Glenny, M. (1996) The Fall of Yugoslavia: the Third Balkan War (3rd ed.). London: Penguin.

Goldsmith, S. (1997) *Privacy: how to live a private life free from big brother's interference*. Reading: Medina.

Goodchild, M. (1996) "Geographic Information Systems and spatial analysis in the social sciences". Aldenderfer, M. and Maschner, H., eds., *Anthropology, space and geographic information systems*. New York. - Oxford: Oxford University Press, 241-250.

Goodchild, M. (1997) *GIS, Spatial Analysis and the Geographical Key.* Presented at the European Research Conference on Socio-Economic Impacts of New Geographic Information Handling Technologies, Castel Vecchio Pastoli, Italy, 17-22 May 1997 (unpublished).

Goodwin, B. (1984) "Economic and Social Innovation in Utopia". Alexander, P. and Gill R., eds. *Utopias*. London: Gerald Duckworth & Co. Ltd, 69-83.

Goonatilake, S. (1990) The Evolution of Information: lineages in gene, culture and artefacts. London: Pinter.

Gordon, T. (1994) "Marketing Community Perspectives on Protecting Privacy". In Onsrud, H., ed., (1995) *Proceedings of the Conference on Law and Information Policy for Spatial Databases: Tempe, Arizona:* October 29-31 1994. <a href="http://www.spatial.maine.edu/tempe/tempe94.html">http://www.spatial.maine.edu/tempe/tempe94.html</a>

Gore, A. (1991) "Infrastructure for the Global Village". Scientific American, Sept. 1991, 108-111.

Gore, A. (1993) From Red Tape to Results: Creating a Government that Works Better and Costs Less. USA: Times Books.

Gould, P. and White, R. (1992) Mental Maps (2nd Ed.). London: Routledge.

Government of Ireland (1963) Official Secrets Act, 1963. Dublin: Stationary Office.

Government of Ireland (1988) Data Protection Act, 1988. Dublin: Stationary Office.

Government of Ireland (1991) Criminal Damage Act, 1991. Dublin: Stationary Office.

Government of Ireland (1995) Freedom of Information Bill, 1995. Dublin: Stationary Office.

Government of Ireland (1997a) Europol Act, 1997. Dublin: Stationary Office.

Government of Ireland (1997b) Freedom of Information Act, 1997. Dublin: Stationary Office.

Government of Ireland (1998) Social Welfare (Consolidation) Act, 1998. Dublin: Stationary Office.

Government of Ireland (1999) Finance Bill, 1999. Dublin: Stationary Office.

Government Publications Office (1937) Bunreacht na hÉireann (Constitution of Ireland). Dublin: Stationary Office.

Gow, D. (1998) "Millennium Bug Hunter Aims to Spread the Word". *The Guardian*, Mar. 11 1998. <a href="http://reports.guardian.co.uk/papers/19980310-23.htm">http://reports.guardian.co.uk/papers/19980310-23.htm</a>

Graves, D. (1997) "Legal First in E-Mail Libel Award". The Irish Independent, Jul. 7 1997.

Gerbner, G., Gross, L. and Melody, W., eds. (1973) Communication Technology and Social Policy: understanding the new 'cultural revolution'. New York, London [etc.]: Wiley-Interscience.

Gray, C. (1989) "The Cyborg Soldier: The US military and the post-modern warrior". Levidow, L. and Robins, K., eds. *Cyborg Worlds: The Military Information Society*. London: Free Association Books; 43-71.

Greenslade, R. (1998) "Digger Fails to Dodge Blows after Patten Book Debacle". *The Irish Times*, Mar 7 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0307/hom8.htm">http://www.irish-times.com/irish-times/paper/1998/0307/hom8.htm</a>

Gregory, D. (1994) Geographical Imaginations. Cambridge, MA., Oxford: Blackwell.

Gregory, D. and Urry, J. (1985) Social Relations and Spatial Structures. Basingstoke: Macmillan.

Grogan, D. (1998) "Role of Libraries seen as Crucial". *The Irish Times*, May 1 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0501/hom11.htm">http://www.irish-times/paper/1998/0501/hom11.htm</a>

Grossman, W. (1997) "Master of Your Domain". Scientific American, Oct. 1997. <a href="http://www.sciam.com/1097issue/1097cyber.htm">http://www.sciam.com/1097issue/1097cyber.htm</a>

Grossman, W. (1998a) "Bringing Down the Internet". Scientific American, May 1998. Association Books. <a href="http://www.sciam.com/1998/0598issue/0598cyber.htm">http://www.sciam.com/1998/0598issue/0598cyber.htm</a>>.

Grossman, W. (1998b) "Downloading as a Crime". Scientific American, March 1998. And Science (1998) Science (199

Gulker, C. (1997) "Without Strong Encryption, Government can Pretty Reliably Track Virtually Every Personal Datum We Possess". *The Independent*, July 15 1997. <a href="http://www.independent.co.uk/net/970715ne/story2.htm">http://www.independent.co.uk/net/970715ne/story2.htm</a>

Gurak, L. (1997) Persuasion and privacy in cyberspace: the online protests over Lotus MarketPlace and the Clipper chip. New Haven, CT., London: Yale University Press.

Gurton, A. (1997) "1 Jan 1999: A Date with Disaster?" *The Independent*, July 15 1997. <a href="http://www.independent.co.uk/net/970715ne/story6.htm">http://www.independent.co.uk/net/970715ne/story6.htm</a>

Hall, E. (1969) The Hidden Dimension: man's use of space in public and private. London: Bodley Head.

Hall, E. (1989) "Proxemics in the Arab World". In Stubbs, M. and Barnet S. The Little Brown Reader. USA: Harper Collins, 573-581.

Hall, E. (1996) Utopia Beckons or are the Barbarians at the Gate?: Emerging Legal Issues. Presented at a Conference on "The Internet: Emerging Legal Issues", Dublin, Mar. 6 1996 (unpublished).

Hall, P. (1984) "Utopian thought: A framework for social, economic and physical planning". Alexander, P. and Gill R., eds. *Utopias*. London: Gerald Duckworth & Co. Ltd, 189-195.

Hanson, R. (1994) "Can Wiretaps Remain Cost Effective?" Communications of the ACM 37(12) "Dec. 1994, 13-15. <a href="http://www.hss.caltech.edu/~hanson/wiretap-cacm.html">http://www.hss.caltech.edu/~hanson/wiretap-cacm.html</a>

Harley, J. (1983) "Meaning and Ambiguity in Tudor Cartography". In Tyacke, S., ed., *English Map Making* 1500-1650 : historical essays. London: British Library, 22-45.

Harley, J. (1987) "Innovation, Social Context and the History of Cartography: Review Article". In *Cartographica* 24(4), 59-68.

Harley, J. (1989) "Deconstructing the Map". In Cartographica 26(2), 1-20.

Harley, J. (1990) "Cartography, Ethics and Social Theory". In Cartographica 27(2), 1-23.

Harris, D., O'Boyle, M. and Warbick, C. (1995) Law of the European Convention on Human Rights. London: Butterworths.

Harris, P. (1997) "Bill Gates Predicts On-Lines Future for Africa". Yahoo!-Reuters News, Mar. 7 1997. <a href="http://www.yahoo.com/headlines/970307/tech/stories/gates\_2.html">http://www.yahoo.com/headlines/970307/tech/stories/gates\_2.html</a>

Harvey, D. (1982) The Limits to Capital. Oxford: Basil Blackwell.

Harvey, D. (1989) The Condition of Postmodernity: an enquiry into the origins of cultural change. Oxford: Blackwell.

Harvey, D. (1996) Justice, Nature and the Geography of Difference. Oxford: Blackwell.

Harvey, P. (1991) Medieval Maps. London: British Library.

Harvey, P. (1993) Maps in Tudor England. London: Public Record Office and the British Library.

Hayashi, A. (1998) "Lost in Cyberspace: Scientists Look for a Better Way to Search the Web". *Scientific American*, July 1998. <a href="http://www.sciam.com/1998/0798issue/0798techbus6.htm">http://www.sciam.com/1998/0798issue/0798techbus6.htm</a>

Hayashi, A. (1998) "Millennium Bug Zapper: A Radical Solution for the Year 2000 Problem". Scientific American, June 1998. <a href="http://www.sciam.com/1998/0698issue/0698techbus3.htm">http://www.sciam.com/1998/0698issue/0698techbus3.htm</a>

Hayes, D. (1989) "The Cloistered Work-place: Military electronics workers obey and ignore". Levidow, L. and Robins, K., eds. *Cyborg Worlds: The Military Information Society*. London: Free Association Books; 73-86.

Havnes, R. (1981) Geographical Images and Mental Maps. Basingstoke: Macmillan Education.

Haywood, T. (1995) Info-Rich - Info-Poor: Access and Exchange in the Global Information Society. UK: Bowker-Saur.

Heap, N., Thomas, R., Einon, G., Mason, R. and Mackay, H. (1995) *Information Technology and Society: A Reader*. London: Sage Publications.

Heasman, M. (1982) "Confidentiality and health service records". Raab, C., ed., Data protection and privacy: proceedings of a conference. London: Social Research Association, 34-40.

Heilbroner, R. (1994a) "Do Machines Make History?" In Smith, M. and Marx, L. Does Technology Drive History? The Dilemma of Technological Determinism. Cambridge, Massachusetts: The MIT Press, 53-65.

Heilbroner, R. (1994b) "Technological Determinism Revisited". In Smith, M. and Marx, L.. Does Technology Drive History? The Dilemma of Technological Determinism. Cambridge, Massachusetts: The MIT Press, 67-78.

Heldman, R. and Bystrzycki, T. (1995) The Telecommunications Information Millennium: a vision and plan for the global information society. New York, London: McGraw-Hill. Herman, E. and Chomsky, N. (1994) Manufacturing Consent: the political economy of the mass media. London: Vintage.

Hewitt, P. and National Council for Civil Liberties (1977) *Privacy: the information gatherers*. London: National Council for Civil Liberties.

Heylin, G. (1997) "Data Act Could Apply to Hacking Legislation". *The Irish Times*, May 11 1997. <a href="http://www.irish-times.com/irish-times/paper/1997/0512/>">http://www.irish-times.com/irish-times/paper/1997/0512/></a>

Heywood, D., Cornelius, S. and Carver, S. (1998) An introduction to geographical information systems. Harlow: Longman.

Hidgkinson, M. and Power, T. (1993) "Managing Market Share with Geodemographic Information". GIS Europe 2(9), Nov. 1993, 30-31.

Hobbes, T. (1998) "The Leviathan". Pojman, L., ed. *Ethical theory: classical and contemporary readings* (3rd ed.). Belmont, Calif., London : Wadsworth, 67-79.

Hoffman, P. (1998) "Internet Electronic Mail". *Scientific American*, Mar. 1998. <a href="http://www.sciam.com/1998/0398issue/0398working.htm">http://www.sciam.com/1998/0398issue/0398working.htm</a>

Holderness, M. (1998) "Moral Rights and Authors' Rights: The Keys to the Information Age". 1998 (1) The Journal of Information, Law and Technology (JILT). <a href="http://elj.warwick.ac.uk/jilt/infosoc/98">http://elj.warwick.ac.uk/jilt/infosoc/98</a> 1hold/>

Holloway, M. (1984) "The necessity of Utopia". Alexander, P. and Gill R., eds. Utopias. London: Gerald Duckworth & Co. Ltd, 179-188.

Holloway, M. (1998) "An Ethnologist in Cyberspace". Scientific American, Apr. 1998. <a href="http://www.sciam.com/1998/0498issue/0498profile.htm">http://www.sciam.com/1998/0498issue/0498profile.htm</a>

Honderich, T., ed., (1995) The Oxford Companion to Philosophy. UK: Oxford University Press.

Horovitz, D. (1998) "Israel Ignores US and PLO on New City Limits". *The Irish Times*, June 22 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0622/wor12.htm">http://www.irish-times.com/irish-times/paper/1998/0622/wor12.htm</a>

Horton, F. and Lewis, D., eds. (1990) Great Information Disasters: twelve prime examples of how information mismanagement led to human misery, political misfortune and business failure. London: Aslib.

House of Commons Committee of Public Accounts (1994) Twenty-ninth Report: Data Protection Controls and Safeguards. London: HMSO.

Hoy, D. (1986) Foucault: A Critical Reader. Oxford: Blackwell.

Huff, C. and Finholt, T., eds. (1994) Social Issues in Computing: putting computing in its place. New York, London: McGraw-Hill.

Hughes, A. (1996) "Britain comes into Line with European Copyright Licensing". *Managing Information* 3(3), March 1996, 34-35.

Hughes, T. (1994) "Technological Momentum". In Smith, M. and Marx, L. Does Technology Drive History? The Dilemma of Technological Determinism. Cambridge, Massachusetts: The MIT Press, 101-113.

Hurcom, S. (1997) "Pictures for Radio". Mapping Awareness 11(7), 30-33.

Hurwitt, M. and Thornton, P. (1989) Civil Liberties: The Liberty/NCCL Guide (4th ed.). UK: Penguin Books.

Huxhold, W. (1991) An introduction to urban geographic information systems. New York, Oxford: Oxford University Press.

Huxhold, W. and Levinsohn, A. (1995) Managing geographic information system projects. New York, Oxford: Oxford University Press.

Huxley, A. (1991) Brave New World. Harlow: Longman.

Information Society Commission (1998a) Information Society Commission Update. Issue no. 6, 28th May 1998. <a href="http://www.Infosocomm.ie">http://www.Infosocomm.ie</a>

Information Society Commission and Jupp, V. (1998b) Information Society Ireland: First report of Ireland's Information Society Commission. Dublin: Stationery Office.

Information Society Commission and Jupp, V. (1999) Information Society Ireland: Second report of Ireland's Information Society Commission. Dublin: Stationery Office. <a href="http://www.Infosocomm.ie/report2/report.pdf">http://www.Infosocomm.ie/report2/report.pdf</a>>

Information Society Steering Committee and Jupp, V. (1996) Information Society Ireland: Strategy for Action (Report of Ireland's Information Society Steering Committee). Dublin: Forfás.

Ingham, R. (1978) "Privacy and Psychology". Young, J., ed. Privacy. Chichester [etc.]: Wiley, 35-57.

Ingle, R. (1998) "Technology Erodes Privacy by Stealth". *The Irish Times*, Apr. 13 1998. < http://www.irish-times.com/irish-times/paper/1998/0413/fin2.htm>

Inness, J. (1992) Privacy, Intimacy, and Isolation. New York, Oxford: Oxford University Press.

INRA (Europe)-E.C.O. (1997a) Eurobarometer 46.1 Information Technology and Data Privacy: Report Produced for The European Commission (DG XV Internal Market and Financial Services). <http://www.ispo.cec.be/ecommerce/eurobaro.zip>

INRA (Europe)-E.C.O. (1997b) Information Technology and The Protection of Personal Data: Qualitative Study for The European Commission (DG XV Internal Market and Financial Services). <a href="http://www.ispo.cec.be/ecommerce/eurobar1.zip">http://www.ispo.cec.be/ecommerce/eurobar1.zip</a>

Institute of Information Science (Irish Branch) and American Society for Information Science (1982) Information and the Transformation of Society: [proceedings of the] First Joint International Conference of the Institute of Information Scientists and the American Society for Information Scientists [i.e. Science], 28-30 June, 1982, St. Patrick's College, Dublin, Ireland. Dublin: Institute of Information Scientists (Irish Branch).

International Working Group on Data Protection in Telecommunications (1996) "Data Protection on the Internet, Report and Guidance 'Budapest Draft'". *The Journal of Information Law and Technology (JILT)*. < http://elj.warwick.ac.uk/jilt/consult/iwgdp/default.htm>

Internet Australia (1995) "The Electronic Economy". Internet Australia 1(3), Mar. 1995. <a href="http://www.interaus.net/old/march/economy.html">http://www.interaus.net/old/march/economy.html</a>

Internet.com (1998) "Report Finds Fault with E-Com Sites". USA Today, June 10 1998. http://www.usatoday.com/life/cyber/tech/ctmeckle.htm>

Ireland, P. (1994) "Mapping at the Leading (and Trailing) Edge / From Cold War to Peace Dividend". Mapping Awareness 8(9), 16-19

Ireland, P. (1997) "Who Needs Maps?" Mapping Awareness 11(5), 24-26.

Irish Direct Marketing Association (1995) IDMA Code of Practice on Data Protection. Ireland: IDMA.

Irish Direct Marketing Association (1997) IDMA Members and Services Directory 1997-1998. Ireland: IDMA.

Irish Geodetic Surveying Liaison Group (1998) Geodetic Surveying in Ireland: National Report of the Current Status of the Geodetic Surveying Profession in Ireland. Ireland: Irish Geodetic Surveying Liaison Group.

Irish GIS Implementation Project (1980) Geographic information systems in Ireland: report by the GIS Implementation Project to the Minister for Science and Technology. Dublin: IGIP.

Irish Internet Association (1998a) Irish Online Survey. <a href="http://www.iia.ie/survey/index.html">http://www.iia.ie/survey/index.html</a>

Irish Internet Association (1998b) The Results of the Third IIA Internet Usage Survey. <a href="http://www.iia.ie/third\_surveyresults.html">http://www.iia.ie/third\_surveyresults.html</a>

Irish Internet Association (1999) The Results of the Fourth IIA Internet Usage Survey. <a href="http://www.iia.ie/fyi/surveyjune1999.html">http://www.iia.ie/fyi/surveyjune1999.html</a>

IRLOGI (1996) "Legal Protection of Geographical Information in Ireland". GIS Ireland: Newsletter of the Irish Organisation for Geographic Information 1(1), 8-10.

IRLOGI (1999a) "GeoDirectory launched at Dublin Castle: Ministers launch first National Address Database". GIS Ireland: Newsletter of the Irish Organisation for Geographic Information 3(1), 6.

IRLOGI (1999b) "ORACLW passes OpenGIS Test". GIS Ireland: Newsletter of the Irish Organisation for Geographic Information 3(2), 5.

Jackson, P. (1992) "Constructions of culture, representations of race: Edward Curtis's 'way of seeing'". Anderson, K. and Gale, F., eds. *Inventing places: studies in cultural geography*. Melbourne, Australia: Longman Cheshire. - New York: Wiley, Halsted Press, 89-106.

Jackson, S. (1998) "Domino theory and the dynamics of civil war". *The Irish Times*, Aug. 27 1998. < http://www.ireland.com/newspaper/opinion/1998/0827/opt2.htm>

Jackson, T. (1999) "Hard Feelings over Greeting Cards". *The Irish Times*, Jan. 4 1999. <a href="http://www.irish-times.com/irish-times/paper/1999/0104/cmp2.htm">http://www.irish-times/paper/1999/0104/cmp2.htm</a>

Jackson, W., ed., (1964) Politics and Geographic Relationships: Readings on the Nature of Political Geography. USA: Prentice-Hall.

Jackson, W. and Samuels, M., eds., (1971) Politics and Geographic Relationships: Toward a New Focus. USA: Prentice-Hall.

Jacob, J. (1994) "Statistics and Data Protection: A Global View". *Proceedings of the International Seminar* on *Statistical Confidentiality*, November 1994. Luxembourg: Office for Official Publications of the European Communities (1995), 43-46.

Jameson, F. (1990) Postmodernism or, The cultural logic of late capitalism. London: Verso.

Janicke, P. (1996) Patentability of Software in the United States. Presented at a Conference on "The Internet: Emerging Legal Issues", Dublin, Mar. 6 1996 (unpublished).

Jellinek, D. (1998a) "For Richer Not Poorer: Does the Net Reduce Global Inequalities or Exacerbate Them". *The Guardian Online*, 28 May 1998. <a href="http://go2.guardian.co.uk/theweb/896346381-harvard.htm">http://go2.guardian.co.uk/theweb/896346381-harvard.htm</a>

Jellinek, D. (1998b) "Net Profit Not for all Strap: Does Technology Exacerbate Differences Between Rich and Poor Countries Rather than Reduce Them". *The Irish Times*, June 8 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0608/cmp4.htm">http://www.irish-times/paper/1998/0608/cmp4.htm</a>

Jennings, M. (1993) "Reducing Risk and Uncertainty in Business: the challenge for geographical analysis". *Mapping Awareness* 7 (8), Oct. 1993, 43-45.

Jewitt, A.(1992) Maps for Empire: the first 2000 numbered War Office maps, 1881-1905. London: British Library.

Johnson, F. (1996) "Cyberpunks in the White House". Dovey, J., ed. *Fractal Dreams*. London: Lawrence & Wishart, 78-108.

Johnson, O. (1994) *Ethics: selections from classical and contemporary writers (7th ed)*. Fort Worth, London: Harcourt Brace College Publishers.

Johnston, R., Gregory, D. and Smith, D. (1986) The Dictionary of Human Geography (2nd ed.). Oxford: Blackwell Reference.

Jones, M., ed. (1974) Privacy. Newton Abbot [etc.]: David and Charles.

Jowell, R. (1982) "Ethical concerns in data collection". Raab, C., ed., *Data protection and privacy: proceedings of a conference*. London: Social Research Association, 43-52.

Kaplan, E., ed. (1988) Postmodernism and its discontents: theories, practices London: Verso.

Katz, A. (1998) "Stars Spar Over US Net Policy". *Wired News*, June 11 1998. <a href="http://www.wired.com/news/news/politics/story/12931.htm">http://www.wired.com/news/news/politics/story/12931.htm</a>

Katz, J. (1998) "A Restricted Revolution?" *Wired News*, Apr. 29 1998. <a href="http://www.wired.com/news/news/wiredview/story/11957.htm">http://www.wired.com/news/news/wiredview/story/11957.htm</a>

KDIS Online (1997) "CCTV - Big Brother in Bradford". *KDIS Online*, March 1997, update June 1 1998. <a href="http://merlin.legend.org.uk/~brs/cctv/kdis12.htm">http://merlin.legend.org.uk/~brs/cctv/kdis12.htm</a>

Keating, B. (1992) "Confidentiality at the National and International Level - Conflicts". *Proceedings of the International Seminar on Statistical Confidentiality, September 1992, Dublin.* Luxembourg: Office des Publications Officielles des Communautés Européennes (1993), 145-150.

Keena, C. (1997) "Debate on Role of Computers Urged". *The Irish Times*, Oct. 2 1997. <a href="http://www.irish-times.com/irish-times/paper/1997/1002/>

Kelleher, D. (1997) "Law is not Tough Enough for Hackers". *The Irish Times*, May 5 1997. <a href="http://www.irish-times.com/irish-times/paper/1997/0505/cmp3.htm">http://www.irish-times.com/irish-times/paper/1997/0505/cmp3.htm</a>

Kelleher, D. (1998a) "New Irish copyright laws are long overdue". *The Irish Times* of Jan 23, 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0223/cmp1.html">http://www.irish-times.com/irish-times/paper/1998/0223/cmp1.html</a>

Kelleher, D. (1998b) "The Contract Fillers". *The Irish Times*, Mar. 30 1998. < http://www.irish-times.com/irish-times/paper/1998/0330/cmp1.html>

Kelleher, D. (1998c) "US Pressure Forces Copyright Crackdown". *The Irish Times*, June 8 1998. <<u>http://www.irish-times.com/irish-times/paper/1998/0608/cmp3.htm</u>>

Kelleher, D. (1998d) "Who Must pay for Y2K?" *The Irish Times*, Oct. 12 1998. < http://www.irish-times.com/irish-times/paper/1998/1012/cmp3.htm>

Kelleher, D. and Murray, K. (1997) Information Technology Law in Ireland. Dublin: Butterworths.

Keller, B. (1998) Condemned to Repeat the Past: The Re-emergence of Misappropriation and Other Common Law Theories of Protection for Intellectual Property. <a href="http://www.cybercon98.org/wcm/keller.htm">http://www.cybercon98.org/wcm/keller.htm</a>

Kelly, J. (1967) Fundamental Rights in the Irish Law and Constitution (2nd ed.). Dublin: Allen Figgis.

Kelly, K. (1995) "Ephemeral Monopoly" (Interview of Kevin Kelly). New Perspectives Quarterly, Fall 1995, 29-34.

Kennedy, G. (1998) "Wexford had Lower Rating than Kerry, Figures Show". *The Irish Times*, Nov. 25 1998. <a href="http://www.irish-times/irish-times/paper/1998/1125/hom4.htm">http://www.irish-times/paper/1998/1125/hom4.htm</a>

Kennedy, M. (1996) The Global Positioning System and GIS: An Introduction. Michigan: Ann Arbor Press.

Kenen, J. (1997) "Panel Urges Privacy Protection of Health Records". *Reuters*, March 7 1997. <a href="http://www.yahoo.com/headlines/970307/tech/stories/privacy\_1.html">http://www.yahoo.com/headlines/970307/tech/stories/privacy\_1.html</a>

Kenny, G. (1996) GIS in Government. Presented at: GIS Ireland '96, Dublin; October 1996.

King, G. (1996) Mapping Reality. UK: Macmillan Press.

Kirwan, R. (1995a) National Mapping Databases - The O.S. View. Presented at IRLOGI GIS Workshop, TCD, June 14, 1995.

Kirwan, R. (1995b) "Preserving the Past". Mapping Awareness 9 (1), Feb. 1995, 28-31.

Kirwan, R. (1996) Ordnance Survey Policy. Presented at: GIS Ireland '96, Dublin; October 1996.

Kitchen R. (1997) Cyberspace, the world in the wires. UK: Wiley.

Kling, R. (1996) Computerization and Controversy: value conflicts and social choices (2nd ed.). San Diego, London: Academic Press.

Kliot, N. and Waterman, S., eds. (1983) *Pluralism and Political Geography: people, territory and state.* London: Croom Helm.

Koprowski, G. (1998) "The Love Boat's Wandering Eye". *Wired News*, 27 April (1998: <a href="http://www.wired.com/news/news/technology/story/1(1909.htm">http://www.wired.com/news/news/technology/story/1(1909.htm</a>

Kroker, A. (1992) The Possessed Individual: technology and postmodernity. London: Macmillan.

Kroker, A. (1996) "Virtual Capitalism". In Aronowitz, et al. *Technoscience and Cyberculture*. New York: Routledge, 167-179.

Kynge, J. (1998) "CHINA: Internet 'Subversive' on Trial". *The Financial Times* (FT.com), Dec. 5 1998. <a href="http://www.ft.com/hippocampus/qdf70a.htm">http://www.ft.com/hippocampus/qdf70a.htm</a>

Lafferty, E. (1998) "Uncle Sam Needs You!" *The Irish Times*, Nov. 24 1998. < http://www.irish-times/irish-times/paper/1998/1124/fea1.htm>

Lang, B. (1996) "Bricks and Bytes: Libraries in Flux". Daedalus (Journal of the American Academy of Arts and Sciences) 125(4), Fall 1996, 221-234.

Lappin, T. (1998) "Privacy and the Net". *The Irish Times Internet Supplement*. <a href="http://www.irish-times.com/internet/int16.htm">http://www.irish-times.com/internet/int16.htm</a>

Laudon, K., Traver, C. and Laudon, J. (1996) Information Technology and Society (2nd ed.). Cambridge, Mass., London: Course Technology, Inc.

Law Reform Commission (1992) Report on the Law Relating to Dishonesty. Dublin: Law Reform Commission.

Law Reform Commission (1996) Consultation Paper on Privacy: Surveillance and the Interception of Communication. Dublin: Law Reform Commission.

Law Reform Commission (1996) 18th Report of the Law Reform Commission. Dublin: Law Reform Commission.

Law Reform Commission (1998) Report on privacy: surveillance and the interception of communications. Dublin: Law Reform Commission.

Leen, M. (1998) "50 Years on, Rights are under new Pressures". *The Irish Times*, Mar. 28 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0328/wor9.htm">http://www.irish-times.com/irish-times/paper/1998/0328/wor9.htm</a>

Lehman, K.-D. (1996) "Making the Transitory Permanent: The Intellectual Heritage in a Digitized World of Knowledge". *Daedalus (Journal of the American Academy of Arts and Sciences)* 125(4), Fall 1996, 307-329.

Leibovich, M. (1998) No Bosses, No Distractions -- No Problem". *The Washington Post*, June 8 1998. <a href="http://washingtonpost.comwp-srv/WPlate/1998-06/08/0581-060898-idx.htm">http://washingtonpost.comwp-srv/WPlate/1998-06/08/0581-060898-idx.htm</a>

Leigh, D. (1980) The frontiers of secrecy: closed government in Britain. London: Junction Books.

Leith, P. (1997) "The Communication of Legislative Information in Ireland". 1997 (2) The Journal of Information, Law and Technology (JILT). <a href="http://elj.warwick.ac.uk/jilt/leginfo/97\_2leit/leith.htm/">http://elj.warwick.ac.uk/jilt/leginfo/97\_2leit/leith.htm/</a>

Lemos, R. (1998) Lloyds to Offer Firms Insurance Against Hackers. ZDNet <a href="http://www.zdnet.com/zdnn/content/zdnn/0423/309664.htm">http://www.zdnet.com/zdnn/content/zdnn/0423/309664.htm</a> Lenczowski, R. (1997) "The military as users and producers of global spatial data". Rhind, D., ed., *Framework for the world*. Cambridge: GeoInformation International, 85-110.

Lenk, K. (1997) "The Challenge of Cyberspatial Forms of Human Interaction to Territorial Governance and Policing". In Loader, B., ed., *The Governance of Cyberspace: Politics, Technology and Global Restructuring*. London: Routledge, 126-135.

Leslie, S. (1994) "Ethics, Professionalism and the AGI". Mapping Awareness 8 (5), June 1994, 18.

Levidow, L. and Robins, K., eds. (1989) Cyborg Worlds: The Military Information Society. London: Free Association Books.

Levidow, L. and Robins, K. (1989) "Towards a military information Society?". Levidow, L. and Robins, K., eds. *Cyborg Worlds: The Military Information Society*. London: Free Association Books; 159-177.

Lewis, T. (1997a) "Cyber View: www.batmobile.car". *Scientific American*, July 1997. <a href="http://www.sciam.com/0797issue/0797cyber.htm">http://www.sciam.com/0797issue/0797cyber.htm</a>

Lewis, T. (1997b) "We Don't Need No Regulation". *Scientific American*, Nov. 1997. <a href="http://www.sciam.com/1197issue/1197cyber.htm">http://www.sciam.com/1197issue/1197cyber.htm</a>

Licken, E. (1998a) "Commission out to get Best from Technology". *The Irish Times*, Feb. 13 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0213/fin15.htm">http://www.irish-times.com/irish-times/paper/1998/0213/fin15.htm</a>

Licken, E. (1998b) "New Engine for Information Age". *The Irish Times*, Feb. 13 1998. < http://www.irish-times.com/irish-times/paper/1998/0213/fin13.htm>

Licken, E. (1998c) "You too May be a Millionaire!" *The Irish Times*, Mar. 2 1998. < http://www.irish-times.com/irish-times/paper/1998/0302/cmp1.htm>

Lievesley, D. (1997) *The Tug of War Between Data Access and Confidentiality*. Presented at The European Research Conference on Socio-Economic Impacts of New Geographic Information Handling Technologies, Castel Vecchio Pastoli, Italy, 17-22 May 1997 (unpublished).

Lillington, K. (1998a) "Black Holes Expose Web Weakness". *The Irish Times*, July 10 1998. <a href="http://www.ireland.com/newspaper/finance/1998/0710/tech5.htm">http://www.ireland.com/newspaper/finance/1998/0710/tech5.htm</a>

Lillington, K. (1998b) "Clinton Goes Crypto in Ireland". *Wired News*, Sep. 4 1998. <a href="http://www.wired.com/news/news/politics/story/14831.htm">http://www.wired.com/news/news/politics/story/14831.htm</a>

Lillington, K. (1998c) " EU legislation on Net becomes law on Monday". *The Irish Times*, Oct. 23 1998. < http://www.ireland.com/newspaper/finance/1998/1023/tech4.htm>

Lillington, K. (1998d) "Surfing for Sex: The Real Power Behind Innovation on the Web". *The Guardian Online*, May 14 1998. <a href="http://go2.guardian.co.uk/theweb/895059985-porn.htm">http://go2.guardian.co.uk/theweb/895059985-porn.htm</a>

Lillington, K. (1999) "Consumer Watchdog Needed to Monitor Digital Revolution". *The Irish Times* (Business This Week), Feb. 12 1999.

Lloyd, I. (1996) "An Outline of the European Data Protection Directive". 1996 (1) The Journal of Information, Law and Technology (JILT). <a href="http://elj.warwick.ac.uk/jilt/dp/intros/">http://elj.warwick.ac.uk/jilt/dp/intros/</a>

Loader, B. (1997) The Governance of Cyberspace: Politics, Technology and Global Restructuring. London: Routledge.

Loader, B., ed. (1998) Cyberspace Divide: equality, agency, and policy in the information society. London: Routledge.

Locke, J. (1998) "Natural Rights". Pojman, L., ed. *Ethical theory: classical and contemporary readings* (3rd ed.). Belmont, Calif., London : Wadsworth, 705-710.

London Observer (1998) "Online May Be Another Gold Rush -- With Frontier Lawlessness". London Observer, June 7 1998.

Longley, P., ed. (1999) Geographical information systems: principles, techniques, applications, and management. New York, Chichester: John Wiley.

Louveaux, S. (1996) "Comments on the EU Data Protection Directive - The Belgian Perspective". 1996 (1) *The Journal of Information Law and Technology (JILT)*. <a href="http://elj.warwick.ac.uk/elj/jilt/dp/2louveau/">http://elj.warwick.ac.uk/elj/jilt/dp/2louveau/</a>

Lowenthal, D. and Bowden M., eds. (1976) *Geographies of the Mind: Essays in Historical Geography*. New York: Oxford University Press.

Loyn, H. (1982) The Norman Conquest. England: Hutchinson.

Lukes, S. (1984) "Marxism and Utopia". Alexander, P. and Gill R., eds. Utopias. London: Gerald Duckworth & Co. Ltd, 153-167.

Lyman, P. (1996) "What is a Digital Library? Technology, Intellectual Property, and the Public Interest". Daedalus (Journal of the American Academy of Arts and Sciences) 125(4), Fall 1996, 1-33.

Lyon, D. (1988) The Information Society: issues and illusions. Cambridge: Polity.

Lyon, D. (1995) "The Roots of the Information Society Idea". In Heap, N. et al., eds., *Information Technology and Society: A Reader*. London: Sage Publications, 54-73.

Lyons, M. (1998) "Information Age Town Untangles the Web". *The Irish Times*, Mar. 20 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0320/wor8.htm">http://www.irish-times.com/irish-times/paper/1998/0320/wor8.htm</a>

Lyotard, J.-F. (1984) *The Postmodern Condition: a report on knowledge* (translation by Geoff Bennington and Brian Massumi). Manchester: Manchester University Press.

MacIntyre, A. (1998) "A critique of Gewirth and the Notion of Rights". Pojman, L., ed. *Ethical theory : classical and contemporary readings* (3rd ed.). Belmont, Calif., London: Wadsworth, 732-734.

Mackay, H. (1995) "Theorising the IT/Society Relationship". In Heap, N. et al., eds., *Information Technology and Society: A Reader*. London: Sage Publications, 41-53.

Mackie, N. (1994) "Worst-Case Scenario: GIS at the Centre of the UK Nuclear Emergency Response". *Mapping Awareness* 8(7), 24-26.

Mackinder, H. (1969) "The scope and methods of geography" and "The geographical pivot of history". London: Royal Geographical Society.

Macmillan B. and Pierce, T. (1994) "Optimisation modelling in a GIS framework: the problem of political redistricting". Fotheringham, A., Rogerson, P., eds. (1994) *Spatial analysis and GIS*. London: Taylor & Francis, 221-246.

Madgwick, D. and Smythe, T. (1974) The invasion of privacy. London: Pitman.

Madsen, W. (1994) "Protecting Indigenous Peoples' Privacy from 'Eyes in the Sky'". In Onsrud, H., ed., (1995) *Proceedings of the Conference on Law and Information Policy for Spatial Databases: Tempe, Arizona:* October 29-31 1994. <a href="http://www.spatial.maine.edu/tempe/tempe94.html">http://www.spatial.maine.edu/tempe/tempe94.html</a>

Maguire, D. (1989) Computers in geography. Harlow: Longman Scientific & Technical.

Maguire, D. (1991) "An overview and definition of GIS". Maguire, D., Goodchild, M. and Rhind, D., eds., *Geographical information systems: principles and applications (2 vols.)*. UK: Longman Scientific & Technical, vol. 1, 9-20.

Maguire, D., Goodchild, M. and Rhind, D., eds. (1991) Geographical information systems: principles and applications (2 vols.). UK: Longman Scientific & Technical.

Malley, I. (1988) National Information Policy in the UK. Shepsted: IMPC.

Mann, M. (1986) The Sources of Social Power Vol 1: A History of Power from the Beginning to A.D. 1760. Cambridge: Cambridge University Press. Mann, M. (1993) The Sources of Social Power Vol.2: Rise of classes and nation-states 1760-1914. Cambridge: Cambridge University Press.

Marchenese, K., Pacheco, D. and Whitney, M. (1997) "Copyright, Copywrong". *The Washington Post.* <a href="http://washingtonpost.com/wp-srv/tech/analysis/copyright/intprop.htm">http://washingtonpost.com/wp-srv/tech/analysis/copyright/intprop.htm</a>

Margolin, M. (1998) "Protecting User Data". *Hotwired*, Dec. 4 1998. <a href="http://www.Hotwired.com/webmonkey/98/48/index4a.html">http://www.Hotwired.com/webmonkey/98/48/index4a.html</a>; index4a\_page2.html; index4a\_page3.html;

Marriott, S. (1998a) "Surfing on Top of the Internet Wave?" *The Irish Times*, June 23 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0623/fea2.htm">http://www.irish-times.com/irish-times/paper/1998/0623/fea2.htm</a>

Marriott, S. (1998b) "Why Women Don't Surf". The Irish Times, Aug. 10 1998. < http://www.irish-times.com/irish-times/paper/1998/0810/cmp1.htm>

Marsden, C. (1997) "The European Digital Convergence Paradigm: From Structural Pluralism to Behavioural Competition Law". 1997 (3) *The Journal of Information, Law and Technology (JILT)*. <http://elj.warwick.ac.uk/jilt/commsreg/97 3mars/>

Martin, D. (1996) Geographic information systems: socioeconomic applications (2nd ed.). London: Routledge.

Martin, F. (1982) "Lindop and after". Raab, Charles D., ed., Data protection and privacy: proceedings of a conference. London: Social Research Association, 1-8.

Martin, K. (1998) *Civil Liberties and National Security on the Internet.* <a href="http://www.cybercon98.org/wcm/martin.htm">http://www.cybercon98.org/wcm/martin.htm</a>

Martin, W. (1995) The Global Information Society. Aldershot: Aslib Gower.

Martinotti, G. (1997) *Many Voices, Lots of Noises: Problems in Building the European Social Science Resource Base.* Presented at The European Research Conference on Socio-Economic Impacts of New Geographic Information Handling Technologies, Castel Vecchio Pastoli, Italy, 17-22 May 1997 (unpublished).

Martius, M. (1982) "The Theory of Social Space in the Work of Henri Lefebvre". In Forrest, R., Henderson J. and Williams, P., Urban Political Economy and Social Theory. Aldershot: Gower, 160-185.

Marx, G. (1994) "Some Information-Age Techno-Fallacies and Some Principles for Protecting Privacy". In Onsrud, H., ed., (1995) *Proceedings of the Conference on Law and Information Policy for Spatial Databases: Tempe, Arizona:* October 29-31 1994. <a href="http://www.spatial.maine.edu/tempe/tempe94.html">http://www.spatial.maine.edu/tempe/tempe94.html</a>

Marx, L. (1994) "The Idea of 'Technology' and Postmodern Pessimism". In Smith, M. and Marx, L. Does Technology Drive History? The Dilemma of Technological Determinism. Cambridge, Massachusetts: The MIT Press, 237-257.

Mason, M. (1996) "The Yin and Yang of Knowing". Daedalus (Journal of the American Academy of Arts and Sciences) 125(4), Fall 1996, 161-171.

Mason, R., Mason, F. and Culnan, M. (1995) *Ethics of Information Management*. California, London: Sage Publications.

Masser, I. and Blakemore, M., eds. (1991) Handling geographical information: methodology and potential applications. UK: Longman Scientific & Technical.

Masser, I., Campbell, H. and Craglia, M., eds. (1996) GIS Diffusion. The Adoption of Geographical Information Systems in Local Government in Europe. London: Taylor and Francis.

Masser, I. and Craglia, M. (1997) *The European Geographic Information Infrastructure Debate*. Presented at The European Research Conference on Socio-Economic Impacts of New Geographic Information Handling Technologies, Castel Vecchio Pastoli, Italy, 17-22 May 1997 (unpublished).

Matsunaga, K. and Houston-Rogers, A. (1996) Personal Privacy Protection Versus Your Right to Know: How the use of GIS in this Computer Age has Overtaken your Individual Rights. <a href="http://www.esri.com/resources/userconf/proc96/TO200/PAP173/P173.htm">http://www.esri.com/resources/userconf/proc96/TO200/PAP173/P173.htm</a>

Matusow, H. (1972) "Communication Rather Than Technology". In Rowe, B. Privacy, Computers and You. Manchester: National Computing Centre, 31-36.

Mayer, C. (1998) "Class Warfare in the Air". *The Washington Post*, May 15 1998. <a href="http://washingtonpost.com/wp-srv/frompost/may98/airlines15.htm">http://washingtonpost.com/wp-srv/frompost/may98/airlines15.htm</a>

McCabe, H. (1998) "Speed: The E-Commerce Mantra". *Wired News*, Apr. 29 1998. <a href="http://www.wired.com/news/news/business/story/11970.htm">http://www.wired.com/news/news/business/story/11970.htm</a>

McCarthy, K. (1996) "Playing our ID Cards Right". The Evening Herald, Oct. 10 1996, 8.

McDonagh, M. (1998) Freedom of Information Law in Ireland. Dublin: Round Hall Sweet and Maxwell.

McGarry, K. (1993) The Changing Context of Information: an introductory analysis. London: Library Association.

McGoldrick, D. (1994) The Human Rights Committee: its role in the development of the International Covenant on Civil and Political Rights. Oxford: Clarendon.

McGonagle, M. (1996) "Respecting Privacy in the Media Age". *The Irish Times*, Oct. 25 1996. <a href="http://www.irish-times.com/irish-times/paper/1996/1025/">http://www.irish-times.com/irish-times/paper/1996/1025/</a>

McGonagle, M. (1998) "Information Act is First Step Towards New Regime". *The Irish Times*, Apr. 22 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0422/opt2.html">http://www.irish-times.com/irish-times/paper/1998/0422/opt2.html</a>

McGovern, G. (1996) Ireland: the digital age, the internet: a discussion document. Dublin: Forbairt.

McHoul, A. and Grace, W. (1995) A Foucault Primer: discourse, power, and the subject. London: UCL Press.

McMahon, B. and Binchy, W. (1990) Irish Law of Torts (2nd ed.). Dublin: Butterworth (Ireland) Ltd...

McNally, F. (1999) "Road Checkpoints to Tackle Welfare Fraud". *The Irish Times*, Feb. 9 1999. <a href="http://www.irish-times.com/irish-times/paper/1999/0209/hom12.htm">http://www.irish-times.com/irish-times/paper/1999/0209/hom12.htm</a>

McRae, H. (1996) The Internet and Society: What Lies in Store. Presented at a Conference on "The Internet: Emerging Legal Issues", Dublin, Mar. 6 1996 (unpublished).

Melaugh, D. (1998) Internet Filtration: Rights to Listen, Rights to Speak, Rights to Tune Out. <a href="http://www.cybercon98.org/wcm/melaugh-2.htm">http://www.cybercon98.org/wcm/melaugh-2.htm</a>

Mellors, C. (1978) "Governments and the Individual-their secrets and his privacy". Young, J., ed. *Privacy*. Chichester [etc.]: Wiley, 87-112.

Melody W. (1989) The Changing Role of Public Policy in the Information Economy. London: Imperial College of Science and Technology.

Melody, W., Salter, L. and Heyer, P. (1981) Culture, Communication, and Dependency: the tradition of H.A. Innis. Norwood, N.J: Ablex.

Menser, M. (1996) "Becoming-Heterarch: On Technocultural Theory, Minor Science, and the Production of Space". In Aronowitz, et al. *Technoscience and Cyberculture*. New York: Routledge, 293-316.

Menser, M. and Aronowitz, S. (1996) "On Cultural Studies, Science, and Technology". In Aronowitz, et al. *Technoscience and Cyberculture*. New York: Routledge, 7-27.

Metzl, J. (1996) "Searching for the Catalog of Catalogs". Daedalus (Journal of the American Academy of Arts and Sciences) 125(4), Fall 1996, 147-160.

Michael, James (1994) Privacy and human rights: an international and comparative study, with special reference to developments in information technology. Aldershot: Dartmouth.

Miller, H. (1998) "Rockets for the Rest of Us". *Wired 4.09*. <a href="http://www.wired.com/wired/4.09/es.space.htm">http://www.wired.com/wired/4.09/es.space.htm</a>

Miller, J. (1994) The Passion of Michel Foucault. UK: Flamingo.

Misa, T. (1994) "Retrieving Sociotechnical Change from Technological Determinism". In Smith, M. and Marx, L., *Does Technology Drive History? The Dilemma of Technological Determinism*. Cambridge, Massachusetts: The MIT Press, 115-141.

Mohammed E. (1999) "An Examination of Surveillance Technology and Their Implications for Privacy and Related Issues - The Philosophical Legal Perspective", 1999 (2) *The Journal of Information, Law and Technology (JILT)*. <a href="http://www.law.warwick.ac.uk/jilt/99-2/mohammed.html">http://www.law.warwick.ac.uk/jilt/99-2/mohammed.html</a>

Moisi, D. (1998) "At Long Last Universality of Justice Recognised". *The Irish Times*, Dec. 11 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/1211/opt2.htm">http://www.irish-times.com/irish-times/paper/1998/1211/opt2.htm</a>

Monmonier, M. (1989) Maps with the News: The Development of American Journalistic Cartography. USA: The University of Chicago Press.

Moore, N. (1998) "Rights and Responsibilities in an Information Society". 1998 (1) The Journal of Infomation, Law and Technology (JILT). <a href="http://elj.warwick.ac.uk/jilt/infosoc/98\_1moor/moore.htm/">http://elj.warwick.ac.uk/jilt/infosoc/98\_1moor/moore.htm/</a>

More, T. (1978) Utopia (trans. Paul Turner). UK: Penguin Classics.

Moriarty, T. (1998) "Microsoft Under Siege". *The Irish Times*, May 4 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0504/cmp2.htm">http://www.irish-times/paper/1998/0504/cmp2.htm</a>

Morley, D. and Robins, K. (1995) Spaces of Identity: Global Media, Electronic Landscapes and Cultural Boundaries. London: Routledge.

Morrill, R. (1997) "Progress in Political Geography". In Dikshit, R., Developments in Political Geography: A Century of Progress. New Delhi, London: Sage Publications Ltd., 355-374.

Morrison, A. (1984) "Uses of Utopia". Alexander, P. and Gill R., eds. Utopias. London: Gerald Duckworth & Co. Ltd, 139-151.

Morrison, J. (1997) "Topographical mapping in the twenty-first century". Rhind, D., ed., *Framework for the world*. Cambridge: GeoInformation International, 14-27.

Morton, O. (1998) "Private Spy". Wired News, 4 April 1998: < http://www.wired.com/wired/5.08/spy.html>

Morwood, J. (1995) The Oxford Latin Minidictionary. UK: Oxford University Press.

Mosco, V. (1989) "Strategic Offence: Star Wars as military hegemony". Levidow, L. and Robins, K., eds. *Cyborg Worlds: The Military Information Society*. London: Free Association Books; 87-112.

Moss, B. (1998) Personal Communication.

Mudrooroo (1994) Aboriginal Mythology: an A-Z spanning the history of the Australian Aboriginal people from the earliest legends to the present day. London: Aquarian.

Muehrcke, P. (1981) "Maps in Geography". In *Cartographica:* Monograph 27: Maps in Modern Geography - Geographical Perspectives on the New Cartography, 18(2), Summer 1981, 1-41.

Muir, R. (1975) Modern Political Geography. London: Macmillan.

Muir R. (1997) Political Geography: a new introduction. London: Macmillan Press.

Muir, R. and Paddison, R. (1981) Politics, Geography and Behaviour. London: Methuen.
Mulqueen, É. and Balls, R. (1997) "Loyalty Card Game Reveals Consumer Spending Trends". *The Irish Times*, Nov 13 1997. <a href="http://www.irish-times.com/irish-times/paper/1997/1114/fin70.htm">http://www.irish-times.com/irish-times/paper/1997/1114/fin70.htm</a>

Mulvihill, M. (1996) "The First Weaver". *The Irish Times*, Dec. 23 1996. <a href="http://www.irish-times.com/irish%2Dtimes/paper/1996/1223/cmp2.htm">http://www.irish-times.com/irish%2Dtimes/paper/1996/1223/cmp2.htm</a>

Murphy, R. (1964) "Social Distance and the Veil". Reprinted in Schoeman, F., *Philosophical Dimensions of Privacy*. UK: Cambridge University Press, 34-55.

Myers, K. (1998) "An Irishman's Diary". The Irish Times, Dec. 17 1998. <a href="http://www.irish-times/irish-times/paper/1998/1217/opt4.htm">http://www.irish-times/irish-time

Negroponte, N. (1996) Being Digital. London: Hodder & Stoughton.

Newbigin, M. (1915) Geographical Aspects of Balkan Problems in their relation to the Great European War. London: Constable.

Niblett, G. (197) "Computers and Privacy". In Rowe, B. Privacy, Computers and You. Manchester: National Computing Centre, 17-23.

Nichols, S. (1996) "Discover: Legal Information". Managing Information 3(3), March 1996, 27-30.

Nietzsche, F. (1992) Ecce Homo. England: Penguin Books Ltd.

Nimmer, R. (1996) *Copyright in Global Cyberspace*. Presented at a Conference on "The Internet: Emerging Legal Issues", Dublin, Mar. 6 1996 (unpublished).

Nobel, J. (1994) "Data Confidentiality and Data Access - Practical and Legal Issues in the Netherlands". *Proceedings of the International Seminar on Statistical Confidentiality*, November 1994. Luxembourg: Office for Official Publications of the European Communities (1995), 207-214.

Noble, D. (1989) "Mental Materiel: The militarization of learning and intelligence in US education". Levidow, L. and Robins, K., eds. *Cyborg Worlds: The Military Information Society*. London: Free Association Books; 13-41.

Norton-Taylor, R. (1998) "Secrets and Files". *The Guardian*, Apr. 14 1998. <a href="http://reports.guardian.co.uk/papers/19980413-28.htm">http://reports.guardian.co.uk/papers/19980413-28.htm</a>

O'Brien, T. (1998) "Computer Inventory Raises Value of Irish Forestry". *The Irish Times*, Nov. 17 1998. <a href="http://www.irish-times/irish-times/paper/1998/1117/hom11.htm">http://www.irish-times/paper/1998/1117/hom11.htm</a>

O'Connor, A. (1996) "Warning on Privacy over New Social Service Card". *The Irish Times*, Oct. 1 1996. <a href="http://www.irish-times.com/irish-times/paper/1996/1001/>">http://www.irish-times.com/irish-times/paper/1996/1001/></a>

O'Connor, A. (1998) "Doctor Claims that Legislation is Unworkable". *The Irish Times*, Apr. 17 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0417/hom25.htm">http://www.irish-times.com/irish-times/paper/1998/0417/hom25.htm</a>

O'Dell, E. (1996) Copyright and Databases. Irish and European Dimensions. Presented at a Conference on "The Internet: Emerging Legal Issues", Dublin, Mar. 6 1996 (unpublished).

O'Harrow, R. Jr. (1998a) "Are Data Firms Getting too Personal?". *The Washington Post*, March 8 1998: <a href="http://washingtonpost.com/wp-srv/frompost/march98/privacy8.htm">http://washingtonpost.com/wp-srv/frompost/march98/privacy8.htm</a>

O'Harrow, R. Jr. (1998b) "For Sale on the Web: Your Financial Secrets". *The Washington Post*, June 11 1998. <a href="http://washingtonpost.com/wp-srv/WPlate/1998-06/11/1551-061198-idx.htm">http://washingtonpost.com/wp-srv/WPlate/1998-06/11/1551-061198-idx.htm</a>

O'Harrow, R. Jr. (1998c) "Picking up on 'Cookie' Crumbs". *The Washington Post*, Mar. 9 1998. <a href="http://washingtonpost.com/wp-srv/frompost/march98/sidebars/cookie10.htm">http://washingtonpost.com/wp-srv/frompost/march98/sidebars/cookie10.htm</a>

O'Harrow, R. Jr. (1998d) "White House Effort Addresses Privacy". *The Washington Post*, May 14 1998. <a href="http://washingtonpost.com/wp-srv/politics/govt/fedguide/stories/gore051498.htm">http://washingtonpost.com/wp-srv/politics/govt/fedguide/stories/gore051498.htm</a>

O'Keefe, B. (1999) "Tax Controversies Prompt Increased Powers in Bill" *The Irish Times* (Business This Week), Feb. 12 1999, 3.

O'Malley, C. (1998) "Apocalypse Not: For Most Private Computers, the Notorious Year 2000 Glitch won't be the End of the World. For the Feds, However, It Could Be a Disaster". *Time* 151 (23), June 15 1998. <a href="http://pathfinder.com/time/magazine/1998/dom/980615/technology\_apocalypse.htm">http://pathfinder.com/time/magazine/1998/dom/980615/technology\_apocalypse.htm</a>

Ó Marcaigh, F. (1997a) "Internet Hero Takes a Fall". *The Irish Times*, Dec. 8 1997. <a href="http://www.irish-times.com/irish%2Dtimes/paper/1997/1208/cmp4.htm">http://www.irish-times.com/irish%2Dtimes/paper/1997/1208/cmp4.htm</a>

Ó Marcaigh, F. (1997b) "Publish and be Scanned". *The Irish Times*, July 28 1997. <a href="http://www.irish-times.com/irish%2Dtimes/paper/1997/0728/cmp1.htm">http://www.irish-times.com/irish%2Dtimes/paper/1997/0728/cmp1.htm</a>

Ó Marcaigh, F. (1997c) "Reach for the Skies". *The Irish Times*, May 5 1997. <a href="http://www.irish-times.com/irish-times/paper/1997/0505cmp2.htm">http://www.irish-times/paper/1997/0505cmp2.htm</a>

Ó Marcaigh, F. (1998a) "10,250 in Irish Email Directory". *The Irish Times*, Mar. 9 1998. < http://www.irish-times.com/irish-times/paper/1998/0309/cmp4.htm>

Ó Marcaigh, F. (1998b) "Who Fears to Speak in '98". *The Irish Times*, May 4 1998. < http://www.irish-times.com/irish-times/paper/1998/0504/cmp1.htm>

Ó Marcaigh, F. (1998c) "Tools for Protecting Privacy on the Internet". *The Irish Times* Internet Supplement. <a href="http://www.irish-Times.com/internet/int10.htm">http://www.irish-Times.com/internet/int10.htm</a>

Ó Marcaigh, F. (1999) "Experts Differ on Danger of Virus". *The Irish Times*, Jan. 4 1999. < http://www.irish-times.com/irish-times/paper/1999/0104/cmp5.htm>

O'Regan, E. and McKenna, G. (1998) "New Law Means Patients can see Files Soon". *The Irish Independent*, Apr. 22 1998. <a href="http://www.independent.ie/1998/111/d03.shtm">http://www.independent.ie/1998/111/d03.shtm</a>

O'Siochru, S. (1997) "The Government's New Information Society Strategy: But is Inclusion Excluded?" Ireland, Europe and the Global Information Society: A Conference for Social Scientists, Dublin, 24 and 25 April 1997 <a href="http://www.dcu.ie/communications/iegis/Siochru.htm">http://www.dcu.ie/communications/iegis/Siochru.htm</a>

O'Sullivan, R. (1998) "Lecturer Says Official Secrets Act Still a Threat". *The Irish Times*, Jun.13 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0613/hom4.htm">http://www.irish-times.com/irish-times/paper/1998/0613/hom4.htm</a>

O'Sullivan, K. (1998) "People Worried About Financial Secrecy". *The Irish Times*, Dec. 15 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/1215/hom8.htm">http://www.irish-times.com/irish-times/paper/1998/1215/hom8.htm</a>>.

O'Sullivan P. (1985)"The Geopolitics of Deterrence". In Pepper and Jenkins. *The Geography of Peace and War*. London: Basil Blackwell, 29-41.

Obermeyer, N. and Pinto, J. (1994) *Managing geographic information systems*. New York, London: Guilford Press.

Odom, A. (1998) GIS for Marketing Strategies. Presented at GIS Ireland 98, Malahide, Dublin.

Office of the Data Protection Commissioner (1999) Personal Communication on the 23rd October, 1999.

Office of the Information Commissioner (1998) *Guide to the Act* (Freedom of Information Act, 1997). <a href="http://www.irlgov.ie/oic/guide.htm">http://www.irlgov.ie/oic/guide.htm</a>

Okerson, A. (1996a) "Who owns digital works?" Scientific American July 1996, 80-84. <a href="http://www.sciam.com/0796issue/0796okerson.htm">http://www.sciam.com/0796issue/0796okerson.htm</a>

Okerson, A. (1996b) "Buy or Lease? Two Models for Scholarly Information at the End (or Beginning) of an Era". Daedalus (Journal of the American Academy of Arts and Sciences) 125(4), Fall 1996, 55-76.

Oliver, E. (1999) "New Copyright Bill Creates Fresh Penalties". *The Irish Times*, Apr. 10 1999. <a href="http://www.irish-times.com/irish-times/paper/1999/0410/fin16.htm">http://www.irish-times.com/irish-times/paper/1999/0410/fin16.htm</a>

Onsrud, H. (1993) "Evidence Generated from GIS". GIS Law 1 (3), 1-9.

Onsrud, H. (1997) *Geographic Information and Ethical Issues*. Presented at The European Research Conference on Socio-Economic Impacts of New Geographic Information Handling Technologies, Castel Vecchio Pastoli, Italy, 17-22 May 1997 (unpublished).

Onsrud, H.; Johnson, J. and Lopez, X. (1994) "Protecting Personal Privacy in Using Geographic Information Systems". In Onsrud, H., ed., (1995) *Proceedings of the Conference on Law and Information Policy for Spatial Databases: Tempe, Arizona:* October 29-31 1994. <a href="http://www.spatial.maine.edu/tempe/tempe94.html">http://www.spatial.maine.edu/tempe/tempe94.html</a>

Openshaw, S., Blake, M. and Wymer, C. (1994) "Using Neurocomputing Methods to Classify Britain's Residential Areas". *GIS Research UK*, April 1994.

Openshaw S. and Steadman P. (1985) "Domesday Revisited". In Pepper and Jenkins. *The Geography of Peace and War*. London: Basil Blackwell, 107-125.

Organisation for Economic Co-operation and Development (1994) *Privacy and data protection: issues and challenges.* Paris: OECD.

Organisation of African Unity (1981) African [Banjul] Charter on Human and Peoples' Rights, adopted June 27, 1981. <a href="http://www1.umn.edu/humantts/instree/zlafchar.htm">http://www1.umn.edu/humantts/instree/zlafchar.htm</a>

Organization of American States (1948) American Declaration of the Rights and Duties of Man, O.A.S. Res. XXX, adopted by the Ninth International Conference of American States. <http://www1.umn.edu/humanrts/oasinstr/zoas2dec.htm>

Organization of American States (1969) American Convention on Human Rights, O.A.S. Treaty Series No. 36, 1144 U.N.T.S. 123 entered into force July 18, 1978. <a href="http://www1.umn.edu/humants/oasinstr/zoas3con.htm">http://www1.umn.edu/humants/oasinstr/zoas3con.htm</a>

Orwell, G. (1998) *Nineteen Eighty-Four*. London: Penguin (Originally published: London: Secker and Warburg, 1949)

Oosterom, P. (1993) Reactive data structures for geographic information. Oxford: Oxford University Press.

Ovington, M. (1999) Personal Communication.

Paasi A., (1996) Territories, boundaries, and consciousness: the changing geographies of the Finnish-Russian border. England: John Wiley and Sons.

Page, J. (1997) "Dial M for Mapping". Mapping Awareness 11(2), 25-27.

Parker, G. (1985) Western geopolitical thought in the twentieth century. London: Croom Helm.

Parker G., (1998) Geopolitics: Past, Present and Future. London: Pinter.

Parker, G. and Dikshit, R. (1997) "Boundary Studies in Political Geography: Focus on the Changing Boundaries of Europe". In Dikshit, R., *Developments in Political Geography: A Century of Progress*. New Delhi, London: Sage Publications Ltd., 170-203.

Parkes, H. (1968) The United States of America: A History. New York: Alfred A. Knopf.

Pascoe, E. (1998a) "Building Trust in the Internet". *The Independent*, Mar. 17 1998. <a href="http://www.independent.co.uk/net/980317ne/story2.html">http://www.independent.co.uk/net/980317ne/story2.html</a>

Pascoe, E. (1998b) "US and EU Skirmish over Domain Names". The Independent, Mar. 3 1998. <a href="http://www.independent.co.uk/net/980303ne/story2.html">http://www.independent.co.uk/net/980303ne/story2.html</a>

Pattie, N., (1993) "Eye Spy Farm Fraud / Farmwatch UK". GIS Europe 2(9), Nov. 1993, 22-24.

Pawson, E. (1992) "Two New Zealands: Maori and European". Anderson, K. and Gale, F., eds. *Inventing places: studies in cultural geography*. Melbourne, Australia: Longman Cheshire - New York: Wiley, Halsted Press, 15-33.

Peck, J., ed., (1987) The Chomsky reader. London: Serpent's Tail.

Peet, R. (1977) Radical Geography: alternative viewpoints on contemporary social issues. London: Methuen.

Peet, R. (1998) Modern Geographical Thought. London: Blackwell Publishers.

Pepper, D. and Jenkins, A., eds., (1985) The Geography of Peace and War. Oxford: Basil Blackwell Ltd..

Phillips, R. (1997) Mapping Men and Empire: A Geography of Adventure. London: Routledge.

Phillips, T. (1998) "Dial S for Satellite". *The Guardian*, Jan. 29 1998. <a href="http://go2.guardian.co.uk/technology/885998273-satellite.htm">http://go2.guardian.co.uk/technology/885998273-satellite.htm</a>

Phillips, W. and Phillips, C. (1992) The Worlds of Christopher Columbus. UK: Cambridge University Press.

Pincus, W. (1998) "Tenet Boosts Oversight on Collection of Data". *The Washington Post*, June 5 1998. <a href="http://washingtonpost.com/wp-srv/WPcap/1998-06/05/023r-060598-idx.htm">http://washingtonpost.com/wp-srv/WPcap/1998-06/05/023r-060598-idx.htm</a>

Plato (1993) The Republic (translated by Robin Waterfield). Oxford, New York: Oxford University Press.

Plunkett, C. (1996) Branding, Advertising and the Use of Names on the Internet. Presented at a Conference on "The Internet: Emerging Legal Issues", Dublin, Mar. 6 1996 (unpublished).

Pojman, L., ed. (1998) *Ethical theory: classical and contemporary readings* (3rd ed.). Belmont, Calif., London: Wadsworth.

Pollack, A. (1999) "School Computers the Key - Ahern". *The Irish Times*, Feb. 9 1999. <a href="http://www.irish-times.com/irish-times/paper/1999/0209/hom11.htm">http://www.irish-times/paper/1999/0209/hom11.htm</a>

Pollitt, M. (1994) "Mapping the Political Landscape - a Question of Balance". *Mapping Awareness* 8 (6), July 1994, 42-44.

Porter, P. and Lukerman F. (1976) "The Geography of Utopia". Lowenthal, D. and Bowden M., eds. Geographies of the Mind: Essays in Historical Geography. New York: Oxford University Press, 197-223.

Posner, R. (1978) "An Economic Theory of Privacy". Reprinted in Schoeman, F., *Philosophical Dimensions of Privacy*. UK: Cambridge University Press, 333-345.

Post, D. (1996) "Cancelbunny and Lazarus Battle it out on the Frontier of Cyberspace - and Suggest the Limits of Social Contracts". *Reason*, April 1996, 29-33.

Poster, M. (1990) The Mode of Information: poststructuralisms and social context. Cambridge: Polity Press in association with Basil Blackwell,

Postrel, V. (1998a) The Lessons of Email Deceit. < http://www.cybercon98.org/wcm/postrel-email.htm>

Postrel, V. (1998b) "Technocracy R.I.P. The Rise of Technology Signals the Fall of Technocracy". *Wired* 6.01: Electrosphere, Jan. 1998. <a href="http://www.wired.com/wired/6.01/postrel.htm">http://www.wired.com/wired/6.01/postrel.htm</a>

Poulantzas, N. (1978) State, Power, Socialism (translated by Patrick Camiller). London: NLB.

Prosser, W. (1960) "Privacy [A Legal Analysis]". Reprinted in Schoeman, F., *Philosophical Dimensions of Privacy*. UK: Cambridge University Press, 104-155.

Punch, M. (1996) Personal Communication.

Quinn, J. (1999) Privacy. Manchester: Carcanet.

Quittner, J. (1997) "Invasion of Privacy". Time, Aug. 25 1997, 41-47.

Quittner, J. (1998a) "Protect Your Kids: Josh Quittner's Tips on Ensuring Your Children's Privacy Online". *Time*, June 15 1998. <a href="http://pathfinder.com/time/personal\_time/980615/technology.htm">http://pathfinder.com/time/personal\_time/980615/technology.htm</a>

Quittner, J. (1998b) "Tell the Kids to Fib: A U.S. Agency Says Laws are Needed to Protect Children's Privacy Online. But You Can Do Better". *Time*, June 15 1998. <a href="http://pathfinder.com/time/magazine/980615/personal\_*Time\_your\_techn20.htm">http://pathfinder.com/time/magazine/980615/personal\_Time\_your\_techn20.htm</a>* 

Raab, C., ed. (1982) Data protection and privacy: proceedings of a conference. London: Social Research Association.

Raab, C. (1994) "European Perspectives on Privacy". In Onsrud, H., ed., (1995) *Proceedings of the Conference on Law and Information Policy for Spatial Databases: Tempe, Arizona:* October 29-31 1994. <a href="http://www.spatial.maine.edu/tempe/tempe94.html">http://www.spatial.maine.edu/tempe/tempe94.html</a>

Raab, C. (1997) "Privacy, Democracy, Information". In Loader, B., ed., *The Governance of Cyberspace: Politics, Technology and Global Restructuring*. London: Routledge, 155-174.

Raab, C., Commission of the European Communities, Directorate General XV (Internal Market and Financial Services) (1998) *Application of a methodology designed to assess the adequacy of the level of protection of individuals with regard to processing personal data: test of the method on several categories of transfer: final report.* Luxembourg: Office for Official Publications of the European Communities.

Rachels, J. (1975) "Why Privacy is Important". Reprinted in Schoeman, F., *Philosophical Dimensions of Privacy*. UK: Cambridge University Press, 290-299.

Rachels, J. (1986) The Elements of Moral Philosophy (2nd ed). New York, London: McGraw-Hill.

Rae, J. and Mulcahey, M. (1993) "Target Marketing in a Changing Economic Climate". *Mapping Awareness* 7 (8), Oct. 1993, 39-41.

Raymond, E. (1998) The Future of Open Source. < http://www.cybercon98.org/wcm/raymond.htm>

Redmond, L. (1997) "Big Business is Watching You". *The Irish Times*, Sept. 8 1997. < http://www.irish-times.com/irish-times/paper/1997/0908/>

Redmond, L. (1998a) "It's the End of the World as We Know It". *The Irish Times*, Aug. 10 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0810/cmp2.htm">http://www.irish-times.com/irish-times/paper/1998/0810/cmp2.htm</a>

Redmond, L. (1998b) "Y2K - The State of the Nation?" *The Irish Times*, June 22 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0622/cmp1.htm">http://www.irish-times/paper/1998/0622/cmp1.htm</a>

Reeve, D. (1997) GIS Database Technologies: From Boutique to Mainstream. Presentation at GIS Ireland '97, Dublin: October 1997.

Reiman, J. (1976) "Privacy, Intimacy, and Personhood". Reprinted in Schoeman, F., *Philosophical Dimensions of Privacy*. UK: Cambridge University Press, 300-316.

Repsilber, D. (1992) "Safeguarding Secrecy in Aggregative Data". *Proceedings of the International Seminar on Statistical Confidentiality, September 1992, Dublin.* Luxembourg: Office des Publications Officielles des Communautés Européennes (1993), 353-368.

Reuters (1998a) "Digital Copyright Bill Advances". *Wired News*, Apr. 30 1998. <a href="http://www.wired.com/news/news/politics/story/12034.htm">http://www.wired.com/news/news/politics/story/12034.htm</a>

Reuters (1998b) "Singapore Vows Property Protection". *Wired News*, Apr. 28 1998. <a href="http://www.wired.com/news/news/politics/story/11956.htm">http://www.wired.com/news/news/politics/story/11956.htm</a>

Reville, W. (1999) "Bad Scientific Idea That Ended in Disaster". *The Irish Times*, Feb. 8 1999. <a href="http://www.irish-times.com/irish-times/paper/1999/0208/sci2.htm">http://www.irish-times.com/irish-times/paper/1999/0208/sci2.htm</a>

Rheingold, H. (1998) Virtual Communities, Phoney Communities? <a href="http://www.cybercon98.org/wcm/rheingold.htm">http://www.cybercon98.org/wcm/rheingold.htm</a>

Rhind, D. (1988) "A GIS Research Agenda". IJGIS 2, 23-28.

Rhind, D. (1991) "Counting the people: the role of GIS". Maguire, D., Goodchild, M. and Rhind, D., eds. (1991) *Geographical information systems: principles and applications (2 vols.)*. UK: Longman Scientific & Technical, vol. 2, 127-137.

Rhind, D. (1995) "Spatial Data from Government". The AGI Sourcebook for Geographic Information Systems. London: AGI, 101-105.

Rhind, D., ed. (1997) Framework for the world. Cambridge: GeoInformation International.

Rhind, D. (1997) "Introduction". Rhind, D., ed., Framework for the world. Cambridge: GeoInformation International, 1-13.

Rich, J. and Menser, M. (1996) "Establishing Markers in the Milieu". In Aronowitz, et al. *Technoscience and Cyberculture*. New York: Routledge, 1-4.

Rimm, M. (1995) "Marketing Pornography on the Information Superhighway: A Survey of 917,410 Images, Description, Short Stories and Animations Downloaded 8.5 Million *Times* by Consumers in Over 2000 Cities in Forty Countries, Provinces and Territories". *Georgetown Law Journal* 83(5). <a href="http://trfn.pgh.pa.us/guest/mrstudy.html">http://trfn.pgh.pa.us/guest/mrstudy.html</a>

Rip, A., Thomas J. and Schot, J., eds. (1995) Managing Technology in Society. London, New York: Pinter Publishers.

Robertson, A. and Merrills, J. (1996) *Human Rights in the World: an introduction to the study of the international protection of human rights (4th ed.)*. Manchester: Manchester University Press.

Robertson, G. (1989) Freedom, the Individual and the Law (6th ed.). UK: Penguin Books.

Robins, K. (1996) "Cyberspace and the World We Live In". Dovey, J., ed. *Fractal Dreams*. London: Lawrence & Wishart, 1-30.

Robinson, A. (1982) Early Thematic Mapping in the History of Cartography. USA: The University of Chicago Press.

Robinson, A., Sale, R., Morrison J., and Muehrcke, P. (1984) *Elements of Cartography*. USA: John Wiley and Sons.

Rodriguez, S. (1998) Email: The Emotional Crutch of the '90s? How Email Affects Students' Lives Academically, Socially, and Even Romantically. <a href="http://www.cybercon98.org/wcm/ridriguez-email.htm">http://www.cybercon98.org/wcm/ridriguez-email.htm</a>

Rogerson, P. and Fotheringham, A. (1994) "GIS and spatial analysis: introduction and overview". Fotheringham, A., Rogerson, P., eds. (1994) *Spatial analysis and GIS*. London: Taylor & Francis, 1-10.

Rorty, R. (1989) Contingency, Irony and Solidarity. Cambridge: Cambridge University Press.

Ross, A. (1996) "Earth to Gore, Earth to Gore". In Aronowitz, et al. *Technoscience and Cyberculture*. New York: Routledge, 111-121.

Ross, C. (1972) "How the Computer is Changing the Dimensions of the Problem". In Rowe, B. Privacy, Computers and You, 25-29.

Rowe B., ed., (1972) Privacy, computers and you. Manchester: National Computing Centre.

Rowland D. (1998) "Cyberspace - A Contemporary Utopia?". 1998 (3) The Journal of Information, Law and Technology (JILT). <a href="http://www.law.warwick.ac.uk/jilt/98-3/rowland.html">http://www.law.warwick.ac.uk/jilt/98-3/rowland.html</a>

Rowlands, I. and Vogel, S. (1991) Information Policies: A Sourcebook. London, Los Angeles: Taylor Graham.

Ruiz, B. (1997) Privacy in telecommunications: a European and an American Approach. The Hague, London: Kluwer Law International.

Rumley, D. and Minghi, J. (1991) The Geography of Border Landscapes. London: Routledge.

Rushkoff, D. (1998) "Tilting at Windows". *The Guardian Online*, June 4 1998. <a href="http://go2.guardian.co.uk/computing/896877881-second.htm">http://go2.guardian.co.uk/computing/896877881-second.htm</a>

Russell, B. (1993) History of Western Philosophy (And its Connection with Political and Social Circumstances from the Earliest Times to the Present Day). London: Routledge.

Rybaczuk, K. and Mac Mahon, H. (1995) Accessing Geographic Information for Ireland. Dublin: Forbairt and Irish Institution of Surveyors.

Sack, R. (1980) Conceptions of Space in Social Thought: a geographic perspective. London: Macmillan.

Sack, R. (1986) Human Territoriality: its theory and history. Cambridge: Cambridge University Press.

Sack, R. (1997) Homo Geographicus: a framework for action, awareness, and moral concern. Baltimore, London: Johns Hopkins University Press.

Said, E. (1985) Orientalism. Harmondsworth: Penguin.

Said, E. (1993) Culture and Imperialism. London: Chatto and Windus.

Sandler, N. (1998) "Infrared Smart Cards Replace Passwords". *Techweb News*. <a href="http://www.techweb.com/wire/story/TWB199804285000">http://www.techweb.com/wire/story/TWB199804285000</a>

Schartum, D. (1998) "Access to Government-Held Information: Challenges and Possibilities". 1998 (1) The Journal of Information, Law and Technology (JILT). <a href="http://elj.warwick.ac.uk/jilt/infosoc/981scha/">http://elj.warwick.ac.uk/jilt/infosoc/981scha/</a>

Schiller, H. (1978) New Modes of Cultural Domination. Dublin: Conradh na Gaeilge.

Schiller, H. (1986) Information and the Crisis Economy. New York, Oxford: Oxford University Press.

Schiller, H. (1989) Culture Inc.: the corporate takeover of public expression. New York, Oxford: Oxford University Press.

Schiller, H. (1996a) "Information Deprivation in an information-rich society". Gerbner, G., Mowlana, H. and Schiller, H., eds., *Invisible crises: what conglomerate control of media means for America and the world*. Oxford, Boulder, Colo.: Westview, 15-26.

Schiller, H. (1996b) Information Inequality the deepening social crisis in America. New York, London: Routledge.

Schoeman, F. (1984) Philosophical Dimensions of Privacy. UK: Cambridge University Press.

Schoeman, F. (1984a) "Privacy and Intimate Information". In Schoeman, F., *Philosophical Dimensions of Privacy*. UK: Cambridge University Press, 403-418.

Schoeman, F. (1984b) "Privacy: Philosophical Dimensions of the Literature". In Schoeman, F., *Philosophical Dimensions of Privacy*. UK: Cambridge University Press, 1-33.

Schoeman, F. (1992) Privacy and Social Freedom. Cambridge: Cambridge University Press.

Schofield, H. (1998) "At the Third Stroke, It Will Be 1900 Precisely". *The Guardian Online*, June 4 1998. <a href="http://go2.guardian.co.uk/technology/896878175-compaq.htm">http://go2.guardian.co.uk/technology/896878175-compaq.htm</a>

Schwartz, J. and O'Harrow, R. (1998) "Databases start to Fuel Consumer Ire". *The Washington Post*, March 10 1998. <a href="http://washingtonpost.com/wp-srv/frompost/march98/privacy10.htm">http://washingtonpost.com/wp-srv/frompost/march98/privacy10.htm</a>

Scranton, P. (1994) "Determinism and Indeterminacy in the History of Technology". In Smith, M. and Marx, L., *Does Technology Drive History? The Dilemma of Technological Determinism*. Cambridge, Massachusetts: The MIT Press, 143-168.

Secretary's Advisory Committee on Automated Personal Data Systems. United States Department of Health, Education, and Welfare (1973) *Records, computers, and the rights of citizens: report*. Cambridge, Mass: MIT Press.

Seipel, P. (1996) "Comments on the EC Data Protection Directive: The View from Sweden". 1996 (1) The Journal of Information Law and Technology (JILT). <a href="http://elj.warwick.ac.uk/elj/jilt/dp/1sweden/">http://elj.warwick.ac.uk/elj/jilt/dp/1sweden/</a>

Senker, P. (1995) "Technological Change and the Future of Work". In Heap, N. et al., eds., Information Technology and Society: A Reader. London: Sage Publications, 135-148.

Shakespeare, W. (Bevington, D., ed.) (1997) The Complete Works of William Shakespeare (4th ed.). New York, Harlow: Longman.

Shakespeare, W. (1997) "Richard III". In Shakespeare, W. (Bevington, D., ed.) The Complete Works of William Shakespeare (4th ed.). New York, Harlow: Longman.

Shanley, A. (1998) *Micromarketing and GIS; the Bank of Ireland Experience*. Presented at GIS Ireland 98, Malahide, Dublin.

Shapiro, A. (1998) The Danger of Private Cybercops. < http://www.cybercon98.org/wcm/shapiro.htm>

Shaw, M. (1997) International Law (4th ed.). Cambridge: Cambridge University Press.

Sibley, D. (1992) "Outsiders in society and space". Anderson, K. and Gale, F., eds. *Inventing places: studies in cultural geography*. Melbourne, Australia: Longman Cheshire - New York: Wiley, Halsted Press, 107-122.

Sieghart, P. (1976) Privacy and Computers. London: Latimer New Dimensions.

Siggins, L. (1998a) "Contract awarded to design EU fishing 'sky spy' system". *The Irish Times*, Apr. 17 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0417/hom(19.htm">http://www.irish-times.com/irish-times/paper/1998/0417/hom(19.htm</a>

Siggins, L. (1998b) "Satellite System to Pinpoint Location". *The Irish Times*, June 8 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0608/sci4.htm">http://www.irish-times.com/irish-times/paper/1998/0608/sci4.htm</a>

Silberman, S. (1998) "Is Web-Based Mail Bad for Your Anonymity?" *Wired News*, Apr. 4 1998. <a href="http://www.wired.com/news/news/culture/story/10555.html">http://www.wired.com/news/news/culture/story/10555.html</a>

Simecka, M. (1984) "A world with utopias or without them?". Alexander, P. and Gill R., eds. Utopias. London: Gerald Duckworth & Co. Ltd, 169-177. Source of the backwork in Heavy Mark

Simons, G. (1982) Privacy in the Computer Age. Manchester: NCC.

Singer, P., ed. (1986) Applied ethics. Oxford: Oxford University Press, 1986.

Singer, P., ed. (1994) Ethics. Oxford, New York: Oxford University Press, 1994.

Slowe, P. (1990) Geography and Political Power. London: Routledge. Mod. 14 1994

Smart, P. (1991) Mill and Marx: individual liberty and the roads to freedom. Manchester: Manchester University Press.

Smith, A. (1986) The Ethnic Origins of Nations. Oxford: Basil Blackwell.

Smith, A. (Playfair, W., ed.) (1995) An Inquiry into the Nature and Causes of the Wealth of Nations (11th ed.) (Facsim. of ed. published: London: T. Cadell and W. Davies, 1805). London: W. Pickering.

Smith, M. and Marx, L. (1994) Does Technology Drive History? The Dilemma of Technological Determinism. Cambridge, Massachusetts: The MIT Press.

Smith, R.(1998) "Risk of Miscalculation in Kashmir Raises Fears: India Pakistan Engage in Slow Buildup". *The Washington Post*, June 5 1998. <a href="http://washingtonpost.com/wp-srv/WPcap/1998-06/05/064r-060598-idx.htm">http://washingtonpost.com/wp-srv/WPcap/1998-06/05/064r-060598-idx.htm</a>>

Smith, S. (1997) "A Dimension of Sight and Sound". Mapping Awareness 11 (8), 18-21.

Smyth, P. (1999a) "Hopes of Maximum EU Funding Doomed". *The Irish Times*, Feb. 25 1999. <a href="http://www.irish-times.com/irish-times/paper/1999/0225/region6.htm">http://www.irish-times/paper/1999/0225/region6.htm</a>

Smyth, P. (1999b) "Ireland May Sign EU Policing Agreement". *The Irish Times*, Mar. 13 1999. <a href="http://www.ireland.com/newspaper/ireland/1999/0313/hom7.htm">http://www.ireland.com/newspaper/ireland/1999/0313/hom7.htm</a>

Snoddy, R. (1998) "Murdoch Censors Chris Patten". The *Times*, Mar. 4 1998. <a href="http://www.the-Times.co.uk/news/pages/Times/timnwsnws01032.html">http://www.the-Times.co.uk/news/pages/Times/timnwsnws01032.html</a>

Sobel, D. (1995) Longitude - The True Story of a Lone Genius Who Solved the Greatest Scientific Problem of His Time. London: Fourth Estate.

Soja, E. (1989) Postmodern Geographies: The Reassertion of Space in Critical Social Theory. London: Verso.

Speake J., ed., (1979) A Dictionary of Philosophy. London: Pan Books Ltd..

Spieker, F. (1994) "Data Security Aspects Associated with the Use of Administrative Data for Statistical Purposes". *Proceedings of the International Seminar on Statistical Confidentiality*, November 1994. Luxembourg: Office for Official Publications of the European Communities (1995), 229-233.

Spinello, R. (1997) Case Studies in Information and Computer Ethics. USA: Prentice-Hall.

Star, J., Estes, J. and McGwire, K., eds. (1997) Integration of geographic information systems and remote sensing. Cambridge: Cambridge University Press.

Star Tribune (1997) "Free Data Flow Could Raise the Price of Privacy". *The Star Tribune*. <a href="http://www.startribune.com/digage/free.htm">http://www.startribune.com/digage/free.htm</a>

Stefoff, R. (1995) The British Library Companion to Maps and Mapmaking. London: British Library.

Stephen, Sir J. (White, R., ed.) (1873) Liberty, Equality, Fraternity (2nd ed.). Cambridge: Cambridge U.P..

Sterling, B. (1992) The Hacker Crackdown: law and disorder on the electronic frontier. New York: Bantam Books.

Sterling, B. (1995) "The Hacker Crackdown: Evolution of the US Telephone Network". In Heap, N. et al., eds., *Information Technology and Society: A Reader*. London: Sage Publications, 33-40.

Stoll, C.(1995) Silicon Snake Oil: second thoughts on the information highway. London: Pan.

Stone, A. (1995) The War of Desire and Technology at the Close of the Mechanical Age. Cambridge, Mass., London: The MIT Press.

Strassman, P. (1994) "Ensuring Privacy Protection for All". *Computerworld*, Nov. 14 1994. <a href="http://www.strassman.com/pubs/ensure-privacy.html">http://www.strassman.com/pubs/ensure-privacy.html</a>

Struck, D. (1998) "'Rites of Youth': Hacking in the '90s - Israel Sympathetic to Teen Linked Pentagon Computer Break-Ins". *The Washington Post*, Mar. 21 1998. <a href="http://washingtonpost.com/wp-srv/WPlate/1998-03/21/1041-032198-idx.htm">http://washingtonpost.com/wp-srv/WPlate/1998-03/21/1041-032198-idx.htm</a>

Strum, P., Nash, G. and Etulain, R. (1998) Privacy: the debate in the United States since 1945. London, Fort Worth, TX: Harcourt Brace College Publishers.

Stutz, M. (1998) "Cryptozilla Thwarts Feds Crypto Ban". *Wired News*, Apr. 3 1998. <a href="http://www.wired.com/news/news/technology/story/11465.htm">http://www.wired.com/news/news/technology/story/11465.htm</a>

Suiter, J. (1998) "Banking Secrecy Highly Valued by the Launderers". *The Irish Times*, Mar. 10 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0310/hom52.htm">http://www.irish-times.com/irish-times/paper/1998/0310/hom52.htm</a>

Sun Tzu (1991) The Art of War (translated by T. Cleary). Boston, London: Shambhala.

Tauböck, M. (1992) "Confidentiality of Individual and Household Data from Official Statistics". Proceedings of the International Seminar on Statistical Confidentiality, September 1992, Dublin. Luxembourg: Office des Publications Officielles des Communautés Européennes (1993), 385-390.

Tang, P. (1997) "Multimedia Information Products and Services: A need for 'Cybercops'?" In Loader, B., ed., *The Governance of Cyberspace: Politics, Technology and Global Restructuring*. London: Routledge, 190-208.

Taylor, P. (1985) Political Geography. London: Longman.

Taylor, P. (1998) "Changing World of the IT Director". *The Irish Times*, June 8 1998. < http://www.irish-times.com/irish-times/paper/1998/0608/cmp1.htm>

Tetlow, E. (1974) The Enigma of Hastings. London: Peter Owen.

The Economist (1997) "Privacy on the Internet: Plans to Control Encryption Software are Futile and Misguided". *The Economist*, Mar. 7 1997. <a href="http://www.economist.com/editorial/freeforall/current/index\_ld4935.html">http://www.economist.com/editorial/freeforall/current/index\_ld4935.html</a>

The Guardian (1998) "How the Web Was Won". *Guardian Online*, Mar. 19 1998. <a href="http://go2.guardian.co.uk/pic.html">http://go2.guardian.co.uk/pic.html</a>

The Holy Bible (1984) The Holy Bible, New International Version. UK: Hodder and Stoughton.

The Irish Independent (1998) "Culture of Secrecy' to End with New Law". *The Irish Independent*, Apr. 17 1998. <a href="http://www.independent.ie/1998/106/d04a.shtm">http://www.independent.ie/1998/106/d04a.shtm</a>>

The Irish Times (1996a) "Zimmerman Case Dropped". *The Irish Times*, Jan. 15 1996. <a href="http://www.irish-times.com/irish%2Dtimes/paper/1996/0115/cmp2.htm">http://www.irish-times.com/irish%2Dtimes/paper/1996/0115/cmp2.htm</a>

The Irish Times (1996b) "Why Web Visitors are Economical with Truth". *The Irish Times*, Dec. 16 1996. <a href="http://www.irish-times.com/irish%2Dtimes/paper/1996/1216/cmp3.htm">http://www.irish-times.com/irish%2Dtimes/paper/1996/1216/cmp3.htm</a>

The Irish Times (1998a) "Cabinet to Seek Change in Status". *The Irish Times*, Nov. 18 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/1118/opt5.htm">http://www.irish-times.com/irish-times/paper/1998/1118/opt5.htm</a>

The Irish Times (1998b) "Calls for 'Passport' Books for Travellers". *The Irish Times*, May 13 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0513/hom61.htm">http://www.irish-times.com/irish-times/paper/1998/0513/hom61.htm</a>

The Irish Times (1998c) "Encryption Ban 'No Real Worry' Outside US". *The Irish Times*, Feb. 23 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0223/cmp4.htm">http://www.irish-times.com/irish-times/paper/1998/0223/cmp4.htm</a>

The Irish Times (1998d) "Eritrea calm with no sign of further air attacks". *The Irish Times*, June 8 1998. <a href="http://www.ireland.com/newspaper/world/1998/0608/wor5.htm">http://www.ireland.com/newspaper/world/1998/0608/wor5.htm</a>

The Irish Times (1998e) "Ethiopia, Eritrea step up bombing raids". *The Irish Times*, June 6 1998. <a href="http://www.ireland.com/newspaper/world/1998/0606/worl2.htm">http://www.ireland.com/newspaper/world/1998/0606/worl2.htm</a>

The Irish Times (1998f) "Information is Good For You". (Editorial on FoIA) "*The Irish Times*, Apr. 22 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0422/edi1.html">http://www.irish-times.com/irish-times/paper/1998/0422/edi1.html</a>

The Irish Times (1998g) "Kashmir at Heart of India-Pakistan Conflict". *The Irish Times*, June 8 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0608/wor2.htm">http://www.irish-times.com/irish-times/paper/1998/0608/wor2.htm</a>

The Irish Times (1998h) "Public Bodies Affected by Information Act". *The Irish Times*, Apr. 22 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0422/hom39.html">http://www.irish-times.com/irish-times/paper/1998/0422/hom39.html</a>

The Irish Times (1998i) "Speed is a Major Problem - Survey". *The Irish Times*, Apr. 6 1998. <a href="http://www.irish-times.com/irish-times/paper/1998/0406/cmp3.htm">http://www.irish-times.com/irish-times/paper/1998/0406/cmp3.htm</a>

The Irish Times (1999a) "Conflict becomes full-scale war". *The Irish Times*, Feb. 24 1999. <a href="http://www.ireland.com/newspaper/world/1999/0224/wor4.htm">http://www.ireland.com/newspaper/world/1999/0224/wor4.htm</a>

The Irish Times (1999b) "Eritrea claims attack repulsed"". *The Irish Times*, Feb. 10 1999. <a href="http://www.ireland.com/newspaper/world/1999/0210/wor7.htm">http://www.ireland.com/newspaper/world/1999/0210/wor7.htm</a>

The Irish Times (1999c) "Ethiopia and Eritrea will not suspend border war". *The Irish Times*, Feb. 13 1999. <a href="http://www.ireland.com/newspaper/world/1999/0213/wor4.htm">http://www.ireland.com/newspaper/world/1999/0213/wor4.htm</a>

The Irish Times (1999d) "Minister Defends Social Welfare Checks". *The Irish Times*, Feb. 25 1998. <a href="http://www.irish-times/paper/1999/0225/hom17.htm">http://www.irish-times/paper/1999/0225/hom17.htm</a>

The Irish Times (1999e) " 'More than 21,000' Eritrean casualties and prisoners ". *The Irish Times*, June 17 1999. <a href="http://www.ireland.com/newspaper/breaking/1999/0616/break8.htm">http://www.ireland.com/newspaper/breaking/1999/0616/break8.htm</a>

The Irish Times (1999f) " OAU summit agenda has to tackle 6 wars ". *The Irish Times*, Jul. 12 1999. <a href="http://www.ireland.com/newspaper/world/1999/0712/worl1.htm">http://www.ireland.com/newspaper/world/1999/0712/worl1.htm</a>

The Irish Times (1999g) "Peace Plan for Eritrea after Badme Loss". *The Irish Times*, Mar. 1 1999. <a href="http://www.irish-times.com/irish-times/paper/1999/0301/worl1.htm">http://www.irish-times.com/irish-times/paper/1999/0301/worl1.htm</a>

The Sunday Times (1999h) "The Sunday Times Power List 1999". The Sunday Times, Oct. 2 1999.

Washington Post (1998a) "Microsoft, Feds Are Talking Again". *The Washington Post*, May 14 1998. <a href="http://washingtonpost.com/wp-srv/business/longterm/microsoft/micro.htm">http://washingtonpost.com/wp-srv/business/longterm/microsoft/micro.htm</a>

The Washington Post (1998b) "UNSCOM Tracks Terror Weapons". *The Washington Post*: <a href="http://washingtonpost.com/wp-srv/inatl/longterm/iraq/maps/satindex.htm">http://washingtonpost.com/wp-srv/inatl/longterm/iraq/maps/satindex.htm</a>

The White House - Office of the Press Secretary (1994) Executive Order 12906: Coordinating Geographic Data Acquisition and Access: The National Spatial Data Infrastructure. <a href="http://www.npr.gov/library/direct/orders/20fa.html">http://www.npr.gov/library/direct/orders/20fa.html</a>

Thomas, R. (1995) "Access and Inequality". In Heap, N. et al., eds., *Information Technology and Society: A Reader*. London: Sage Publications, 90-100.

Thomson, J. (1975) "The Right to Privacy". Reprinted in Schoeman, F., *Philosophical Dimensions of Privacy*. UK: Cambridge University Press, 272-289.

Thomson, J. (1990) The realm of rights. Cambridge, Mass., London: Harvard University Press.

Thygesen, L. (1992) "Technological Aspects of Confidentiality: New Technology Threat or Greater Protection?" *Proceedings of the International Seminar on Statistical Confidentiality, September 1992, Dublin.* Luxembourg: Office des Publications Officielles des Communautés Européennes (1993), 299-305.

Thygesen, L. (1994) "The Influence of the Technological Development on Data cCollection Methods in Surveys". How is the Protection of Personal Data Affected. *Proceedings of the International Seminar on Statistical Confidentiality*, November 1994. Luxembourg: Office for Official Publications of the European Communities (1995), 197-199.

Todd, R. (1978) "Electronics and the Invasion of Privacy". Young, J., ed. *Privacy*. Chichester [etc.]: Wiley, 309-318.

Toon, M. (1997) "Making the Web Pay". Mapping Awareness 11 (8), 12.

Tosta, N. (1995) "Data Policies and the National Spatial Data Infrastructure". In Onsrud, H., ed., (1995) *Proceedings of the Conference on Law and Information Policy for Spatial Databases: Tempe, Arizona:* October 29-31 1994. <a href="http://www.spatial.maine.edu/tempe/tempe94.html">http://www.spatial.maine.edu/tempe/tempe94.html</a> Tosta, N. (1997) "National spatial data infrastructures and the roles of national mapping organisations". Rhind, D., ed., *Framework for the world*. Cambridge: GeoInformation International, 173-186.

Towle, H. (1996) *Contracts for Online Services*. Presented at a Conference on "The Internet: Emerging Legal Issues", Dublin, Mar. 6 1996 (unpublished).

Tuan, Y. (1975) Topophilia: a study of environmental perception, attitudes, and values. Englewood Cliffs, London [etc.]: Prentice-Hall.

Tuan Y. (1976) "Geopiety: A Theme in Man's Attachment to Nature and to Place". Lowenthal, D. and Bowden M., eds. *Geographies of the Mind: Essays in Historical Geography*. New York: Oxford University Press, 11-39.

Tuan, Y. (1977) Space and Place: the perspective of experience. London: Edward Arnold.

Tuan, Y. (1979) Landscapes of Fear. Oxford: Blackwell

Turkle, S. (1984) The Second Self: computers and the human spirit. London: Granada.

Turkle, S. (1995) Life on the Screen: identity in the age of the internet. New York: Simon and Schuster.

Turner, B. (1993) Citizenship and Social Theory. London: Sage.

Tyacke, S., ed. (1983) English Map Making 1500-1650: historical essays. London: British Library.

Tynan, M. (1999) "Increased Powers for Revenue Criticised". *The Irish Times*, Feb. 25 1999. <a href="http://www.irish-times/irish-times/paper/1999/0225/hom4.htm">http://www.irish-times/paper/1999/0225/hom4.htm</a>

UK Government (1984) Data Protection Act, 1984. <a href="http://www.legislation.hmso.gov.uk/acts/acts1984/1984035.htm">http://www.legislation.hmso.gov.uk/acts/acts1984/1984035.htm</a>

UK Government (1998) Data Protection Act, 1998. <a href="http://www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm">http://www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm</a>

UK Home Office (1996) Consultation Paper on the EC Data Protection Directive. Journal of Information, Law and Technology (JILT) <a href="http://elj.warwick.ac.uk/jilt/consult/ukdp/dataprot.htm">http://elj.warwick.ac.uk/jilt/consult/ukdp/dataprot.htm</a>

Ustaran, E. (1997)"Data Protection Regulation: The Challenge Ahead", Commentary, 1997 (3) The Journal of Information, Law and Technology (JILT). <a href="http://elj.warwick.ac.uk/jilt/dp/97\_3ust/">http://elj.warwick.ac.uk/jilt/dp/97\_3ust/</a>

United Nations (1948) Universal Declaration of Human Rights. UN High Commissioner for Human Rights <a href="http://www.unhchr.ch/udhr/lang/eng.htm">http://www.unhchr.ch/udhr/lang/eng.htm</a>

United Nations (1952) Convention on the International Right of Correction. United Nations High Commissioner for Human Rights, 1997. <a href="http://www.unhcr.ch/html/menu3/b/i\_ilocor.htm">http://www.unhcr.ch/html/menu3/b/i\_ilocor.htm</a>

United Nations (1966a) International Covenant on Civil and Political Rights (Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966). <a href="http://www.unhchr.ch/html/menu3/b/a\_ccpr.htm">http://www.unhchr.ch/html/menu3/b/a\_ccpr.htm</a>

United Nations (1966b) International Covenant on Economic, Social and Cultural Rights. (Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966). <a href="http://www.unhchr.ch/html/menu3/b/a\_cescr.htm">http://www.unhchr.ch/html/menu3/b/a\_cescr.htm</a>>

University of Texas (1996) Ethical Issues in Electronic Information Systems. <a href="http://www.utexas.edu/depts/grg/gcraft/notes/ethics/">http://www.utexas.edu/depts/grg/gcraft/notes/ethics/</a>

Unwin, P. (1992) The Place of Geography. Harlow, Essex, England: Longman Scientific and Technical -New York: Wiley.

US Congress, Office of Technology Assessment (1994) Information Security and Privacy in Network Environments. USA: US Government Printing Office. Van Der Wusten, H. (1997) "Political Geography of International Relations: The World Stage, Regional Arenas, the Search for a Play". In Dikshit, R., *Developments in Political Geography: A Century of Progress*. New Delhi, London: Sage Publications Ltd., 318-355.

Van Dosselaar, P. (1992) "Between Scylla and Charybdis: Controlling Disclosure Risks Whilst Preserving Information". *Proceedings of the International Seminar on Statistical Confidentiality, September 1992, Dublin.* Luxembourg: Office des Publications Officielles des Communautés Européennes (1993), 445-450.

Van Eechoud, M. (1997) Legal Protection of Geographical Information: Copyright and Related Rights. Presented at The European Research Conference on Socio-Economic Impacts of New Geographic Information Handling Technologies, Castel Vecchio Pastoli, Italy, 17-22 May 1997 (unpublished).

Velecky, L. (1978) "The concept of privacy". Young, J., ed. Privacy. Chichester [etc.]: Wiley, 13-34.

Vowles, R. (1995) *Censorship and Privacy on the New Zealand Internet*. <a href="http://www.interaus.net/1995/8/nz1.html">http://www.interaus.net/1995/8/nz1.html</a>

Wall, R. (1996) "Copyright Forum". Managing Information 3(3), March 1996, 25-32.

Wallich, P. (1997) "Cyber View: Parental Discretion Advised". Scientific American, Aug. 1997. <a href="http://www.sciam.com/0897issue/0897cyber.htm">http://www.sciam.com/0897issue/0897cyber.htm</a>

Walsh, D. (1998) "Breaking Down the Walls of Secrecy". The Sunday Business Post, Nov. 8 1998; 21-22.

Ward, L. (1998) "Computer Bug Time Lag 'Will Risk Lives'". *The Guardian*, June 17 1998. <a href="http://reports.guardian.co.uk/articles/1998/6/17/6666.htm">http://reports.guardian.co.uk/articles/1998/6/17/6666.htm</a>

Ward, M. (1998) "Cyberview: Name Games". *Scientific American*, Mar. 3 1998. <a href="http://www.newscientist.com/ns/980307/nfocus.htm">http://www.newscientist.com/ns/980307/nfocus.htm</a>

Warner, M. and Stone, M. (1970) The data bank society: organizations, computers and social freedom. London: Allen & Unwin.

Warren, S. and Brandeis, L. (1890) "The Right to Privacy [The Implicit made Explicit]". Reprinted in Schoeman, F., *Philosophical Dimensions of Privacy*. UK: Cambridge University Press, 75-103.

Wasserstrom, R. (1978) "Privacy: Some Arguments and Assumptions". Reprinted in Schoeman, F., *Philosophical Dimensions of Privacy*. UK: Cambridge University Press, 317-332.

Waterman, S. and Kliot, N., eds. (1991) The Political Geography of Conflict and Peace. London: Belhaven.

Wayt Gibbs, W. (1997a) "Command and Control: Inside a Hollowed-Out Mountain, Software Fiascoes--and a Signal Success". *Scientific American*, Aug. 1997. <a href="http://www.sciam.com/0897issue/0897techbus1.htm">http://www.sciam.com/0897issue/0897techbus1.htm</a>

Wayt Gibbs, W. (1997b) "Cyber View: World Wide Widgets". Scientific American, May 1997. <a href="http://www.sciam.com/0597issue/0597cyber.htm">http://www.sciam.com/0597issue/0597cyber.htm</a>

Webster, F. (1995) Theories of the Information Society. London, New York: Routledge.

Wegener, M. (1997) *Brave New GIS Worlds Revisited*. Presented at The European Research Conference on Socio-Economic Impacts of New Geographic Information Handling Technologies, Castel Vecchio Pastoli, Italy, 17-22 May 1997 (unpublished).

Wegener, M. and Masser, I. (1996) "Brave New GIS Worlds". In Masser, I, Campbell, H. and Craglia, M., eds., *GIS Diffusion. The Adoption of Geographical Information Systems in Local Government in Europe.* London: Taylor and Francis, 9-21.

Westin, A. (1967) "The Origins of Modern Claims to Privacy". Reprinted in Schoeman, F., *Philosophical Dimensions of Privacy*. UK: Cambridge University Press, 56-74.

Westermeier, J. (1996) "Validation of Electronic Commerce Contracting Practices". GIS Law 3(3), Fall 1996, 4-7.

Whine, M. (1997) "The Far Right on the Internet". In Loader, B., ed., *The Governance of Cyberspace: Politics, Technology and Global Restructuring*. London: Routledge, 209-228.

Whitfield, P. (1994) The Image of the World: 20 centuries of world maps. London: British Library.

Whitfield, P. (1998) New Found Lands: maps in the history of exploration. London: British Library.

Wiebe, A. (1996) "Harmonisation of Data Protection Law in Europe", Conference Report. 1996 (3) The Journal of Information Law and Technology (JILT). <a href="http://elj.warwick.ac.uk/elj/jilt/confs/3dp/">http://elj.warwick.ac.uk/elj/jilt/confs/3dp/</a>

Wieland, U. (1994) "Information Security and Statistical Confidentiality". *Proceedings of the International Seminar on Statistical Confidentiality*, November 1994. Luxembourg: Office for Official Publications of the European Communities (1995), 221-224.

Wilford, J. (1981) The Mapmakers. London: Junction Books.

Wilkin, P. (1997) Noam Chomsky: On Power, Knowledge and Human Nature. London: Macmillan Press Ltd.

Wilkinson, G. and Fisher, P. (1987) "Recent Development and Future Trends in Geo-Information Systems". *The Cartographic Journal* 24, June 1987, 64-69.

Wilkinson R. (1951) Maps and Politics.

Williams, B. (1993) Ethics and the Limits of Philosophy. UK: Fontana Press.

Williams C., (1993) The Political Geography of the New World Order. London: Belhaven Press.

Williams, M. and O'Harrow, R. Jr. (1998) "Online Searches Fill in Many Holes". *The Washington Post*, May 8 1998. <a href="http://washingtonpost.com/wp-srv/frompostmarch98/sidebars/kaplan8.htm">http://washingtonpost.com/wp-srv/frompostmarch98/sidebars/kaplan8.htm</a>

Winett, B. (1998a) "Long Distance Tracking". *Hotwired*, 1998. <a href="http://www.Hotwired.com/webmonkey/98/22/index1a.htm">http://www.Hotwired.com/webmonkey/98/22/index1a.htm</a>

Winett, B. (1998b) "Tracking Your Visitors". *Hotwired*, 1998. <a href="http://www.Hotwired.com/webmonkey/98/16/index2a.html">http://www.Hotwired.com/webmonkey/98/16/index2a.html</a>

Wired News (1998a) "Computers Buoy US Economy". *Wired News*, Apr. 30 1998. <a href="http://www.wired.com/news/news/business/story/12017.htm">http://www.wired.com/news/news/business/story/12017.htm</a>

Wired News (1998b) "Man's Online Murder Confession". *Wired News*, Apr. 10 1998. <a href="http://www.wired.com/news/news/business/story/12014.htm">http://www.wired.com/news/news/business/story/12014.htm</a>

Womack, H. (1997) "No Privacy in the Land of the Huddled Masses". *The Irish Times*, Mar. 4 1997. <a href="http://www.irish-times.com/irish%2Dtimes/paper/1997/0304/for9.htm">http://www.irish-times.com/irish%2Dtimes/paper/1997/0304/for9.htm</a>

Wood, D. (with Fels, J.) (1992) The Power of Maps. London: Routledge.

Wood, D. (1993) "The Fine Line between Mapping and Mapmaking". Cartographica 30(4), 50-60.

Wood, D. and Fels, J. (1986) "Designs on Signs: Myth and Meaning in Maps". Cartographica 23(3), 54-103.

Woods, L. (1996) "The Question of Space". In Aronowitz, et al. *Technoscience and Cyberculture*. New York: Routledge, 279-292.

Worboys, M., ed., (1994) Innovations in GIS 1. London: Taylor and Francis.

Worboys, M. (1995) GIS: a computing perspective. London: Taylor & Francis.

Yeates, P. (1999) "Dubliners 'Worse Off by £44 a Week'". The Irish Times, Feb. 20 1999. < http://www.irish-times.com/irish-times/paper/1999/0220/news2.htm>

Yeo, G., Cresson, E., Rushkoff, D., Kelly, K. and Negroponte, N. (1995) "The Soul of Cyberspace". New Perspectives Quarterly, Fall 1995, 18-25.

Young, E. (1992) "Hunter-gatherer concepts of land and its ownership in remote Australia and North America". Anderson, K. and Gale, F., eds. *Inventing places: studies in cultural geography*. Melbourne, Australia: Longman Cheshire - New York: Wiley, Halsted Press, 255-272.

Young, J., ed. (1978) Privacy. Chichester [etc.]: Wiley.

Ziauddin, S. (1988) Information and the Muslim World: a strategy for the twenty-first century. London: Mansell.

Zorpette, G. (1997) "Spying Saucer". *Scientific American*, June 1997. <a href="http://www.sciam.com/0697issue/0697techbus4.htm">http://www.sciam.com/0697issue/0697techbus4.htm</a>

Zuboff, S. (1988) In the Age of the Smart Machine: The Future of Work and Power. Oxford: Heineman Professional Publishing.

253

Internet Departments and Offices Idmininistration (other than health a education public bodies Ice/assurance/pensions Unions

Mierence(incl. of Debt Coll nest togon

(00)

narketing/ mailing

commercial organisations

us (general)

eann e caffai nedaraith. Anns e caffai nedaraith

5

ion

l parties

45

onirellar

ocessor

# **Appendix One**

# **Data Protection Registration**

254

Year	1989		
Government Departments and Offices	79		
Local administration (other than health a education)	74		
Other public bodies	130		
Insurance/assurance/pensions	104		
Credit Unions	186		
Other Financial Institutions	81		
Credit reference(incl. of Debt Coll. post 1989)	11		
(just debt)	8		
Direct marketing/ mailing	22		
Other commercial organisations	101		
Hospitals (general)	29		
Other health organisations	69		
Pharmacists	179	1d	
Doctors	41		
Dentists	4		
Education	69		
Political parties	4		
Religious	3		
Data Castrollar	1106		
Data Controller	88		
Data Processor	00		
TOTAL	1194		
Lionale distribution scholassic stall			
Data Processors			
Other health organisations			
Colleges of Education			

Year on the second secon	1990	1993	1991	1992	1993	1994
Government Departments and Offices	86		84	38.86	87	00 05
Civil Service Departments	60		56	55	55	50
Civil Service Offices	10		10	13	15	15
Attachments to Departments or Offices	16		18	18	17	21
Local admininistration (other than health & education)	81		80	81	83	83
County Councils	27		27	27	20	20
Corporations	12		12	12	12	12
Urban District Councils	36		36	37	37	37
Others	6		5	5	5	5
State-sponsored bodies (not financial, health & educ.)	113		112	110	112	112
Commercial	79		79	78	80	80
Developmental/ research	18		18	17	17	17
Cultural Concerned Debuggies	6		6	6	6	6
Regulatory	10		q	q	a	q
Financial	376		386	421	438	474
State-sponsored	5		5	6	5	6
Associated Banks	15		16	17	18	18
Non-associated Banks	37		35	41	39	42
Building Societies	11		10	10	8	8
Credit Card Company	1		1	1	1	1
Insurance/assurance/pensions	110		109	115	117	123
Credit Unions	197		210	231	250	276
Commercial	151		60	60	75	79
Manufacturing distribution wholesale retail	3		3	3	3	4
Credit reference (incl. of Debt Coll. post 1989)	22		20	22	25	26
Direct marketing/ mailing	29		32	30	36	39
Data Processors	94					
Accountants			2	2	1	1
Computer Bureau			_	_		1
Miscellaneous	3		3	3	10	8
Health	532		540	559	587	635
Health Boards	33		12	12	12	12
Public hospitals & clinics	27		19	25	26	27
Private hospitals & clinics	15		16	16	16	18
Other health organisations	48		47	50	55	56
Pharmacists	316		332	339	342	359
Doctors Dentists & Other health practitioners	93		108	117	136	163
Education	62		62	65	74	78
Vocational Education Committees	35		35	37	38	38
Other regulatory bodies	2		2	3	4	4
University Colleges	11		11	11	11	11
Regional Technical College	1		1	1	7	9
Colleges of Education	6		5	4	5	6
Other third level	1		1	2	3	3
Second level schools	6		7	7	6	7
Political parties and Public Representatives	10		19	32	29	30
Voluntary charitable benevolent	3		4	5	5	5
Religious	15		18	18	19	19
Media	3		3	3	3	3
INGMIA						
Data Controller			1.368	1440	1512	1613
Data Processor			92	96	309	331
TOTAL	1432		1460	1536	1821	1944

Category	1993	1994	1995	1996
Civil Service Departments/Offices	87	95	98	99
Local authorities and Vocational Education Committees	121	121	121	118
Health Boards and public hospitals/clinics	38	39	39	41
Third-level education	26	29	33	31
Primary and secondary schools	6	7	9	14
Commercial state-sponsored bodies	85	86	81	75
Non-commercial and regulatory public bodies	36	36	45	93
Associated banks	18	18	19	22
Non-associated banks	39	42	44	47
Building societies	8	8	8	8
Insurance and related services	117	123	115	120
Credit Unions and Friendly Societies	250	276	431	439
Credit reference/Debt collection	25	26	24	19
Direct marketing	36	39	42	42
Miscellaneous commercial	15	15	17	12
Private hospitals & clinics/other health	71	74	77	81
Doctors, dentists & other health professionals	136	163	180	242
Pharmacists	342	359	349	495
Political parties & public representatives	29	30	28	31
Religious, voluntary & cultural organisations	27	27	29	31
Sub-Total (Data Controllers)	1512	1613	1789	2060
Data Processors	309	331	293	293
Total	1821	1944	2082	2353

A Study of the Privacy Implications of Digitally-Held Geographically-Referenced Information in Ireland

Appendix Two

### Questionnaire

All Results of this Study will be treated confidentially. Answered questionnaires will not be seen by any other person. No individuals or organisations will be individually identified in relation to the results of the survey; all data arising from the survey will be presented in aggregate form. Section 1: Data & its Collection.

[1], (a)What categories of data are collected (i.e. what is the nature of personal data)

(Examples: name, address, RSI No., other Reference Number, some other major anributes or which information is being collected.)

## A Study of the Privacy Implications of Digitally-Held Geographically-Referenced Information in Ireland

## Questionnaire

If no, can you give me some examples

1.2 Is there any method used to refer the data to space

All Results of this Study will be treated confidentially. Answered questionnaires will not be seen by any other person. No individuals or organisations will be individually identified in relation to the results of the survey; all data arising from the survey will be presented in aggregate form.

Aodán Edmonds

1998

259

# Section 1: Data & its Collection.

1.1. (a)What categories of data are collected (i.e. what is the nature of personal data)

(Examples: name, address, RSI No., other Reference Number, some other major attributes on which information is being collected.)

(b) Are they stored under these headings (or are they turned into other indicators)?

If no, can you give me some examples

1.2 Is there any method used to refer the data to space.

Examples: an address, co-ordinate reference (national grid), a spatial aggregation (census area).

Y

Y

Y

N

N

N

N

1.3 Do you have a sensitivity ranking for the data you hold. ("Sensitivity" here refers to personal privacy concerns - highly sensitive data being that which would cause serious problems for individual privacy)

If yes can you describe it.

If no, could you rank the categories you mentioned in Question 1.1 according to their sensitivity (high to low).

1.4. Do different individuals records ever get linked together (e.g. on basis of family relationship, other association) Y

Please give some examples.

1.5. For the 5 most important operations ("operation" refers to analysis of data) performed on the data, please give a % value to the relevance of each of the fields of data mentioned in question 1 (for example "address 85% relevant").

1.6. Briefly describe the process by which the initial data are collected (for example individual in person, survey, use of magnetic cards, other institutions, etc.). Is there a form? (*How collected, By whom, Methodology*).

1.7 Could you give an example of the types of procedure used to check data quality and consistency (if for example data come from more than one source).

1.8. What information audit trails are there (for example maintaining paper archives, tape/disk backups of the original data).

1.9 If there are such materials kept, At which stages of the process of data input, update, manipulation does this occur.

-for how long are they kept,

-and how are they disposed of?

# Section 2: Data Input and Update.

2.1. What is the organisational structure in terms of data collection, input and update. i.e. it is unlikely that the same group does everything.

Which of the following might apply:

Same person

Same unit/room- is there a data collection unit?

Same department, different unit

Different departments, same organisation

Any employee

2.6. And there Outside agency provides the data, update happens in organisation.

#### 2.2. What training relevant personnel have.

a) What is the skill level when they start.

For a) choose from:

No Necessary Skills

Keyboard skills

Informal low-level computer experience (word-processing etc.)

EU Computer Driver's Licence

Software specific training course

Informal computer programming experience (if so what level)

Formal 3<sup>rd</sup> level computer qualification (diploma, certificate, degree, higher degree)

Private sector qualification of a similar level Other (specify).

b) What if any training on the job do they receive.

For b) choose from:

None

Software specific training course Data handling training Informal training from predecessor/ colleague Other formal training (specify) Other (specify).

2.3. Is data input and updated manually, automatically or both (describe).

2.4. Is there a documented procedure for data input and update.

Y

N

2.5. If not is there a standard working procedure (for input & update) in which employees are trained.

Y

Y

Y

Y

N

N

N

N

If yes, Outline its chief steps.

2.6. Are there any other safeguards to ensure accuracy at the input stage; at the update stage (e.g. double checked by themselves/another).

2.7. What is the policy regarding update. Choose from:

Informal, Incomplete.

Regular Optional Update (Complete/ Incomplete).

Regular Obligatory Update(Complete/ Incomplete).

Other (describe)

Is input entirely comprehensive (must all fields mentioned in Question 1 be filled).

Section 3: The Information System / Database.

3.1 Is the system (a) an "off the shelf" one. (name of system?)

(b) was it designed specifically to meet the organisation's needs

strally located with remote access via terminal o

## 3.2. Nature of data storage.

#### Database

RDBMS Object orientated Object Relational other

#### Spreadsheet Other (specify)

3.3. Does the system make use of a unique identifier.

If yes, What is the general nature of the identifier assigned number, or another database category such as the address, or a combination of more than one

Y

Y

N

N

#### If the system is a GIS ignore the next question:

3.4. Is there a GIS package linked to the system or are the data ever exported into a GIS for analysis. If yes which package.

3.5. If no; Does the database itself include some GIS functionality (e.g. for map production, geographical proximity analysis, etc.). What form do these take

programmed for the organisation, a GIS extension for databases (Oracle's SD Cartridge / IBM's SD Extender)

3.6. What is precise nature of database.

Centrally located, central access only Central location, central access (with remote access for programmers) Centrally located with remote access via terminal or PC Centrally located with changes being communicated via mail, email, phone Diffusely located (different sections in different departments) Other (specify).

# Section 4: Access.

#### General

4.1. What technical security procedures (if any) are in operation. Choose from:

passwords encryption Firewall (describe) other multiple security systems (e.g. password + coded scrambler) other (specify).

If passwords: Policy on changing passwords?

4.2. What other non-technical or organisational procedures are there. Choose from:

staff checks monitoring of unusual access patterns other (specify).

4.3. Who can access the information on the system.

Choose from:

Access for individual who entered information Access for all in same unit Intradepartmental Access Cross departmental Access Access for anybody in organisation Outside Access (specify).

Are there any restrictions placed on access to any categories of information within this framework. (e.g. Sensitive Information limited; Access based on seniority; Based on Job profile).

Y N

If yes, which data items/categories are most commonly limited.

4.4 Are there different levels of access in terms of changing data. (certain grades of employee / management allowed to do certain things).

Y

Y

N

N

4.5. What protections are there against deliberate falsification of information

by an employee,

by an outsider (e.g. hacker),

by the individual data subject

Are there checks of informational consistency?

Do changes of information outside of standard updates need outside verification (can employees of a certain rank make alterations).

#### b) Internal.

4.6. Is there a record of who accesses the data and the purpose for which it is accessed.

If yes, How long is this record kept for.

4.7. What would be defined as unusual accessing of database. Are there procedures to check for this?

4.8. Can data be downloaded to paper, disk, other systems (e.g. personal PC), or other media.

If yes, In what circumstances is this allowed.

Is it permitted to remove such material from the premises.

If yes, In what circumstances is this allowed.

In either case, What safeguards against the unauthorised removal of such material by employees.

#### c) External.

4.9. Are data services offered via the world wide web.

If yes, At what Internet address.

4.10. If yes, What information do those services access and obtain.

4.11. What security procedures are in place for such services

Y N

N

Investigative Y

N

## 4.12 Is data ever shared with outside organisations

If yes With what other organisations is information exchanged as a matter of course:

<u>Private Sector</u> Other similar institutions Financial Institutions Government Other (specify)

 Public Sector

 Other Public sector Bodies

 -Departments

 -Semi-State

 -Police, Other

 Investigative

 Private Sector

 Other (specify)

4.13. In what ways are such data exchanges carried out?

(Examples: direct access to your system/database itself via a network, direct transfer via network, on disk/tape through mail, courier?, telephone, other).

If yes, please outline them

4.14. If there is networking to other institutions (banks for example), what measures are in place to secure this.

Choices: Password, encryption (what type), etc.

4.15 Does the person accessing the system remotely have:

-Full access/Access for specific cases, etc

-Ability to download the data from parent database without necessarily receiving updates which may subsequently be made

-Ability to change parent database

-Full metadata regarding the information they access

-Other (specify)

N

Y

4.16. Do staff have email accounts.

		Y .	N
If man the set of the			
If yes, Are these purely internal, or	external. What protection of them is there (pa	sswords, etc	<b>:.)</b> .
4.17. If yes (to 4.16), To what exter company policy on this?	nt are email accounts policed or monitored. Is	there a	
		Y	N
If yes, outline it please?			
4.18. If yes (to 4.17), Are email ac	counts transferable between employees.		
		Y	Ν
4.10 Are there energifie requirement		1	
telephone in response to requests.	its to be met before information can be given o	ut over the	
		Y	N
If yes, please outline them.			

Banks/Financial institutions: 4.20. What security procedures for automated telephone banking are in place.

Government:

4.21 With which other Government Departments / Semi-State bodies do you share information most commonly. Rank the top five.

## Section 5: Data Protection & Codes of Practise.

5.1 Is your organisation required to register under the terms of the Data Protection Act. Y N **Government Bodies** Financial / Insurance / Direct Marketing / Credit-referencing / Debt collecting Sensitive Information Physical/Mental Health **Racial Origin Political Opinions** Religious/Other beliefs Sexual Life Criminal Convictions Data Processor (but not data controller) 5.2. If yes, Have you registered. Y N 5.3. Are there specific procedures in place to ensure compliance with DPA.

Y

Y

N

N

Please outline them.

5.4. How would you rate the impact of the Act on your organisation within the Irish context. Choose from the following:

Easy to comply with Awkward to comply with in terms of the extra work it necessitates Curtails activities somewhat Curtails activities seriously.

5.5. How would you rate the impact of the Act on your international activities (if relevant).

Easy to comply with Awkward to comply with in terms of the extra work it necessitates Curtails activities somewhat Curtails activities seriously.

5.6. Does the organisation belong to a professional or other representative body.

If yes, please specify.

# Appendix Three **Initial List of Potential Interviewees**

AIB Bank Bank of Ireland Ulster Bank ACC Bank National Irish Bank EBS (Building Society) Irish Permanent (Building Society) Irish Nationwide (Building Society) First National (Building Society) League of Credit Unions **Revenue Comissioners** Social Welfare Gardai Siochana An Post Ordnance Survey of Ireland Central Statistics Office Land Registry & Registry of Deeds Dept. of Education Dept. of Health Dept. of Justice Valuation Office Data Protection Commissioner's Office **Dublin Corporation Fingal County Council** DunLaoighre County Council South Dublin County Council Irish Direct Marketing Association VHI **BUPA** Irish Life Eastern Health Board IRIS IRLOGI Agripost **Bill Moss & Associates** Telecom Eireann

Mater Hospital St. James' Hospital **Dunnes** Stores Tesco/Quinnsworth Superquinn Statoil Data Entry Bureau Dun & Bradstreet Family Album Gemini Direct Mail Precision Marketing Information Ltd Irish Data services Kompass Ireland Ltd Ouatro Direct Ltd A1 Credit reference Bureau Dun & Bradstreet International Fletcher & Collins Ireland Ltd. Irish Credit Bureau Interface Business Information Ltd **ITPA** Ltd Marex Ltd Transax Ltd Transnational Corporation Ltd, ESB Texaco Shell Esso Eircell Esat Digifone **Trinity College** University College Dublin Dublin City University Maynooth University University College Cork University College Galway University of Limerick

OIS Laboratory, Dept. of Geography Tunity College, Dublin 2

Appendix Four Template of Letter to Interviewees

in carrying dut has study I will be conducting a series of structured interviews with information system managers or data protection personnel from a wide variety of organizations in the public and povate sector in Ireland. These interviews will last approximately twenty five minutes. All information follocted will be treated confidentially, and results will only be used in approach form.

The sum of the project is to build up a picture of which type of information is involved, how it is callocted and stored, and how it is projected

If is intended that the survey be completed by the ord of the first week in June. I would be grateful of I could organize a meeting with you, or another appropriate person, as the carbost domain conventence, and will be obitacting you by telephone in a few days time.

If you have any queries regarding the project plants life the to contact Dr. Rybacruk, or neveral (Dr. Rybacruk, or neveral (Dr.

Yours sincerely,

Aodán Edmonds

GIS Laboratory, Dept. of Geography, Trinity College, Dublin 2.

2<sup>nd</sup> May 1998.

Dear \_\_\_\_\_,

My name is Aodán Edmonds. I am involved in a doctoral project to assess the implications of digitally stored geographically-referenced personal information for privacy in this country. The project is being undertaken in the Department of Geography in Trinity College, under the supervision of Dr. Krysia Rybaczuk. The information referred to includes all types of spatially-referenced information.

In carrying out this study I will be conducting a series of structured interviews with information system managers or data protection personnel from a wide variety of organisations in the public and private sector in Ireland. These interviews will last approximately twenty five minutes. All information collected will be treated confidentially, and results will only be used in aggregate form.

The aim of the project is to build up a picture of what type of information is involved, how it is collected and stored, and how it is protected.

It is intended that the survey be completed by the end of the first week in June. I would be grateful if I could organise a meeting with you, or another appropriate person, at the earliest possible convenience, and will be contacting you by telephone in a few days time.

If you have any queries regarding the project please feel free to contact Dr. Rybaczuk, or myself (Dr. Rybaczuk's contact details are given below).

Yours sincerely,

Aodán Edmonds