Regulating the Internet: policy and practice with reference to the control of Internet access and content

Regulating the Internet: policy and practice with reference to the control of Internet access and content

by

Louise Cooke

Submitted in partial fulfilment of the requirements for the award of
Doctor of Philosophy of Loughborough University

2004

ACKNOWLEDGEMENTS

I would like to express sincere thanks and appreciation to Professor Paul Sturges of the Department of Information Science, Loughborough University, for his advice, support and guidance in the supervision of this research project. I would also like to thank Professor Charles Oppenheim for his additional advice and helpful suggestions as Director of Research for the project.

In addition, I would like to acknowledge the joint financial assistance of my employers, Buckinghamshire Chilterns University College, and the Department of Information Science at Loughborough University, without which assistance the research would not have been possible.

The research would also not have been possible without the co-operation of members of the New Information Technology project team at the Council of Europe, who facilitated the participation of the researcher in the formulation of Guidelines for Public Internet Access. Likewise, it would not have been possible without the co-operation of those who provided access at the three case study sites and of those at the sites who willingly contributed their time, ideas, experience and insights when being interviewed. The students at the three institutions who responded so openly and frankly when asked to co-operate in the questionnaire study are particularly deserving of my thanks and appreciation. I am very grateful for all of these contributions.

Last but not least, I would like to thank all those whose tolerance and forbearance have made completion of this project possible, including my colleagues at the University College, and all friends and family. I hope that they will, one day, come to forgive me for the neglect that I have shown them during the time that I have been so engrossed with this project. In particular, I would like to thank Richard, Maurice and Sara for their enduring friendship, humour, support, ideas and encouragement. And, of course, Simon and Zoë, who have had much to contend with during the writing up of this thesis.

TABLE OF CONTENTS

Page

APPENDICES

LIST OF TABLES, GRAPHS AND DIAGRAMS

List of Tables

List of graphs

List of Diagrams

GLOSSARY OF ABBREVIATIONS AND ACRONYMS

ACLU American Civil Liberties Union, founded to protect American constitutional rights and civil liberties, including that of free expression. Of recent years it has been actively involved in fighting threats to unfiltered Internet access in public libraries.

ACPO Association of Chief Police Officers, established to co-ordinate policy-making between the 44 different UK police forces.

ALA American Library Association, the professional body for library and information professionals in the USA.

ARPA Advanced Research Projects Agency, a US Agency established within the US Department of Defence in the 1950s to 'establish and maintain a worldwide lead in science and technology' (Slevin, 2000, p.28). ARPA was responsible for developing a communications network, ARPANET, in 1969 to facilitate the exchange of information between researchers. This network is generally held to be the origin of the Internet.

AUP Acceptable Use Policy, a statement outlining the purposes for which Internet access is provided and the limitations of use for which that access is provided. The terminology 'Internet Use Policy' has been suggested as preferable (see, for example, Sturges, 2002, p.120) as it avoids the subjectivity of the term 'acceptable', but nevertheless AUP remains the terminology in most frequent and commonly understood usage, and therefore is that adopted in this text.

AUT The Association of University Teachers, a trade union and professional association representing UK higher education professionals.

BITNET BITNET was started in 1981 with a link between Yale University and City University of New York CUNY) to facilitate non-commercial exchange

of information between academic institutions and some not-for-profit organizations.

BPI The British Phonographic Industry Ltd, the trade association for UK record companies. Its priority activities include the promotion of the music industry; the provision of legal support to member companies; combating music piracy; and the production of key industry statistics for the UK record business.

CCSR Centre for Computing and Social Responsibility at De Montfort University, UK. The CCSR is an academic centre whose mission is 'To undertake research and provide teaching, consultancy and advice to individuals, communities, organisations and governments at local, national and international levels on the actual and potential impacts of computing and related technologies on society and its citizens' (*ex* <www.ccsr.cms.dmu.ac.uk>).

CCTV Closed Circuit Television, the use of cameras to conduct covert and overt surveillance of public spaces, and increasingly of the workplace.

CERN The European Laboratory for Particle Physics in Switzerland, where the development work on the graphical interface and hypertext linking that resulted in the World Wide Web took place.

CHEST Combined Higher Education Software Team. CHEST is a not-for-profit organisation that negotiates agreements for the provision of software and datasets for the UK higher education community.

CIEC Citizens Internet Empowerment Coalition, a coalition of library and civil liberties groups, ISPs, publishers, recording industry associations and individual Internet users set up in the US in 1996.

CILIP Chartered Institute of Library and Information Professionals, the UK professional body formed through the unification in 2002 of the Institute of Information Scientists and the Library Association.

CVCP Committee of Vice-Chancellors and Principals, a consultative body linking the Heads of universities in the UK. In 2000, CVCP changed its name to Universities UK.

DfES Department for Education and Skills, the UK government department responsible for education, training, skills development and lifelong learning.

DTI Department for Trade and Industry, the UK government department responsible for the promotion of the business sector, the support and development of science and innovation, and regulation of market conditions in the UK.

EESC The European Economic and Social Committee is a consultative forum where the various socio-economic organisations in the Member States of the European Union are represented. The EESC is part of the European Union's institutional system and is intended to provide a link between the official bodies of the Union and civil society.

EFF The Electronic Frontier Foundation, founded in 1990 to 'protect privacy, free expression, and access to public resources and information on-line, as well as to promote responsibility in new media' (Electronic Frontier Foundation, 1996).

EPIC Electronic Privacy Information Centre, a US public interest research centre based in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values.

FAIFE IFLA (see below) Committee on Free Access to Information and Freedom of Expression. FAIFE aims to extend free access to information and freedom of expression in all aspects related to libraries and librarianship; to monitor the state of intellectual freedom within the library community world-wide;

to support IFLA policy development and co-operation with other international human rights organisations; and to respond to violations of free access to information and freedom of expression.

FAST Federation Against Software Theft. FAST was established by the British Computer Society's Copyright Committee to raise awareness of software piracy and to lobby for legislation protecting the rights of software publishers.

G8 An informal group of eight countries: Canada, France, Germany, Italy, Japan, Russia, the UK and the USA. The European Union also participates and is represented by the President of the European Commission and by the leader of the country that holds the presidency of the European Council at the time of the G8 summit. The group has developed from a forum dealing principally with macroeconomic issues to a coalition that holds an annual summit with a broad agenda addressing a wide range of international economic, political and social issues.

GILC Global Internet Liberties Campaign, an international coalition of organisations campaigning for human rights and no prior censorship on the Internet.

HEI Higher Education Institution: the term is used to cover a range of institutions from universities, university colleges, specialist colleges and colleges of higher education, all of whose primary function is the delivery of higher education (i.e. post-18 education at undergraduate and postgraduate levels) and the carrying out of academic research.

ICRA Internet Content Rating Association, an international, independent, non-profit-making organization that aims to provide a means for the objective labelling of content of electronic media.

ICT Information and Communications Technologies, generally used to refer to networked computer technologies.

IFLA International Federation of Library Associations, an umbrella organisation representing national library associations worldwide.

IFPI The International Federation of the Phonographic Industry, the international organisation representing the international recording industry. With similar aims to the BPI, IFPI's priorities are to fight music piracy; to promote fair market access and adequate copyright laws; to help develop the legal conditions and technologies that will enable the recording industry to prosper; and to 'promote the value of music in the development of economies, as well as in social and cultural life' (*ex* <www.ifpi.org>).

IWGCR International Working Group on Content Rating, a coalition of national and international watchdog organisations set up to establish an international rating system for internet content. The group subsequently led to the formation of ICRA, the Internet Content Rating Association.

ISP Internet Service Provider, a company that sells access to the Internet.

ISPA Internet Service Providers Association, the trade association for UK providers of Internet services. ISPA was established in 1995 and has over 100 members. Its aim is to promote competition, self-regulation and the development of the Internet industry.

IWF Internet Watch Foundation – a private quasi-regulatory company established in the UK in September 1996, with the backing of the government, to operate a hotline for reporting complaints about potentially illegal Internet content.

JANET Joint Academic Network, the computer communications network established in 1984 linking UK academic institutions. JANET is managed and developed by UKERNA (see below) under a Service Level Agreement from the Joint Information Systems committee (JISC – see below).

JISC Joint Information Systems Committee. JISC works with further and higher education institutions by providing strategic guidance and advice in the use of Information and Communication Technologies to support teaching, learning, research and administration.

MEP Member of the European Parliament. Members are directly elected in national elections on a five-yearly basis.

MIT Massachusetts Institute of Technology, a Higher Education Institution located in Boston, USA.

NATFHE National Association of Teachers in Further and Higher Education, a Trade Union and Professional Association representing lecturers in UK Colleges and Universities.

NCIS National Criminal Intelligence Service – a UK organisation that provides strategic and tactical intelligence on serious and organised crime, nationally and internationally. NCIS also co-ordinates action between UK police forces and the UK Security Service.

NOF New Opportunities Fund, established in the UK to fund the costs of connecting of all UK public libraries to the Internet.

NSFNET US National Science Foundation network, established in 1986 by linking five university supercomputers with a backbone speed of 56 Kbps, thus opening up the possibility for external universities to access superior processing power and share resources. When ARPANET was disbanded in 1990, NSFnet took over administration of the Internet.

OECD The Organisation for Economic Co-operation and Development: a group of 30 nation states that 'share a commitment to democratic government and the market economy' (*ex* <www.oecd.org>). The work of OECD covers research,

monitoring and the production of statistics to aid policy makers in areas such as trade, macroeconomics, education, development, science and innovation.

PICS Platform for Internet Content Selection, a rating system for Internet content. PICS is widely supported by various governments and industry-based organisations. It works by embedding electronic labels in text or image documents to vet their content before the computer displays them or passes them on to another computer.

QAA Quality Assurance Agency, the body responsible for the monitoring of the quality of higher education provision in the UK.

RIPA Regulation of Investigatory Powers Act 2000, a UK legislative Act controlling the use of surveillance, interception, data mining and data retention.

RSAC Recreational Software Advisory Council. Disbanded in 1999, RSAC was "folded into" a new organization, the Internet Content Rating Association (ICRA). The original aims of RSAC, to protect children from potentially harmful content while preserving free speech on the Internet by providing a mechanism for the objective labelling of electronic media content, continue to form the basis of ICRA's work.

UKERNA The United Kingdom Education Research Networking Association was formed as a not-for-profit organisation by the Higher Education Funding Councils for England, Scotland and Wales and the Office of Science and Technology in 1993. It is responsible for managing the network programme of the UK's higher and further education and research communities.

UNESCO United Nations Educational, Scientific and Cultural Organisation. With 189 member states, the main objective of UNESCO is 'to contribute to peace and security in the world by promoting collaboration among nations through education, science, culture and communication in order to further universal respect for justice, for the rule of law and for the human rights and fundamental freedoms

which are affirmed for the peoples of the world, without distinction of race, sex, language or religion, by the Charter of the UN' (*ex* <http://www.unesco.org/general/eng/about/what.shtml>).

URL Uniform Resource Locator: a standard format for describing the type and location of an information resource accessed over the World Wide Web.

USENET A system of public discussion newsgroups which are organised hierarchically into different forums for the debate of particular topics. Users participate in these public discussions by posting messages to the group and reading the reactions posted to their comments by others.

WIPO World Intellectual Property Organisation – one of the 16 specialised sections of the United Nations, WIPO has 179 member states and is dedicated to the promotion and protection of intellectual property. It currently administers 23 international treaties dealing with different aspects of intellectual property protection.

WWW World Wide Web (also referred to as W3), a hypertext interface to the Internet invented at CERN (see above), initially in order to enable nuclear physicists to exchange working papers over computer networks.

W3C The World Wide Web Consortium, created in October 1994 to 'lead the World Wide Web to its full potential by developing common protocols that promote its evolution and ensure its interoperability' (*ex* <http://www.w3.org/Consortium/>). The W3C is an international non-governmental organisation with around 450 member organisations, including Internet industry leaders, trade associations and public interest groups.

ABSTRACT

Organisations, national governments and supranational bodies have all been active in formulating policy measures to regulate access to, and use of, Internet content. The research investigated policy responses formulated and implemented within the European Union, the Council of Europe, the UK government and three UK academic institutions during a five-year period from 1998 to 2003. This investigation took place from a perspective of concern for the potential impact on freedom of expression and freedom of enquiry of such policy initiatives. On a theoretical level, the study aimed to illuminate the *process* of information policy formulation in this area.

Habermas' ideas about the erosion of the public sphere, and the promotion of conditions favourable to an 'ideal speech' situation, were used as an analogy to the issues posed by the regulation of speech on the Internet. The growth in use of the Internet worldwide as an informational, recreational and communications tool has been accompanied by a moral panic about 'unacceptable' Internet content. The effectiveness of a range of responses that have been made to control this 'problematic' medium, including the use of technical, ethical and legal constraints, were examined. Freedom of expression and freedom of access to information were considered, both as a fundamental human right and in the context of a professional ethic for information professionals and academic staff and students.

Policy-making by the European Union and the UK government was explored via longitudinal analysis of primary and secondary documentary sources; by the Council of Europe via a combination of documentary analysis of primary and secondary sources and participant observation at a policy-making forum; and at the organisational level via case study research at three UK Higher Education Institutions. This case study research used a combination of documentary analysis and semi-structured interviews with relevant personnel. Findings from the three case studies were triangulated via a questionnaire study carried out with student respondents at each of the Institutions, to explore students' actual use, and misuse, of University computer networks and their attitudes towards attempts to regulate

this use. The SPSS computer software package was used to analyse the data collected via the questionnaire study.

The re-interpreted policy process model proposed by Rowlands and Turner (1997) and the models of direct and indirect regulation proposed by Lessig (1999) were used as heuristic tools with which to compare the findings of the research. A new model, the reflexive spiral, was designed to illustrate the dynamic, evolving and bi-directional character of the policy formulation processes that were identified. The enquiry was exploratory in nature, allowing theories and explanations to emerge from the data rather than testing a pre-determined set of conclusions.

The conclusion is that the democratising potential of the Internet has indeed been constrained by policy measures imposed at a range of levels in an attempt to control the perceived dangers posed by the medium. Regulation of the Internet was found to be a problematic area for organisations, national governments, and international organisations due to its inherently 'resistant' architectural structure and its transborder reach. Despite this, it was found that, at all levels, the Internet is subject to a multi-tiered governance structure that imposes an increasingly wide range of regulatory measures upon it.

The research revealed that of the three re-interpreted policy process models, those of the Garbage Can and the Bureaucratic Imperative were found to be particularly illustrative of the policy formulation process at all levels. The use of Lessig's models of regulation (Ibid) was also found to be applicable to this area, and to be capable of illuminating the many forces impacting on information flow on the Internet. Overall, the measures taken to control and regulate Internet content and access were found to have exerted a negative impact on freedom of expression and freedom of access to information.

"Give me the liberty to know, to utter and to argue freely according to conscience, above all liberties".

Areopagitica: For the Liberty of Unlicensed Printing
John Milton, 1644.

CHAPTER ONE: INTRODUCTION

> *Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer…The content on the Internet is as diverse as human thought.*
>
> Reno v. ACLU 521 US 844, 870 (1997)[1]

1.1 Aims and objectives

What are governments, international organisations, institutions and society in general 'doing' about the Internet, in response to the many calls for regulation and control of 'dubious' content to be found on it, and its potential for misuse? This question leads into consideration of the potential impact of such measures on freedom of expression, which forms the central research question of this thesis. The aims of the study were:

1. To investigate policy measures intended to control and regulate access to illegal, 'harmful', 'undesirable' or 'inappropriate' content on the Internet. The investigation included measures formulated and implemented during a five-year period from 1998 until 2003 at national, supranational and organisational level.
2. To determine what effects, if any, such measures were having on freedom of expression, freedom of access to information and academic freedom.
3. From a methodological and theoretical perspective, to explore, test and extend existing methods and frameworks available for the analysis of information policy measures.

[1] US Supreme Court ruling on the Communications Decency Act.
<http://www.firstamendmentcenter.org/faclibrary/case.aspx?id=1658> [Last accessed 5/7/2004]

The specific objectives of the research were:

1. To monitor and analyse policy formulation over the relevant time period towards regulation of Internet content and access at transnational level by the Council of Europe and the European Union (EU).
2. To monitor and analyse policy formulation over the relevant time period towards regulation of Internet content and access at national level by the government of the United Kingdom (UK).
3. To learn how policy measures to regulate and monitor Internet access are being formulated and implemented in UK Higher Education Institutions through a case study approach.
4. To evaluate the impact of these measures on Internet use at the institutions, particularly with regard to the freedom of academic enquiry.
5. To compare and relate the findings of the policy formulation and implementation analyses to a range of policy models in order to explore and explain how the issues relating to the regulation of Internet access and use were framed, and solutions shaped, by the decision-making process.
6. From a methodological viewpoint, to examine the usefulness of the re-interpreted process model of policy-making suggested by Rowlands and Turner (1997) and the regulatory models proposed by Lessig (1999) as heuristic devices to explore information policy concerns.

The policy monitoring at national and transnational levels was conducted primarily through documentary analysis, and in part through participant observation. The documentary monitoring included retrospective analysis from 1996 onwards and extended through to the end of 2003, thus providing a longitudinal insight into shifts in policy emphases over the period under consideration. Although there was also much pertinent legislative activity taking place in the US during this period, analysis of this activity warrants a major study in its own right and here only brief reference is made to such developments as have impacted on UK and European contexts. Similarly, although there are many other aspects of information policy

that impact on the freedom of an individual to access information on the Internet (such as data protection, copyright and privacy), as well as other potential barriers to use such as available network infrastructure and access to computer facilities, the policy monitoring concentrated on policy that specifically aimed to regulate access to illegal, offensive or harmful Internet content. Nevertheless, some discussion is made of the 'panopticon'[2] model of the Internet as this is seen as being central to the mechanisms of 'governmentality' (Foucault, 1991 and 1997; Dean, 1999; Mehta and Darier, 1998) that promote the self-regulation of access to Internet content.

Policy studies at the institutional level were conducted via case study research at three UK academic institutions, complemented with a questionnaire study carried out with student respondents at each of the case study sites. The fieldwork for the academic case studies and the questionnaire study was carried out between October 1999 and December 2001.

1.2 Structure of the thesis

In addition to presenting the aims and objectives of the study, this initial chapter outlines the rationale and theoretical framework for the research. It provides some background to the development of the Internet and its relevance to freedom of expression and introduces the policy models that are subsequently considered in the discussion of the findings of the study.

Chapter Two will discuss the methods adopted, and the rationale for using the methods in question. The subsequent four chapters are devoted to presentation of the findings of the different components of the research: thus Chapter Three presents the results of the longitudinal policy monitoring at European Union and United Kingdom macro levels; Chapter Four presents a case study of policy

[2] After Jeremy Bentham's 19th Century vision of building design for prisons, asylums and factories that incorporated a central surveillance facility allowing observers to view the behaviour of every resident whilst preserving the invisibility of the observer (Bentham in Bozovic, 1995).

formulation within the Council of Europe; Chapter Five describes the findings of the institutional case studies carried out within three UK Higher Education Institutions; and Chapter Six presents the results of the questionnaire study carried out to explore student use and misuse of university computing networks.

Chapter Seven discusses these findings with particular regard to the theoretical and methodological implications of the findings, and their relevance to the development and advancement of knowledge in this area. Any limitations identified in the methods adopted are also discussed here. Chapter Eight is confined to discussion of the final conclusions in response to the study's central question, aims and objectives, and also identifies potential areas for further work.

1.3 Rationale and theoretical framework

The Internet is now exerting a significant impact on global patterns of access to information, education, commerce and entertainment. It has been categorised alternately as a neo-utopian liberating force facilitating the expression of alternative and dissenting speech; or a dystopian space that is responsible for an increased atomisation and fragmentation of modern societies. The author's thesis is that the Internet offers a forum that has the potential to repair, at least in part, the erosion of the public sphere identified by Habermas (1984; 1987; 1989). According to Habermas, this erosion has led to a reduction in the rational discussion of public affairs that once enabled democratic decision-making to take place. With regard to the Internet, the moral panic (Cohen, 1980) that has characterised its portrayal by the media, the resulting high levels of public anxiety and the very real dangers posed by its use to perpetrate a range of criminal activities, have led to a range of legal and policy measures on the parts of international organisations, governments and organisations. It is suggested that these measures are, at least in part, preventing the full democratic and informational potential of the Internet from being realised, and are limiting its effectiveness as a forum for rational debate.

The German thinker Jürgen Habermas devoted much attention to the conditions that he believed would make possible the rational discussion of public affairs and promote democratic decision making in order to reach the most favourable policy outcomes for society. He considered that the 'public sphere' (Őffentlichkeit) that had previously been provided by the coffee houses, clubs and salons of the Eighteenth Century, where public discussion of the important events of the day could take place independent of politicians and the court, had been eroded and distorted. This decline and distortion could be attributed to factors such as an increasing manipulation of information by the media, political 'spin doctors', technocratic 'experts' and commercial advertising. The extension of the role of the State, and the trend towards an increasing legal regulation of private life ('Verrechtlichung') was also incurring restrictions on the freedom of the individual (Outhwaite, 1994).

Habermas saw a potential remedy to this situation in the development and promotion of 'ideal speech' situations in which there is genuine equality of participation in the analysis of social problems and public policy decision-making rather than the domination of an instrumental technocratic rationality. This current thesis supports the notion of the benefits of promoting 'ideal speech', and is premised on the basis that the Internet has the potential to facilitate the expression of 'viewpoint diversity' (Newey, 1999) represented by this concept. However, it also recognises that content on the Internet, and access to that content, is subject to significant levels of regulation, that in themselves threaten to exert the same kind of distortion and erosion of debate described by Habermas (op cit).

Over the last century, the developed world has undergone a radical transformation from an Industrial to a Post-Industrial Age (Bell, 1974), characterised by a dependence on the value of services, information and knowledge as the economic and social foundations of society. Although the origins of this transformation can be traced back to the early Twentieth Century, the current rise of this 'Information

Society' has been encouraged and fostered largely by the rapid development and global reach of the Internet[3].

Many writers have recognised that the introduction of new technologies tends to be accompanied by a desire on the part of public authorities to control and regulate their use and access to them (for example, Sola Pool, 1983; Moore, 1991; Hill and Hughes, 1998, p. 181; Green, 1999; Slevin, 2000, p.220; Davies, 2002). The invention of the moveable type printing press is a good illustration of this tendency. And so it was with the Internet as it permeated beyond its military and research-led origins, and came to be used as a primary communications medium and information source, as well as a means of recreation, in universities, libraries, schools, the workplace and private homes. However, the control of Internet content and access presents very particular difficulties, as content transcends national boundaries and legislative jurisdictions. Attempts to define illegal or offensive content inevitably encounter problems due to differing cultural values and norms, as well as different legislative regimes. Technical solutions, originally hailed as holding the solution to the 'problem' of Internet control, have evidenced serious – and seemingly insurmountable – limitations and shortcomings.

Despite these difficulties, concern regarding the availability and dissemination of offensive, potentially libellous and illegal content on the Internet has led to the adoption of a number of policy measures at institutional, national and international level, with the expressed intention of monitoring and controlling access to, and dissemination of, such content. The investigation of these policy measures at both macro and micro level, and their comparison against a range of policy process models, was intended to facilitate a fuller understanding of the policy formulation process in this arena, and how this could potentially be enhanced in order to improve the decision-making process.

[3] For a useful overview of this development, see Dearnley and Feather (2001), Chapter One 'Theorizing the Information Society'.

Peace (1997) has noted the paucity of research that has been carried out to date into the issue of censorship in the university environment or University policies towards Internet regulation, whilst Bawden (1997) has noted that information policy, in particular, has been under-researched at organisational level. Likewise, Rowlands (1996) asserts the need for more 'value-critical' and 'paradigm-critical' approaches towards information policy research, and, together with Turner (Rowlands and Turner, 1997, p.51) has identified the potential for research into the interaction and impact of different theoretical models in an information policy context. In particular, they note the potential for exploration of the policy process model to engender a deeper understanding of policy problems. It is intended that this study will contribute towards developing this understanding and addressing some of the identified gaps in current research.

The study is, by definition, multi-disciplinary in that it draws on a range of academic areas of study such as the public policy sciences, law, technology and the social sciences. Its primary disciplinary focus, however, comes within the field of Information Science. According to Browne (1997b), within this discipline area the positivist paradigm has tended to prevail over other theoretical perspectives. This paradigm is based on a belief in the existence of a fixed 'truth', and the role of research is to reveal and prove this objective truth. However, this study has preferred to adopt the paradigm of post-positivism as a theoretical framework, as the inherently value-driven stance of the researcher and the role of interpretation in defining truth is considered to be of critical importance.

The post-positivist paradigm accepts the multiplicity of causes and effects that impact on a phenomenon, and, while it does accept and aim to illuminate the existence of an objective reality, it also accepts that this reality can never be fully understood or explained. Moreover, it takes account of the impact of values on the policy environment and process. To quote Browne (Ibid, p.346):

> *"..information policy, like all public policy, is embedded in the political and cultural context and consequently different values will shape both the policy and the process used to derive it."*

The mode of enquiry was intended to be exploratory and explanatory, allowing the theories and explanations to emerge from the data, rather than imposing a predetermined set of conclusions (Glaser and Strauss, 1967), and, in accordance with the post-positivist perspective used multiple sources of predominantly qualitative data. It adopted the first two of the eight approaches to policy studies identified by Hogwood and Gunn (1984), namely those that focus on policy content and on policy process, with a particular emphasis on the latter approach. It is intended to provide a normative contribution to knowledge of information policy approaches rather than focussing solely on a descriptive approach.

1.4 Social and historical context of the study

1.4.1 Development and growth of the Internet

The Internet was originally conceived in the US in 1969 with a project led by the Advanced Research Projects Agency (ARPA) to link four computers in a distributed network, ARPANET, which would be capable of surviving the impact of a nuclear strike. By 1973 ARPANET had become a national network across the US, but access was limited to universities, research establishments and defence agencies, and the network operated with a lack of overall control or security. At the same time, academic communities in the US were beginning to establish their own electronic networks. At Duke University two students established a system called USENET, a network built and organised by the users themselves, allowing them to swap information on specific topics without restriction or external control. This was followed by the establishment of a similar network for academic staff, called BITNET. The American government, identifying the potential in networking activity, subsequently decided to fund the National Science Foundation's network, NSFNET, linking universities and academic research establishments throughout the United States.

Similarly, British universities established JANET (the Joint Academic Network) in 1984, linking academic institutions across the United Kingdom. In contrast to the

earlier emphasis in the US on use for scientific purposes only, JANET had an explicit aim to serve the entire higher education community, regardless of discipline (Kahn et al, 1997, p.140).

By the late 1980s the technology existed to link the individual networks together and academics were able to exchange information internationally. From this time onwards the Internet has grown at an impressive rate and has become a communications medium of global reach, largely as a result of the development of the World Wide Web (WWW) by Tim Berners-Lee from 1989 onwards at the CERN Particle Physics laboratory in Switzerland. This facilitated a graphical interface with hypertext linking and easy browsing and navigation thus making its use more accessible and attractive to non-scientists. The popularisation of the Internet was also a result of the growth of independent, commercially-funded Internet Service Providers (ISPs): as the Internet was initially government-funded its use was originally limited to research, education and government purposes, commercial uses being prohibited unless they directly served the goals of research and education.

The combination of the development of the WWW and the coming into existence of commercial ISPs means that it is no longer just academics, students and government workers who use and provide services on the Internet. The most rapid growth in recent years has been in the area of business use, and individuals worldwide use the Internet for private and work-related communication, and for recreational, consumer and educational purposes. In the second quarter of 2001 it was reported that around 38% of UK households had home access to the Internet (Office for National Statistics, 2002); by December 2003 this had risen to approximately 50% of all UK households, with a government target having been set of all households that want it having access by 2008 (Wray, 2003). Worldwide, forecasts suggest that there will be around 1 billion Internet users by 2005 and this figure is likely to have doubled by 2010 (Castells, 2001, p.3) [4].

[4] However, these statistics should be interpreted in context: despite the global reach of the Internet there is still a huge 'digital divide' between the developed and the developing world. In 2001 the

1.4.2 The Internet and freedom of expression

Despite this popularisation and commercialisation, the education and research driven origins of the Internet have had a strong influence on Internet use and content (Faulhaber, 1997; Hill and Hughes, 1998; Valauskas, 1996). Moreover, the unplanned – and even anarchistic – origins of the Internet led to its characterisation as a forum for individualism and the free expression of alternative or controversial content, ranging from unorthodox political expression through to pornographic and obscene matter. Jordan (1999, p.3) has noted the egalitarian potential of the Internet, commenting that 'in cyberspace[5] no one can be silenced because their voice is the quietest, and no one can be heard with more effect simply because they are more aggressive'. As long ago as 1965, Arthur C. Clarke was giving poetic expression to a utopian vision of the liberating potential of new communications technologies:

> *The advent of communications satellites will mean the end of the present barriers to the free flow of information; no dictatorship can build a wall high enough to stop its citizens listening to the voices from the stars.*
>
> (Clarke, 1965)

The metaphor of McLuhan's 'global village' (McLuhan and Powers, 1989) has also been applied to the Internet to describe its ethos of a world-wide community of citizens with shared values, symbols, rituals and norms (Bekkers, 1997).

Castells (1997 and 2001) gave early recognition to the potential of the Internet as a tool for democracy. He noted that

---

Internet still connected less than 2% of the world's population and it was reported that 80% of the world's population had never made a telephone call (Millar: 2001a).

[5] The term 'cyberspace' was first used by William Gibson in his 1984 science-fiction novel *Neuromancer* referring to the geographically unlimited, non-physical space created by the interlinking of computers, telecommunications networks and digital media.

> *…online information access and computer-mediated communication facilitate the diffusion and retrieval of information, and offer possibilities for interaction and debate in an autonomous, electronic forum, bypassing the control of the media…More importantly, citizens could form, and are forming, their own political and ideological constellations, circumventing established political structures, thus creating a flexible, adaptable political field.*
>
> (Castells, 1997, pp.350-351)

A highly significant factor in determining the future development and culture of the Internet was the decision by Berners-Lee not to patent the Web; his vision of the Web was 'a global space where people could share information, ideas and goods, unfettered by any central body' (Woolnough, 2001). Laudon (1995, p.36) has noted that:

> *Among Internet aficionados there is a strong libertarian ethic that argues that individuals should be able to 'do what they want, when they want' and that the collective social welfare is advanced by the pursuit of a kind of minimally organized anarchy.*

However, he does also concede that, when carried to an extreme, such an approach risks turning into 'an amoral free-for-all with no connection to the collective social welfare' (Laudon, 1995, p.36). Such fears, combined with intensive media reporting that created a 'moral panic' (Cohen, 1980) in which the Internet was seen as almost synonymous with pornography, led to strenuous calls for regulation of Internet content – and of access to content.

In addition, from the early optimistic notions of the Internet as a virtual marketplace of ideas and opinions, 'marketplace' being used in the classical sense of an open public forum (agora), it has become a literal marketplace, where business corporations rely on a secure, 'decent' and non-controversial environment. Such pressures have led to demands for legislation and the development of a variety of non-legislative control techniques to regulate the Internet.

Thus, it can be argued that the Internet 'control' debate has been characterised by the competing perspectives of technological and political utopianism, with the Internet portrayed as an instrument of liberation, democracy and social benefit, and that of technological dystopia, with it seen as contributing to moral breakdown and loss of control on the part of Nation States. Wall (2000) has referred to these competing perspectives as being those of the 'cyber-liberators' versus the 'cyber-regulators'. Castells (2001) also maintains that the Internet has evolved into what he describes as a 'contested terrain' between the contrasting paradigms of freedom and regulation. These two perspectives are central to the investigation and discussion of measures to regulate Internet content that forms the substance of this thesis.

1.4.3 Theoretical conceptions of censorship and freedom of expression

The drive to censor information and ideas has historically been based on one of two concepts, that of harm or that of morality (Dhavan and Davies, 1978; Heins, 2001; Robertson, 1993). The first premise adopts a causalist justification for the imposition of censorship, on the grounds of the potential specific harm to society, or sections of society, liable to be incurred through the creation and dissemination of, or access to, the controlled material. The second premise is based more on a notion of 'upholding community standards' and the preservation of the morals of the individual and the society – access to material is controlled on the grounds that it is inherently 'bad'. Within UK law, definitions of obscenity have been based on whether the item in question, if taken as a whole, is liable 'to deprave and corrupt those whose minds are open to such immoral influences and into whose hands such a publication might fall'[6].

In contrast to the paternalistic approach of protecting the population from the potential harm or corruption they will undergo as a result of exposure to materials deemed to be unacceptable, the premise of freedom of expression is that the

[6] This definition, on which the *Obscene Publications Act 1959* (Parliament, 1959) is still based, was originally made by Lord Chief Justice Cockburn in 1868 (cited in Hannabuss and Allard, 2001)

government has no right to impose their versions of morality through censorship of unconventional, "bad" or "dangerous" ideas: citizens are entitled to decide these matters for themselves (Heins, 2001). Censorship on the grounds of harm is also seen as problematic on account of the near impossibility of providing evidence of a direct causal link between 'harm' and access to such material. For example, research studies have consistently failed to prove a causal link between access to pornography and the committing of sex crimes (Dhavan & Davies, 1978; O'Toole, 1998; Gavison, 1998). Feminist claims that pornography causes harm through the subjugation and objectification of women (for example, see MacKinnon, 1993; Dworkin, 1981 among many others) are harder to dismiss, although a strong argument against this line of reasoning is put forward by Feminists Against Censorship[7] and by Strossen (1996) who suggest that censorship is itself a form of oppression that ultimately patronises and disempowers women.

1.4.4 Freedom of expression as a professional ethic

Freedom of expression, according to Robertson (1993, p.95), entails '…the right to entertain ideas of any kind, and to express them publicly'. Measures aimed at controlling Internet content and access to information available via the Internet risk conflicting with a long-standing tradition in libraries and in universities of upholding the right to freedom of expression and freedom of enquiry, and of a strong hostility to censorship. The erstwhile UK Library Association[8] Code of Conduct and the American Library Association (ALA) Bill of Rights both vigorously defend the concept of free access to information without restriction. The Code of the UK Library Association states that

> *…Members have an obligation to facilitate the flow of information and ideas and to protect and promote the rights of every individual to have free and equal access to sources of information without discrimination and within the limits of the law.*
>
> (Library Association, 1996, 2e)

[7] <http://www.fiawol.demon.co.uk/FAC/> [Last accessed 5/7/2004]

[8] The Library Association has now become the Chartered Institute of Library and Information Professionals (CILIP), following a merger with the Institute of Information Scientists.

Although the professional guidance from the new body, CILIP, is less developed in this area, its draft Code of Professional Ethics disseminated for consultation in 2003 claims as one of its general principles 'commitment to the defence of, and enhancement of, access to information'. It also advocates 'impartiality, and the avoidance of inappropriate personal bias, in acquiring, and evaluating information and in mediating it to information users' (CILIP, 2003).

The ALA Statement On Professional Ethics contains the following commitment:

> *In a political system grounded in an informed citizenry, librarians are members of a profession explicitly committed to intellectual freedom and the freedom of access to information. We have a special obligation to ensure the free flow of information and ideas to present and future generations…Librarians must resist all efforts by groups or individuals to censor library materials.*
>
> (American Library Association, 1981, p.335)

Indeed, the concept of intellectual freedom has been called the library profession's 'central ethic' (Du Mont, 1991; Bundy and Stielow, 1987). The American Civil Liberties Union (ACLU) declares its opposition to censorship within libraries with the statement that 'Libraries are free speech zones' (ACLU, 1997).

1.4.5 Academic freedom[9]

Likewise, the concept of academic and intellectual freedom has been central to the development of universities – and, indeed, Castells (2001) maintains that without the academic freedom granted to US researchers in the latter half of the Twentieth Century, the Internet itself would probably never have evolved. The concept of academic freedom can be traced back at least as far as Ancient Greece, with the role of philosophers in framing arguments in support of intellectual freedom on the grounds that only through intellectual argument could one arrive at the final truth

[9] Some of the author's comments made in the course of this section have been previously published in the proceedings of the 9th International BOBCATSSS Symposium on Library and Information Science (see Cooke, 2001).

of a matter. During the early Middle Ages the academic community in a range of European universities sought to utilise the principle of academic freedom in order to create a sanctuary from the conflicting powers of the Church and the State (Sturges, 1999). A useful overview of the history of the notion of 'academic freedom' with regard to freedom of expression and of enquiry (as opposed to concerning government interference in the institutional control of universities) is provided in the text of a lecture given by Sir Robert Birley in 1972. He argues powerfully that

> *Scholarship cannot flourish in an atmosphere of suspicion and distrust. Teachers and students must always remain free to enquire, to study and to evaluate, to gain new maturity and understanding. Otherwise our civilisation will stagnate and die.*
>
> (Birley, 1972, p.12)

Birley cites an early example of a challenge to academic freedom in late 17th Century Germany where, in 1690, Christian Thomasius, a lecturer at the University of Leipzig who criticised a book by a Court Preacher in Denmark, was subsequently forbidden to lecture and threatened with prosecution. Thomasius, who nevertheless later went on to become Professor of Jurisprudence at the Academy of Halle, claimed that the Academy should be a place of 'unfettered freedom, yea, freedom which is the very life of the spirit, and without which human reason is as good as dead' (quoted in Hertz, 1962, p.111).

In the UK a strong defence of the principle of academic freedom was made by Lord Robbins in a lecture to the British Academy in 1966:

> *A society which respects and cherishes the freedom of its academic institutions and their members is much less likely to fall victim to the enemies of freedom in general than a society which does not.*
>
> (Robbins, 1966)

Section 43 of the Education Act (No.2) of 1986 endeavours to embody the principle of academic freedom within UK law with the following statement:

> *Every individual and body concerned with the government of any Further or Higher Education Institution shall take such steps as are reasonably practicable to ensure that freedom of speech within the law is secured for members, students and employees of the establishment, and for visiting speakers.* (Cited in Saunders, 1999)

This (somewhat lukewarm) embracing of the principle of academic freedom is also espoused in Section 202(2)(a) of the Education Reform Act 1988, which stipulates that an educational institution's governance arrangements must

> *Have regard to the need…to ensure that academic staff have freedom within the law to question and test received wisdom and to put forward new ideas and controversial or unpopular opinions, without placing themselves in jeopardy of losing their jobs or privileges they may have at their institutions…*
>
> (Ibid)

Middlehurst proposes the notion that academic freedom is not simply an entitlement for university personnel, but imposes a 'duty of enquiry' upon them. Thus, she comments:

> *'Academic freedom implies individual discretion to pursue (and promote in others) the quest for knowledge and truth in ways that are guided by individual choice within a framework of professional norms of conduct and behaviour. As the main vehicle for the pursuit of knowledge, scholarly enquiry carries with it a duty to question, to exercise independence of thought and judgement and to strive after creativity: in short to reflect and to evaluate critically upon past knowledge and future premises. The results of such critical enquiry must then be presented according to the conventions of reasoned argument'.*
>
> (Middlehurst, 1993)

It has been suggested by Arrowsmith (1998) that without the recognition, and indeed the 'constant cherishing', of academic freedom, an intrinsic part of the mission and purpose of higher education is lost. This freedom does not relate solely to the ability to express ideas and opinions, but also implies the ability to access freely the body of knowledge and ideas accumulated within society.

Barnett (1990, p.136) emphasises that academic freedom should be founded on the principle that academic pursuits, carried out in academic settings by academic persons, should be directed ultimately by those persons. He also notes that current defences of academic freedom tend to centre on the freedom of academic staff rather than on that of students. He points out that the early German universities were founded on a spirit of enquiry ('lernfreiheit') with the student at the centre and knowledge being acquired through reasoned debate. Such a notion of 'lernfreiheit' may be critical to the success of current trends in higher education towards independent, autonomous and lifelong learning.

The importance of academic freedom to the democratic process has been highlighted by Middlehurst (Ibid) who noted the role played by university 'centres of intellectual expertise' to the dissemination of knowledge to inform decision-making within the community as a whole, and within governmental and transnational bodies in particular. In the Germany of the early 1920s and late 1940s, Jaspers (1965) envisaged the university as having 'a role to play in the reconstruction of a more humane society, based on a more unitary and purposeful conception of knowledge' (cited in Barnett, 1990).

Given the protection awarded to free speech by the First Amendment[10] of the US constitution, and the lack of any such constitutional protection in the UK, it is perhaps ironic that the literature relating to academic freedom suggests greater restriction of such freedom in the US than has been apparent in the UK. In particular, the free speech of academics came under threat during the immediate post-war period of the McCarthy era, with academics being required to state under oath that they did not harbour any pro-Communist sympathies (Stewart, 1950). More recently the era of 'political correctness' has raised the difficult matter of drawing a distinction between the right to express ones own ideas and the duty not to cause offence. In addition, the aftermath of the terrorist attacks on New York in

[10] The First Amendment offers US citizens a constitutional right to freedom of speech by prohibiting Congress from making any law abridging the freedom of speech or of the press. For the text of the Constitution and its Amendments see <http://www.usconstitution.net/const.html> [Last accessed 5/7/2004].

September 11th 2001 and the war in Iraq in early 2003 have led to a number of attempts to suppress any 'unpatriotic' sentiments on the part of university academics in the US. Such attempts include the publication of a report listing over 100 statements that 'fail America' made by US academics such as Noam Chomsky and Jesse Jackson, (Fine, 2001).

Indeed, the threats to academic freedom in recent times in western democracies such as the UK and the US are various, emanating from a range of different sources, as described by Amit (2000, p.217):

> *Ethics reviews, codes of conduct, sexual harassment policies, increasing limits on the way in which researchers use and administer their own research grants combine with a host of frequent auditing exercises…the university is being remade into a panopticon in which university professors censor, police, audit and market themselves while institutional administrations strive ever harder to limit their own liability.*

In the UK, new challenges to academic freedom continue to present themselves; during the period in which this study was undertaken, a number of cases came under review. In one case, police confiscated a book of photographs by the late Robert Mapplethorpe belonging to the library of the University of Central England, and instructed the Vice Chancellor of the University to destroy the book; the Vice Chancellor refused to do so (Knight, 1998; O'Leary, 1998; Walmsley, 1998). There were even suggestions that the University could face prosecution for lending the book (Library Association Record, 1998a). In another case, the home of a writer and researcher engaged on writing a history of pornographic films was raided and a large collection of films and documents seized, along with his computer (Campbell, 1998a). A report by the Quality Assurance Agency (QAA, 1999) in the UK in 1999 strongly condemned the University of Lincolnshire and Humberside for allowing the censorship of Jewish books and authors from reading lists in its provision at a partner college in the United Arab Emirates. Disciplinary proceedings have been taken against Chris Brand, a lecturer at Edinburgh University, following the publication of his book, *The G Factor,* outlining

controversial opinions linking race to IQ, and comments made by Brand in an Internet newsletter on paedophilia.

However, academic freedom should not imply a lack of due sensitivity or responsibility. The tribunal report in the Brand case stated that

> *It is incumbent on any citizen to act responsibly in the manner of his public utterances. This is particularly true of the academic in exercising his academic freedom, which does not give licence to express any opinion in any way one chooses. One must be acutely aware of the manner in which material is expressed and individual views should be set in a suitable framework with due care to the sensitivity of the issue and regard to the implications of controversial statements made.*
>
> (Wojtas, 1998)

These sentiments echo those expressed in an earlier era by Albert Einstein (cited in Tight, 1998, p.74), who commented:

> *By academic freedom I understand the right to search for the truth and to publish and teach what one holds to be true. This right also implies a duty: one must not conceal any part of what one has recognized to be true. It is evident that any restriction of academic freedom serves to restrain the dissemination of knowledge, thereby impeding rational judgement and action.*

It is now common practice for Western universities to have written policy statements on the protection of academic freedom, including freedom of enquiry and freedom of expression. However, the introduction of new Information and Communication Technologies (ICT) into universities has led to a number of cases suggesting restrictions to academic freedom. Despite the potential for ICT to open up access to a 'virtual marketplace'[11] of ideas and minority viewpoints (Newey, 1999; Golding, 2000; Walker, 2000), the Human Rights Watch Academic Freedom programme[12] commented that 'While the means of transmitting

[11] The original concept of a 'marketplace of ideas' comes from Mill (1859) in *On Liberty* in referring to the potential offered by 'a constellation of printing presses and bookstores' to promote an informed and active political community in which individuals have freedom of expression.

[12] <http://hrw.org/advocacy/academic/> [Last accessed 5/7/2004]

information may be new, the old impulse to control the academics who convey this information has also grown' (Zia-Zarifi, 2001). It was reported in March 2004 that the websites of 300 academics at Birmingham University had been removed, following controversy over alleged anti-semitic content on one site. This was despite the fact that the content on the majority of the sites related to issues such as air quality, genealogy or academics' CVs (Curtis, 2004). Other specific recent examples of cases involving constraints on academic freedom linked to the use of ICT are described by Dearnley (1999) and Baty (2003)[13].

Simon Davies, Director of Privacy International[14], suggests that recent UK legislative developments such as the *Regulation of Investigatory Powers Act 2000* (RIPA)[15] (Parliament, 2000a) threaten to 'turn universities into wired Dickensian workhouses with central control and monitoring' (Davies, 2000). He envisages the implications for academic freedom of such measures as being potentially very serious: 'Once management institutes an architecture of surveillance…the relationship changes between academics and their institutions' (Ibid). It will be seen that such fears were also reflected in the comments made by academic respondents during the course of the three academic case studies described in Chapter Five of this thesis. With regard to filtering technologies, Davies describes their implementation in an academic context as representing a 'Faustian Pact' that compromises academic freedom by the drive towards self-censorship that it incurs and the repression of 'controversy' that he considers should characterise academia (Ibid).

The role of self-censorship in preventing true freedom of expression and freedom of access to information should not be underestimated. The potential for surveillance of electronic communications to induce a new power structure of 'electronic governmentality' (Foucault, 1991; Dean, 1999; Mehta and Darier,

[13] These examples are also discussed in greater detail in Chapter Five.

[14] <http://www.privacyinternational.org/> [Last accessed 5/7/2004]

[15] <http://www.hmso.gov.uk/acts/acts2000/20000023.htm> [last accessed 5/7/2004]

1998) by acting as a modern-day version of Bentham's design of the Panopticon has been noted by several writers. The visionary prison design of Bentham's panopticon meant that prisoners could not tell whether or not they were under observation, which led to them behaving as if they were being observed even when no guard was actually present. There are clear parallels that can be drawn here with the 'self-censorship' that an Internet user who is aware of the possibility of having their communications monitored may consequently exercise. Indeed, Castells (2001, p.173) maintains that the use of electronic workplace surveillance is, in the Information Age, a more pervasive and invidious means of replacing the shop floor control of workers that was previously exercised by management in the Industrial Age. Miller comments that 'The Information Superhighway's ability to move us further toward a panoptic society can counter any positive impact it may have on strengthening democracy or free speech' (Miller, 1996, p.265). Blanchette and Johnson also make the point that democracy cannot flourish in an environment of surveillance, and maintain that 'the very nature of self and the kinds of personalities that develop in a surveillance society are different' (Blanchette and Johnson, 2002, p.36).

However, a desire to protect freedom of expression is not easily reconciled with the fears of network providers, systems operators and university administrators concerning their legal liabilities with regard to the dissemination of offensive and/or illegal Internet content. Librarians have also demonstrated concern with regard to liability issues raised by their provision of unrestricted Internet access to the general public, to students and to the wider academic community. In particular, the availability of pornographic, defamatory, and 'race-hate' material on the Internet have led to fears concerning possible breaches of the *Obscene Publications Acts* of 1959 and 1964 (Parliament, 1959; Parliament, 1964), the *Protection of Children Act 1978* (Parliament, 1978), the *Computer Misuse Act 1990* (Parliament, 1990) and the *Criminal Justice and Public Order Act 1994* (Parliament, 1994a).

1.4.6 Measures to regulate Internet access and content

These concerns have led to the development of a variety of restraints and controls by software developers, network providers and administrators, librarians and others responsible for the provision of Internet facilities and content. Such measures include the development and implementation of filtering, monitoring and ratings technologies; metadata schemes for describing and organising Internet resources; Acceptable Use Policies (AUPs) and Codes of Conduct governing network use within institutions and organisations; user education to promote appropriate use of facilities; and requirements for users to sign disclaimers limiting the legal liabilities of access providers.

Within the UK academic community UKERNA (the United Kingdom Education and Research Networking Association), the body responsible for the provision of the JANET service to the UK Higher Education community, has its own JANET AUP[16] (Wood, 2003) and urges individual institutions to devise their own AUP. Penalties that may be imposed on institutions for contravention of the JANET AUP range from suspension of network services through to referral for legal action. In addition, a number of legislative and self-regulatory initiatives have been implemented by national governments and international organisations in order to control the provision of, and access to, 'inappropriate' Internet content – such measures are given detailed consideration in Chapters Three and Four of the thesis.

1.4.7 Technical solutions: filtering, rating and labelling

> *…we must not think to make a staple commodity of all the knowledge in the land, to mark and license it like our broad-cloth and our woolpacks.*
>
> (Milton, 1973, p.26, originally published 1644)

[16] <http://www.janet.ac.uk/documents/use_policy.pdf> [Last accessed 5/7/2004]. Detailed consideration of the JANET AUP is given in Chapter Five of the thesis.

From the time of the initial moral panic concerning the Internet it has often been suggested that the control of Internet content and problems of access to 'inappropriate' content would be resolved through the implementation of technical solutions, in particular the use of filtering software (Burt, 1997; Volokh, 1997). In the US a number of legislative initiatives have been put forward to mandate the implementation of filtering software, in particular with regard to public access to the Internet in schools and libraries. Many private corporations and public sector organisations have also adopted Internet filtering and monitoring software with enthusiasm as a means of avoiding time-wasting by employees and reducing the risk of potential legal liability for their communications (Datamonitor, 2002).

However, such software has demonstrated considerable technical limitations and its potential impact on freedom of expression and freedom of enquiry has been noted. It has been argued that the installation of filtering software affords greater control to the end user over access to content and balances the right to freedom of expression with the right not to have to encounter offensive material (Burt, 1997; Auld, 2003; Cronin cited in Pierce, 2003). This perspective has been subject to much debate and challenge, not least on account of the inaccuracy of many of the products, their potential for bias and the lack of transparency of the process that determines blocking decisions by software providers.

Filtering software usually works on the basis either of blocking pre-specified keywords found on a web page or website, or by blocking websites that have been identified by the software providers as containing 'undesirable' content. Keyword blocking in particular, has been demonstrated to be an inaccurate and imprecise 'blunt instrument' with a tendency to under- and over-block as a result of the ambiguity of terms and lack of context sensitivity. It is also not suited to handling inappropriate graphic images that are liable to slip through the filter if they do not contain any offensive text. Other forms of filtering include keyboard monitoring, which checks keyboard input against a pre-set list of terms, preventing users from using particular search terms. It can also be useful for blocking outgoing information such as credit card numbers and personal information in chat rooms or emails (Thomason, 2001). In addition, it is possible for systems administrators to

restrict access to certain protocols, thus preventing the use of specific types of Internet services such as chat rooms or Usenet (Ibid).

Lasica puts forward arguments against the use of filtering software, quoting David Sobel, legal counsel for the Electronic Privacy Information Center (EPIC)[17], who defines the use of such software as 'a move toward the privatising of censorship' (Lasica, 1997). He shares the concern that filters are too subjective and constitute a threat to freedom of speech, screening out 'much more than smut' such as information on alternative lifestyles, family planning, atheism, feminism and women's organisations, animal rights groups, political organisations, safe sex and drug use. An example of evidence of bias in the selection of sites blocked by CyberPatrol[18], a popular filtering software package, was demonstrated by a University student who reverse-engineered the software to enable him to access the list of sites blocked by the software. He found that the list included sites critical of CyberPatrol and its parent company, Mattel, as well as a website for the American left-wing magazine *Mother Jones* (Fine, 2000).

Mezey also notes the inaccuracy of most filtering programs and the tendency to block useful and non-sensitive sites (Mezey, 1998). In particular, he notes the conclusions of an EPIC report *Faulty Filters: how content filters block access to kid-friendly information on the Internet* (EPIC, 1997), which found that 'the world's first family-friendly Internet search site', Net Shepherd Family Search, regularly blocked over 99 per cent of non-sensitive material that could be of interest to children. An updated EPIC report published in 2001 suggested that filtering and rating systems, far from being mere software features or tools, can be considered to constitute 'fundamental architectural changes that facilitate the suppression of speech far more effectively than national laws alone ever could' (EPIC, 2001).

[17] <http://www.epic.org> [Last accessed 5/7/2004]

[18] <http://www.cyberpatrol.com> [Last accessed 5/7/2004]

In addition to the first EPIC report cited above (EPIC, 1997), which made comparisons between 100 searches using Net Shepherd and 100 using the unfiltered Alta Vista search engine on which it is based, there have been other attempts at testing filtering software to assess the performance of the various programs. One of the more extensive projects was the TIFAP (The Internet Filter Assessment Project) study[19], which was carried out by a team of librarians in the US in 1997. Conclusions arising from the study included the importance of being able to configure settings on the software to best meet local needs; software based on site lists (lists of blocked URLs) is more accurate than that based on keyword blocking; user feedback is important, both in terms of informing users that material has been blocked, and in enabling feedback from users to software suppliers; users are not satisfied with retrieving material from 'guided' Internet access but require powerful search engine facilities; and finally, there is demand for software that includes a "patron override function", that is, that warns users of explicit and/or offensive content, but does not block access (TIFAP, 1997). Much of the work carried out by the TIFAP study is outlined in greater detail by Schneider (1997).

The potential issues arising from the technical imperfections and limitations of filtering technologies, and the difficulties encountered in arriving at a universal definition of 'acceptable content' that is nevertheless sensitive to the norms of local 'community standards', are significant. Apart from the potential impact on individual freedoms of over-blocking that the implementation of filtering software may incur, concerns have also been expressed with regard to the 'false complacency' that may result from its use. Parents, librarians and teachers may be led to adopt a misplaced sense of security, putting too much reliance on filters rather than personal supervision to prevent children from accessing content that they consider harmful.

Several projects aimed at testing the accuracy of filtering software have been carried out demonstrating that a substantial extent of both under- and over-

[19] <http://www.bluehighways.com/tifap/> [Last accessed 5/7/2004]

blocking of 'objectionable' content occurs with the most popular software packages. For example, one study found that SurfWatch failed to block 56% of objectionable material (in contrast to its claim to block 90% to 95% of objectionable material) and improperly blocked 7% of non-objectionable sites (Hunter, 2000). These results have been replicated in several other studies; for example, a *Consumer Reports* study carried out in 2001 that tested a range of the more widely-used software, together with AOL's parental control facility, reported that 'Internet filters have shown little improvement since the magazine last tested them in 1997' (Consumer Reports Online, 2001). An Australian study found that the filters that they tested blocked 78.6% of pornographic sites, but only 50% in the other 'offensive' categories (CSIRO, 2001). It also found evidence of substantial over-blocking, as did a study carried out by the National Coalition Against Censorship (Heins and Cho, 2001). The latter commented, 'No filtering technology, no matter how sophisticated, can make contextualized judgements about the value, effectiveness or age-appropriateness of online expression' (Ibid).

However, not all forms of filtering work on the basis of excluding resources: recommender systems use evaluation of resources to select 'in' those that meet certain specified criteria (Resnick and Varian, 1997). Both selection and exclusion filtering rely on metadata, described by Dempsey and Heery as 'knowledge which allows humans and automated users to behave intelligently' (Dempsey and Heery, 1998, p.149) but which is more easily understood as 'data about data'. In practice, metadata involves the tagging of data records to label resources in such a way as to enable the identification, description and location of networked resources and to facilitate the rating of content according to suitability for different user groups (Sturges, 1997, p.21). Links to a wide range of online metadata resources, including background documents, are provided by the International Federation of Library Associations (IFLA, 2003). A useful review of metadata standards and practice is provided by Dempsey and Heery (1998), who also discuss the management of metadata and the use of search and retrieve protocols and models of metadata format.

Ratings and labelling systems are intended to aid the end user in making a decision about the suitability of a particular resource. Labelling is a means of identifying the contents of an electronic data file without having to open it, the label providing the user with enough information to decide whether to open it. Rating provides a means of assigning a value to the data file, based on defined assumptions or criteria. Details of the rating of a file may be stored on a metadata label. Filtering can be carried out on the basis of selecting or excluding files as a result of the rating assigned to them. The rating or label can be assigned either by the creator or distributor of a resource, or by an independent agency designated for the purpose (as, for example, with the British Board of Film Classification for the UK film industry). It is probable that many different agencies will become involved in the rating of Internet resources, but the quantity of sites and the rapid growth of the Internet would make it an impossible task for any one body to rate more than a small percentage of available resources.

PICS, the Platform for Internet Content Selection, is a rating standard that established a consistent way to rate and block online content. It was developed in 1996 by Paul Resnick and James Miller of the World Wide Web Consortium (W3C), an international non-governmental consortium of Internet industry leaders, trade associations and public interest groups. PICS aims to facilitate the development of technologies that give Internet users the ability to control the kinds of material to which they, or their children, have access. The PICS technology allows any organization or individual to develop a labelling system which reflects their tastes and standards and, if they wish, to enable others to use these labels to select or block content (Australian Broadcasting Authority, 1997, p 13). It is thus not a rating system in itself, but 'a technique that allows rating and filtering systems to operate' (Slevin, 2000, p.227).

An example of a PICS-based rating system is RSACi, originally devised by the Recreational Software Advisory Council (RSAC) and subsequently further developed by the Internet Content Rating Association (ICRA)[20], which succeeded

[20] Information about ICRA can be found at <http://www.icra.org/about> [Last accessed 5/7/2004]

RSAC on its dissolution in 1999. ICRA states as its aim to empower the public, especially parents, by helping them to make informed decisions about electronic media via the open and objective labelling of content (ICRA, 2003). It thereby hopes to combine the dual aims of protecting children from potentially harmful material, and simultaneously protecting free speech on the Internet (Ibid). The ICRA scheme consists of label descriptors that users can assign to resources on a scale of 0 – 4 on five content categories: chat; language used on the site; nudity and sexual content; violence; and 'others' such as gambling, drugs and alcohol. An important point is that ICRA itself does not rate Internet content, nor does it make value judgements about sites. The system is intended to allow the content providers to self-rate their sites using the ICRA labelling scheme.

In addition to this initiative, the Microsoft Corporation, Netscape and Progressive Networks have co-operated in the formation of the Information Highway Parental Empowerment Group. The Group has been working on a system that relies on content providers conforming to a rating system that identifies the type of material they offer. However, while voluntary rating may work well, in the majority of cases it requires the co-operation of content providers and only a minority of providers elect to rate their sites. Moreover, it has been argued that voluntary practices are unlikely to deter those who are really determined to get their message across, and should not be relied on by those responsible for providing public access to the Internet as a means of preventing offensive material being accessed on their machines (Capitanchik and Whine, 1996, p.13).

A comprehensive list of links to Web sites offering further arguments against the use of ratings and labelling schemes has been provided by Finkelstein of the MIT Student Association for Freedom of Expression (Finkelstein, 1998). Similarly, ACLU has produced a strong criticism of the long-term implications of Internet rating and blocking schemes, suggesting that they will lead to the Internet becoming 'bland and homogenized' (ACLU, 1997). More worryingly, they maintain that such schemes are 'open to abuse by governments eager to censor and control information' (Ibid).

This argument is also put forward by Lessig (1999) who suggests that labelling schemes offer a potential for invisible 'upstream' filtering and a lack of transparency in restrictions to information access. Moreover, he makes a strong case against 'perfect filtering', even if the technology allowed this to take place. If rating and labelling schemes do permit us accurately to screen out undesirable content, society may be the poorer because we never have to 'confront the unfiltered', for example issues of poverty and inequality elsewhere in the world (Lessig, 1999, p.180). This point is also made by Shapiro (1999), and by Stoker (1999) who applies it to the use of filters in an academic environment by commenting that it is not part of the role of a University to deliberately shield its students from 'some of the more unpleasant features of life' (Ibid, p.4). Shapiro (1999) comments that 'total filtering' allows us to avoid information that leads to 'cognitive dissonance' by confronting us with challenging or uncomfortable facts ("freedom *from* speech"). This in turn means that, instead of re-evaluating our own beliefs and behaviours in the light of new evidence, we 'would likely become self-satisfied and unchallenged, lacking motivation or curiosity' (Ibid, p.111). Even the W3C have noted the dangers of any one labelling standard becoming too powerful: 'If a lot of people use a particular organisation's labels for filtering, that organisation will indeed wield a lot of power. Such an organization could, for example, arbitrarily assign negative labels to materials from its commercial or political competitors' (cited in Slevin, 2000, p.227).

1.5 Introduction to policy models

In investigating the decision-making process that determines policy measures with regard to regulation of the Internet, and the implications of those decisions, the study used the 're-interpreted policy process' typology proposed by Rowlands and Turner (1997) as an aid to understanding the complexity of factors involved in this area of decision-making. A central aim of the study was to compare the features of the three policy-making models presented in the typology with those that appeared to be evident in policy formulation towards Internet content and regulation within the European Union, the Council of Europe, the UK national government and three selected UK Higher Education Institutions. The use of

policy models in this way can be useful as a means of representing and simplifying reality, in order better to understand social processes – although Parsons (1995) warns of the need to always maintain a critical stance towards such models as there is a danger that we will use them to enable us to see what we want to see.

The three policy process models, the '**rational actor**', the '**bureaucratic imperative**' and the '**garbage can**' are derived from a re-interpretation of Lasswell's functional staged model. Lasswell (1970) noted the value of using models as a heuristic tool to explore and explain policy-making, noting that 'Systematic models provide a means of exploring interdependence among the functional components of a policy process' (Ibid, p.9). The functional staged model represents policy making as a linear process, with clearly defined, logical stages and the rational, unimpeded pursuit of policy goals from initial issue identification through to evaluation of policy outcomes:

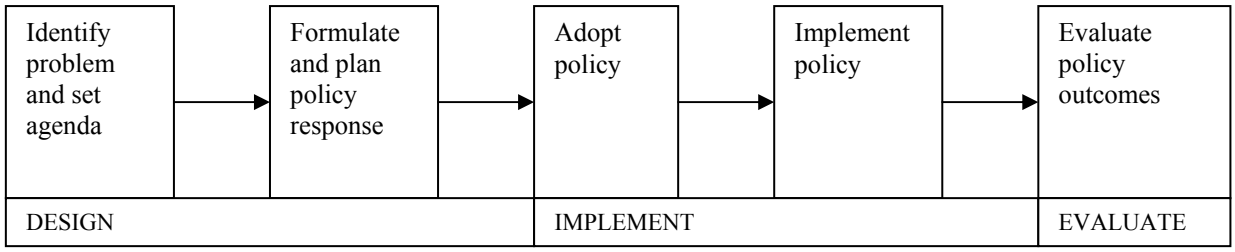


Fig. 1.1: Lasswell's staged model of the policy-making process (as represented by Rowlands and Turner, 1997, p.50)

However, this depiction of policy making as an unencumbered, wholly rational, uni-directional and finite process does not easily fit with the more chaotic, turbulent nature of policy making in a real-life organisational context. Recognition of this mismatch has encouraged a redefinition of the policy process in order to better understand and interpret the reality of what actually happens in the process and how real-world policy decisions are shaped. This redefinition forms the basis of the re-interpreted policy process model (Rowlands and Turner, 1997), as illustrated diagrammatically in fig. 1.2 overleaf.

POLICY PROCESS MODEL IDENTIFIED AS	RATIONAL ACTOR	BUREAUCRATIC IMPERATIVE	GARBAGE CAN
Policy process based on	Rational analysis and objectivity	Experience, intuition and achievement of consensus	Influence of policy actors, networks and power structures
Policy process conceptualised as	Objective and impartial planning activity	Incremental and short-term problem-solving	Random attachment of solutions to problems
Policy process characterised by	Decision-making in context of perfect knowledge and availability of all pertinent information Cost-benefit assessment of all possible policy alternatives Adequate time-frame for decision-making and policy implementation Control over policy environment – implementation unimpeded by extermal variables Consistent pursuit of explicitly stated policy goals to successful achievement of policy outcomes	Rationality constrained by real-world context and lack of control over external variables Takes account of organisational context and cultures Recognises human limitations and imperfections of policy actors Knowledge is imperfect and the selection and interpretation of information is subject to potential bias of policy actors Values, norms and institutional procedures subvert original policy goals Rules-governed, cautious and pragmatic, aiming at achievement of consensus and conformation with organisational rules	Unpredictable, non-linear, random and chaotic pursuit of ill-defined policy goals Ambiguity and lack of clarity in problem definition, which is ultimately determined by political preferences of stake holders Problems constructed to justify solutions Organised 'networks of anarchies' with political bargaining and 'horse-trading' Fluid participation of range of actors in policy process – no active participant dominates Complexity – decisions driven by politics, people and events Involves fundamental value-shift (Rommetveit, 1976)

Fig.1.2: Characteristics of the Re-interpreted policy process

1.5.1 Re-interpretation of the policy process: the 'Rational Actor'

Of the three policy process models in the reinterpreted typology, it is that of the 'Rational Actor' that is closest to Lasswell's original representation of the policy process. The 'Rational Actor' model suggests that in an ideal world, decision-making would be the outcome of perfectly rational processes in a context of perfect knowledge; policy implementation would be pursued consistently, unimpeded by external variables and brought to a successful conclusion (Rowlands and Turner, 1997). Within the model, decision-making is based on a linear process involving the identification of problems; thorough consideration and description of all facets of the problem; consideration of different solutions based on the constraints identified; outlining of the advantages and disadvantages of each potential solution; and the choice of a solution that will achieve maximum benefit (Burger, 1993). This implies that decision-making takes place in a context in which adequate time is available, and that implementation is not impeded by any interfering variables. However, Rowlands and Turner (1997) also suggest that this model represents an unattainable ideal, assuming, as it does, that policy formulators and implementers pursue policy goals in a wholly rational manner and that they can exert a perfect control over the policy environment.

1.5.2 Re-interpretation of the policy process: the 'Bureaucratic Imperative'

A potentially more realistic interpretation of rational policy-making in the real world is offered by the notion of 'bounded rationality' proposed by Simon (1957; 1976), in which 'rational decision-making has to be understood in terms of the organizational and psychological context within which decisions are taken' (Parsons, 1995, p. 279). This 'bounded rationality' takes account of the context in which decision-making takes place, the 'passions' of decision-makers, the impossibility of obtaining perfect knowledge on which to base decisions, and the human limitations of those who are making and implementing policy decisions (Ibid).

The notion of 'bounded rationality' characterises the 'bureaucratic imperative' model of the re-interpreted policy process (Rowlands and Turner, 1997; Hill, 1993), in which rational attempts to achieve policy goals are subverted by organisational factors and cultures. The cognitive limitations of individuals, and the organisational division of labour that encourages a limited 'departmental' perspective, detract from a perfect rationality. In addition, personal and institutional values, norms, procedures and accepted wisdoms all affect policy in ways that are not always conducive to the achievement of the ideal outcomes (Burger, 1993; Rowlands and Turner, 1997). Policy-making is essentially rule-governed (Burger, 1993) and aimed at the achievement of consensus; this favours policy measures that tend towards conservative and cautious approaches, and the protection of the interests of the most powerful stakeholders (Rowlands and Turner, 1997). The emphasis on rules and regulations tends towards a situation where conformity to these rules and regulations becomes an end in itself, rather than achievement of the original policy goals.

The model also suggests that policy-makers tend to react in an incremental fashion to immediate short-term problems rather than engage in long-term planning. Solutions are based on a pragmatic agreement of what can be achieved in circumstances of uncertainty or ignorance: it is, as described by Rowlands and Turner (Ibid), 'the art of the possible'.

1.5.3 Re-interpretation of the policy process: the 'Garbage Can'

Whereas the other two policy making models assume that policy formulation is inherently an orderly, rational, continuous and linear process, proceeding from an initial understanding of a problem to the application and evaluation of measures designed to resolve it (Rowlands and Turner, 1997), the garbage can model depicts policy making as

> *…a garbage can into which policy goals, organizational rules and constraints, the 'right climate' and other often unexpected variables are thrown together. The resulting policy*

outcome is often unpredictable and because of the ambiguous nature of the policy goals themselves, often unrecognisable.

(Kingdon, 1984)

With garbage can policy formulation the place that an issue occupies on the policy agenda depends largely on the importance attached to it by the various stakeholders, and problems are 'constructed' in order to justify solutions. The model is particularly useful in illuminating the early stages of policy formulation, in particular, the issue of problem definition. There is an emphasis on the role of policy actors, and the influence that individual stakeholders can bring to bear on the policy process, particularly at the problem definition stage: indeed, Rowlands and Turner (Ibid) have characterised this model as being more about politics and power structures than about rational argument.

1.5.4 Lessig's models of direct and indirect regulation

The models proposed by Lessig (1999), indicating the forces and modes of control that act to exert direct and indirect regulation on an issue or policy area, have also been used to interpret and understand the findings of this study. It was anticipated that these would be of heuristic use in the light of the multiplicity and complexity of the forces and modes of control involved in regulatory measures towards Internet use and content.

Baker (1989) recognised that control over knowledge can be exercised by a range of different forces and means, such as individuals, governments, the market place, legislation and social censure. Peace (1997) has noted the complexity of legal, ethical, technical, governance and economic issues that are involved in the formulation of information policy at the micro level within academic institutions. At the macro level, the multiplicity of forces that constitute a 'national information policy' have been described by Rowlands and Turner (1997, p.48) as an amalgam of statutory law, common law, social norms, administrative practice, market forces and international agreements and treaties.

The model developed by Lessig (1999) can be used to illustrate the way in which these varied forces act to constrain and regulate information flows, as shown in Figure 1.2.

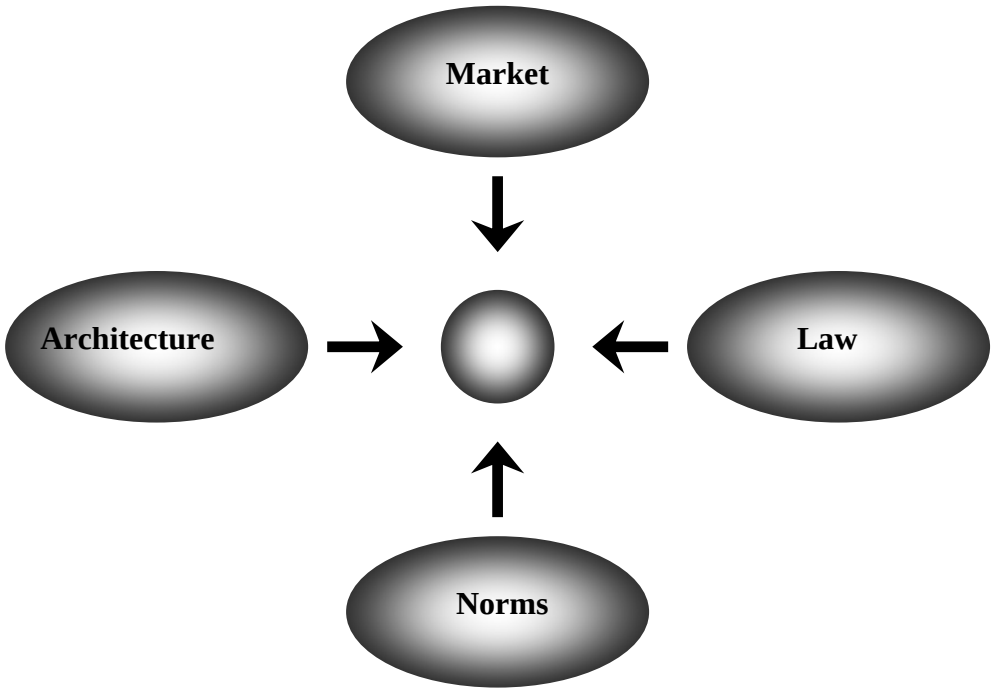


Fig. 1.3: Lessig's model of direct regulation (Lessig, 1999, p.88)

In the model, regulation is exerted on the central 'dot' by the different forces of law, the market, social norms and 'architecture' (in Lessig's application of the model to Internet regulation, this is represented by 'code'[21]). As an example to illustrate the different modalities of regulation represented by the model, censorship in the online or offline environment may be exercised through legislation (for example, Acts such as the *Obscene Publications Acts* of 1959 and 1964); the market (for example, pricing strategies that restrict access to information to specific sectors of the population); norms (for example, religious beliefs that may, in particular, lead us to 'self-censor' our own access to information sources); and 'architecture' (for example, shelving pornographic

[21] For example, the use of age verification schemes, or filtering software.

magazines on the top-shelf to restrict access). The regulation is direct and usually transparent to those whom it affects.

However, regulation is not always direct, and this is particularly true of the many self-regulatory initiatives that have been implemented with regard to the control of Internet use and content. Lessig has therefore further developed his model to illustrate the ways in which indirect regulation can operate, particularly through the implementation of legislation that exerts an influence on the other modalities of regulation. This model of indirect regulation is shown in Figure 1.3.

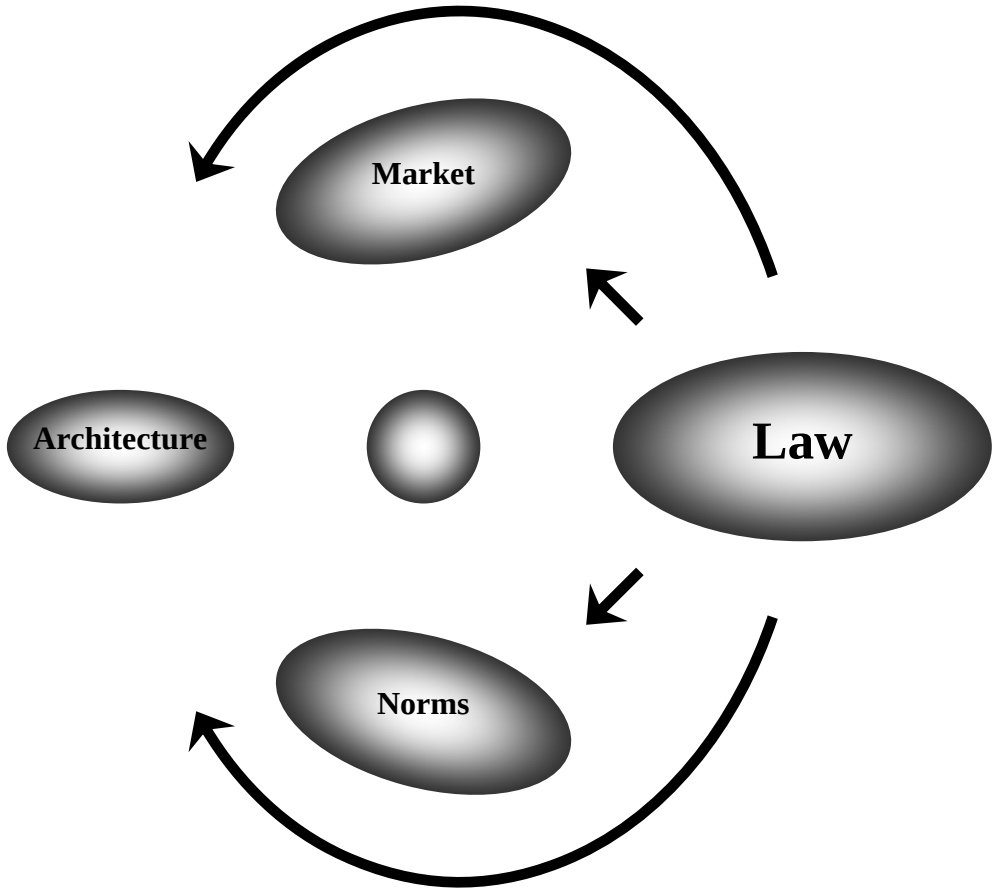


Fig. 1.4: Lessig's model of indirect regulation (Lessig, 1999, p.93)

In this model direct regulation, whereby the law instructs citizens on how they should behave and punishes deviation from that behaviour, is replaced by legislative and regulatory initiatives that are used to modify the other modes of constraint (the market, social norms or technical 'architecture') in order to produce the desired control. For example, market conditions (such as the cost of petrol) may be manipulated by government (for example, by higher taxation) in order to regulate behaviour (in this case, perhaps, to reduce traffic congestion). With regard to the regulation of Internet content, the withholding of grants to libraries that do not implement filtering software[22] is a good illustration of the government exercising indirect control. As Lessig (Ibid) points out, this model of regulation risks producing a regulatory environment that lacks transparency and undermines political accountability. Whereas a law restricting the use of private cars can be seen to be a clear statement of the government's position on transport regulation, higher petrol prices through increased taxation may be confused by consumers as being the responsibility of 'greedy' oil companies and petrol station owners.

However, an alternative perspective on self-regulation is offered by McIver et al (2003), who maintain that the kind of 'soft law' that is represented by self-regulatory approaches, such as charters and codes of practices, is more effective than 'hard law' (legislative instruments) in coping with the 'turbulence' resulting from changing norms, values and systems in an era of globalisation and rapidly changing technical and political environments. In some cases, it may also act as the 'stepping stone' to hard law. This kind of 'norm-based governance', with rule-making derived from established community values and unwritten norms could be argued to represent a more democratic form of regulation than the more top-down approach of formal hard law (*Harvard Law Review,* 1999).

[22] As, for example, is the case with the Children's Internet Protection Act in the US.

1.6 Conclusion

This Chapter has introduced the research question that the study intended to explore, namely the alignment (or non-alignment) between measures being adopted at a range of organisational levels to regulate Internet use and content, and the protection of freedom of expression and freedom of access to information in the online environment. It has suggested that the resolution of the apparent conflict between the role of universities and libraries in upholding freedom of expression and opposing censorship, whilst remaining responsive to the need to remain at all times within the confines of legality and to avoid undue offence to the sensitivities of their clientele, is of crucial importance.

It has also introduced a range of models that were used in the study to inform and illuminate the policy-making process that led to the adoption of such measures. With regard to the theoretical context of the study, the work of Jűrgen Habermas has been discussed in reference to the concept of the public sphere and the ideal speech situation, as an analogy to the democratising potential of the online environment. The rationale for the study has been presented on both a methodological basis, and in terms of the challenges to freedom of expression presented by current modes of Internet regulation. With regard to the theoretical framework for the study, this has been located within the paradigm of post-positivism.

The next Chapter will outline the methods adopted in carrying out the research and will discuss the rationale behind the adoption of such methods, with particular reference to the relevant literature on methodology.

CHAPTER TWO: METHODS ADOPTED

2.1 Introduction to the research strategy

This chapter outlines the different stages of the research, describes the general characteristics of the methods chosen, and indicates the rationale for choosing each of the particular methods. Limitations to the scope of the research are identified, as are any ethical issues pertinent to the research strategy. Chapters Three to Six inclusive of the thesis present the findings from the different components of the study, the relevance and implications of which, when taken as a coherent entity, are discussed in Chapter Seven. Chapter Seven also discusses any limitations of the methods adopted that emerged in providing answers to the research questions. Chapter Eight offers reflection on alternative approaches that might have yielded additional useful data, and suggests areas for potential future investigation.

The research involved three separate studies, although these were closely related in terms of aims and objectives, and there was some overlap in methods adopted:

1. Longitudinal monitoring, over a fixed period, of policy formulation and implementation at national and transnational levels, to characterise the development of policy over time and the predominant nature of the policy making process. This policy monitoring was carried out through a combination of analysis of primary and secondary documentary sources and participant observation.
2. Institutional policy formulation, implementation, and impact, was investigated using the case study approach at three UK Higher Education Institutions (HEIs). The case studies were carried out using a combination of methods including semi-structured interviews, observation and scrutiny of documentary evidence. The information thus obtained was supplemented by that obtained from the third element of the research, the questionnaire study.
3. At each case study site a questionnaire survey was carried out among a targeted group of students to determine their experiences of, and attitudes

towards, measures implemented in their institutions to control their network use.

Given the use of multiple methods, attention was paid to applying an integrated approach to the data collection strategy, with different elements of the study aiming to build on, clarify, or test previous findings. This process of triangulation was intended to ensure reliability and validity of the findings.

In order to advance the theoretical understanding of policy formulation, the findings of the studies were analysed against the re-interpreted policy process models proposed by Rowlands and Turner (1997) and Turner (1999). To gain further insight into the role of the different factors impacting on policy in this area, the models of direct and indirect regulation proposed by Lessig (1999) were also used to illuminate the findings of the study. A further model is also proposed, based on the findings of the study, in order to build on the understanding and explanation that can be gained from the use of the existing models.

2.2 Longitudinal monitoring of policy

A central aim of the study was to monitor the development over time of national and international policy formulation with regard to regulation of Internet access and content. In order to assure an appropriate depth and integrity of analysis of the issue under investigation, the monitoring was limited to policy approaches adopted by the UK at national level, and by the EU and the Council of Europe at transnational level. This macro-level policy monitoring was important in terms of understanding the wider context within which institutional policy formulation was taking place, and in informing the debate concerning the desirability of alternative models of Internet governance. The policy monitoring took place between 1998 and 2003 inclusive, at a time when the issue of access to 'unacceptable' Internet content was receiving considerable media attention and was therefore high on the policy-making agenda of private and public sector institutions, national governments and international bodies. Relevant literature was also reviewed in

order to conduct retrospective policy study for the years 1996 – 1997 inclusive, to set the context for subsequent policy initiatives.

The methods used to carry out the policy monitoring consisted of the analysis of primary and secondary documentary sources, and participant observation in the process of formulating Council of Europe guidelines to access to networked information (see Sturges, 2000a). Although some reference is made in the course of the thesis to important policy developments in other geographic areas where these have clearly impacted on the areas under study, the scale of the study precluded in-depth investigation beyond the stated geographical and political scope.

2.2.1 Documentary analysis as a research method[23]

Developments in policy approaches by the EU, the Council of Europe and the UK government towards the control of Internet use and content were monitored primarily by regular scanning of the professional literature, the news press and relevant websites. In addition, a wide range of formal policy documents from government bodies and Non-Governmental Organisations (NGOs) were scrutinised. The chosen approach accorded with Denscombe's assertion (1998, pp.158-159) that documentary analysis is appropriate in circumstances where documents can be considered as 'a source of data in their own right'. Such an approach also offers the advantage of relatively easy availability to data sources with fewer ethical problems than may be encountered in gaining access to people as research subjects. The use of official policy documents, whose primary purpose is to enhance accountability, offers potential advantages in terms of their attention to detail, systematic approach, accuracy and public availability. However, such sources may also lack objectivity, offering a partial version and selective interpretation of the evidence, and thus require a high level of critical evaluation. Nevertheless, if a sufficiently critical approach is adopted, such documents can

[23] For the purposes of this study, and the discussion that follows in this chapter, 'documents' refers to a range of sources including websites, electronic mail messages and press coverage, as well as published hard copy sources.

reveal much through the analysis of the priorities and values conveyed through the text, and the manner in which different ideas are related through the text (Ibid). The focus on values in the current study meant that these official sources, in addition to being readily accessible, proved to be a rich source of data, in particular with regard to the analysis of policy priorities and emphases.

The advantages of relatively easy (and generally non-costly) access to data presented by documentary analysis as a method are accompanied by those of the permanence of the data thus acquired, and its openness to scrutiny by subsequent researchers. Creswell (1997) also adds the concept of the benefit obtained from using 'thoughtful' data, enriched by the attention given to its compilation. Nevertheless the method has its disadvantages and limitations: careful consideration needs to be given to the authenticity and credibility of the source, its representativeness, and its true meaning (for example, what has been left unsaid, and what is written 'between the lines'?). It is also important to use a balanced selection of documents that is influenced as little as possible by one's own bias or a desire to confirm one's own hypothesis (Bell, 1993, p.70). This is particularly true in the case of value-critical research, such as the current study. Relevant documentary sources may not be publicly available, or may be hard to locate, and issues of privacy, confidentiality and consent may also have to be addressed (Ibid). The wide public availability of a full range of relevant documentary sources on the Internet meant that the current research did not encounter significant access difficulties, although it was necessary to give continual consideration to issues of bias and representativeness. Considerable press coverage and attention in the professional literature to issues related to 'unacceptable' Internet content further extended the range of sources.

The advantages of use of the Internet as a data source for policy research of this nature have been described by Hamilton (2003): for example, its global reach, constant updating of topical issues, access to a broad spectrum of bodies with a wide range of viewpoints and easy retrieval facility. However, these advantages are accompanied by some limitations, such as potential bias, the lack of scientific rigour and the questionable validity of some Internet sources, together with the

transitory nature of much of the information. To resolve the latter issue, hard copies of important documents were made. The issues of bias and validity were addressed by using careful evaluation of the source of documents. While it was necessary to recognise the possibility of bias in documents, it was also considered important that the documentary evidence reflected the wide range of viewpoints held by stakeholders in the Internet regulation debate. The data obtained via documentary analysis was further supplemented by insights obtained through participant observation in the Council of Europe policy formulation process (see **2.2.2**).

In order to identify relevant documents for analysis, an initial literature search was carried out using a range of online databases and library catalogues. New UK, European Union and Council of Europe official publications were scanned, as were the newspaper press and the professional library and information science literature. The publication of policy documents on the World Wide Web meant that official websites of bodies such as the European Union and the Council of Europe provided a particularly rich source of primary documents. In particular, the Legislative Observatory of the European Parliament[24] that tracks the trajectory of EU policy initiatives through the various consultative and legislative stages was exceptionally useful. This was further supplemented by the Quick Links[25] current awareness service, which provides an email alerting service linking to online access to international coverage of information policy developments, together with a website that offers a helpful thematic gateway to relevant sites.

There is a wide range of organisations with issues relating to Internet censorship at the centre of their mission. Their websites also proved to be extremely useful in monitoring new policy initiatives relating to regulation of Internet access and content[26]. Useful UK sites of this kind included Cyber-Rights & Cyber-Liberties,

[24] <http://wwwdb.europarl.eu.int/dors/oeil/en/default.htm> [Last accessed 5/7/2004]

[25] <http://www.qlinks.net> [last checked 5/7/2004]

[26] The website addresses of these organisations can be found in the bibliography at the end of the thesis.

founded in 1997 by Yaman Akdeniz at the Cyberlaw Research Unit of the University of Leeds, with the purpose of promoting free speech and privacy on the Internet and raising public awareness of such issues; and the Campaign for Internet Freedom, an organisation dedicated to opposing online censorship.

In the US, the Electronic Frontier Foundation (EFF), was founded in 1990 to "protect privacy, free expression, and access to public resources and information on-line, as well as to promote responsibility in new media" (Electronic Frontier Foundation, 1996). The EFF launched the Blue Ribbon Campaign, which encourages websites favouring freedom of expression to carry the blue ribbon motif. The EFF also hosts the site of Computers for Academic Freedom on its server, an organisation maintaining an archive of documents relating to on-line information access in the academic environment.

Other useful US and international sites included those of the Citizens Internet Empowerment Coalition (CIEC); the American Civil Liberties Union (ACLU); the Center for Democracy and Technology, which advocates public policies that promote civil liberties in the networked environment; the Global Internet Liberties Campaign (GILC), an international coalition of organisations campaigning for human rights on the Internet; MIT SAFE, a student organisation originating in the US to fight against on-line censorship; and Peacefire, an organisation that campaigns for the rights of young people under 18 to unfiltered access to the Internet. Clearly, many of these organisations have a US-focus, and they all have very specific value-laden missions as their driving force. Although it was necessary to be aware of the potential bias reflected in their publications they proved to be an important alerting source to new policy initiatives and alternative perspectives on the Internet control debate.

Thus, in addition to monitoring new monograph and journal publications, policy information was obtained from a wide range of online sources. Details of all relevant documents examined were recorded on a database using Endnote[27]

[27] Available from Adept Scientific <http://www.adeptscientific.co.uk>

bibliographic software, and given identifying keywords and a unique accession number to facilitate retrieval of hard copy. These documents were used to provide a chronological 'narrative' of policy updates and trends – the results of this analysis are described in Chapter 3, Policy Context and Policy Monitoring.

2.2.2 Observation as a research method

The monitoring of policy initiatives via the analysis of documentary sources facilitated a comprehensive longitudinal overview of policy developments, and in particular of regulatory and legislative mechanisms. However, it did not permit an in-depth insight into the detailed internal aspects of the public policy formulation process. In this respect, therefore, the opportunity to participate directly in the development of the Council of Europe's *Guidelines for Public Access to and Freedom of Expression in Networked Information* (Sturges, 2000a) was invaluable in contributing towards this dimension of the study. This participation involved responsibility for the monitoring and collation of responses to an electronic consultation on initial draft guidelines. It also involved attendance at an international conference held in Helsinki in 1999 at which the guidelines were presented and debated, with responsibility for collating, summarising and feeding back the range of viewpoints that were expressed. Direct observation of this process, as a 'partial participant' (Harvey and MacDonald, 1993, p.155) offered an illuminative insight into the nature of international policy formulation, and the difficulties presented by the need to reconcile a wide range of vested interests and culturally diverse opinions.

Observation as a method for this part of the study was particularly useful; as Bell (1993) has noted, observation can reveal characteristics of individuals, groups or processes that would be impossible to discover by other means. It should afford an insight into what *actually* happens, rather than society's perception of events and can 'provide data on previously unrecorded aspects of the social world' (Harvey and MacDonald, 1993, p.188). In the current context, the emphasis was very much on the policy *process* and the roles played by the different stakeholders in the process, making observation an appropriate method to adopt.

Nevertheless, observation does have some potential drawbacks. Data is necessarily subject to the researcher's interpretation, both in terms of what data are deemed significant and worthy of recording, and the meaning that is derived from the data. It can be very difficult for the researcher to eliminate his or her own preconceptions, and therefore a systematic and reflexive approach on the part of the researcher is crucial. Unless the observation is covert there is also considerable potential for the 'researcher effect' to influence events and processes.

In the context of both the electronic consultation and participation in the Helsinki Conference, no particular attempts were made to conceal the observation process from other participants. However, with regard to the electronic consultation, participants were not specifically aware of the researcher's involvement in the research process for any purposes other than as intermediary for the Council of Europe in publicising the exercise. Similarly, although many of those attending the Conference were aware of the researcher's interest in observing the outcomes of the debate, they were not specifically made aware of the observation of the policy process itself. There was, therefore, no cause for believing that the presence of the researcher would have had any direct effect on the conduct of the decision-making process.

It is less easy to assume that the researcher was able to eliminate all bias and preconceptions in recording and interpreting the observation data; however, the role of collating the views expressed by participants and presenting these to the author of the *Guidelines* required a very systematic and objective approach. A daily journal was kept in which detailed notes from panel sessions were recorded and this formed the basis of the feedback presented. Considerable efforts were made to ensure that the formal feedback report represented an impartial and comprehensive reporting of all expressed viewpoints.

2.2.3 The Council of Europe consultation process

The process of arriving at the agreed set of guidelines began with the appointment of Prof. Paul Sturges of the Department of Information Science at Loughborough University as Consultant to the Council of Europe's Culture Committee, initially with a brief to prepare a report on *Freedom of Expression and the Communications Networks* (Sturges, 1998a[28]) which was accepted by the Culture Committee at a meeting in Strasbourg in October 1998. The Council of Europe claims a commitment to the promotion of public access to information and freedom of expression as being central to the maintenance of democracy[29]. With the advent of new information technologies, the Council stated a concern to ensure that these technologies would not only pose no risk to the protection of this freedom, but would be harnessed to enhance it. Thus, following acceptance of the report on *Freedom of Expression and the Communications Networks* (Ibid), Sturges was further commissioned to draft recommendations for guidelines on public access and freedom of expression in networked information. It was anticipated that the guidelines would be used by governments and European policy makers, as well as by all providers of local public access to the Internet.

The initial draft of the guidelines was presented to the Council at a meeting of the Culture Committee on 21-23 April 1999[30]. They were also posted on the Council of Europe website for consultation. In order to draw attention to the consultation, the researcher was requested to post an email soliciting responses to the consultation to a range of relevant email lists (details of these lists are provided in Table 4.1 on p.123). However, due to delays on the Council's part in posting the guidelines on their website, and technical problems with the automated response system, the consultation resulted in a very limited response. The guidelines were

[28] <http://www.coe.int/T/E/Cultural_Co-operation/Culture/New_Technologies/N.I.T/Working_strands/Public_access/Sturges98_18.asp> [Last accessed 30/4/2003]

[29] <http://www.coe.int/T/E/Communication_and_Research/Contacts_with_the_public/About_Council_of_Europe/An_overview/Media_and_democracy/default.asp#TopOfPage> [Last accessed 22/7/2003]

[30] The researcher was given an opportunity to comment on an early draft of these guidelines, prior to their presentation to the Culture Committee.

also circulated to relevant bodies of the Council of Europe for discussion. Most importantly, they were presented and discussed at an international conference on "Public Access and Freedom of Expression in Cultural Institutions", attended by a wide range of policy makers, politicians, academics and representatives of professional organisations. The researcher was also invited to attend as an observer, and requested to collate a summary of responses to the guidelines for their author.

The results of this wide-ranging consultation exercise are discussed in Chapter Four of the thesis. The resulting final draft of the *Guidelines* was approved by the Culture Committee in March 2000, and by the Council for Cultural Co-operation in May 2000.

2.3 Case Study Approach

> *…a case study is an exploration of a "bounded system" or a case (or multiple cases) over time, through detailed, in-depth data collection involving multiple sources of information rich in context.*
>
> (Creswell, 1997, p.61)

The term *case study* is commonly used to describe the in-depth investigation of a particular case, whose uniqueness warrants study (an *intrinsic* case study), or of a particular issue, the case being used as a means of illustrating particular aspects of the issue (an *instrumental* case study). The latter would be a more accurate description of the case study approach adopted for the investigation under discussion. A case study is bounded by time and by place, and is considered within its contextual setting. Yin (1994, p.13) describes a case study as an empirical enquiry that

- *Investigates a contemporary phenomenon within its real-life context, especially when*
- *the boundaries between phenomenon and context are not clearly evident.*

Since the investigation of the case is likely to involve a variety of different research methods, such as interviewing, documentary analysis, and observation, it

can more accurately be considered as a research *approach, strategy* or *tradition*, rather than as a research method. Yin (op cit) identifies three broad categories of case study research design: exploratory, descriptive and explanatory, the specific category for any particular study being determined by the theoretical perspective of the research question. For the study in question, an exploratory approach was deemed most appropriate in the context of the research question. A case study may involve a single case or multiple cases (a collective case study, as in this particular research project). The data collection and analysis is usually qualitative in nature.

In deciding whether to use the strategy of case study research to investigate a particular phenomenon, Creswell (1997) notes that it is an appropriate strategy for studying a case with clearly identified boundaries, where there is abundant contextual material available, and a wide range of information sources to provide an in-depth picture of the phenomenon under investigation. He considers the rationale for using the case study approach thus:

> *For a case study, the researcher should focus on an event, process or program for which we have no in-depth perspective on this "case". Conducting the case study provides a picture to help inform our practice or to see unexplored details of the case.*
>
> (Ibid, p.95)

Denscombe (1997) considers the case study to be the most suitable approach when the aim is to focus on a particular instance of the question to be investigated, and the approach should provide the means to "illuminate the general by looking at the particular". It is an appropriate approach when the researcher wishes to focus on relationships between forces, and the processes involved in shaping phenomena. It should enable the researcher to determine how the different forces affect one another, and to explain why certain outcomes may happen, through investigation of issues in their natural setting (Ibid). In the current context, the researcher aimed to explore the forces impacting on policy formulation within the chosen sites, and therefore the case study approach was considered to offer significant advantages and relevance.

Hamel (1993) considers that the case study approach allows for a more inductive approach affording a search for the meanings inherent in a phenomenon. It is also more appropriate when one wishes to incorporate the actor's point of view on an issue, rather than taking a more detached stance (Ibid). Again, both these factors were considered important in the context of this study.

Consideration of the nature of the research question should be paramount in determining whether to adopt the case study approach, the use of case studies being most suited to the investigation of *'how?'* and *'why?'* questions (Yin, 1994). It is also the ideal strategy when the researcher lacks control over actual behavioural events, and where the focus is on contemporary or historical phenomena. Yin notes that the use of the case study approach 'allows an investigation to retain the holistic and meaningful characteristics of real-life events' (Ibid, p 3) and that it is 'the method of choice when the phenomenon under study is not readily distinguishable from its context' (Yin, 1993, p 1).

Schramm supports the use of case studies for exploring decision-making processes commenting that

> *The essence of a case study, the central tendency among all types of case study, is that it tries to illuminate a decision or set of decisions: why they were taken, how they were implemented, and with what result.*
>
> (Schramm, 1971, cited in Yin, 1994)

According to Yin (Ibid), in a policy study context, the case study approach should be considered when the research aims to:

- Explain causal links in real-life interventions;
- Describe an intervention and the real-life context in which it occurred;
- Illustrate topics within a policy evaluation;
- Explore situations in which the intervention being evaluated has no clear, single set of outcomes;

- Conduct a meta-evaluation.

The advantages of selecting the use of case studies as a research approach include the ability such an approach offers to deal with the subtleties of complex social situations and relationship processes; the integration of a variety of research methods and use of multiple data sources, thus allowing for a high level of triangulation; the lack of pressure to impose controls on the investigation of naturally occurring phenomena; and its suitability for theory-building and theory-testing (Denscombe, 1998). These factors were all considered important to the current study.

However, concerns have been expressed with regard to the desirability of the case study approach. Yin (1994) has noted concerns relating to a potential lack of rigour, due to the difficulties of overcoming bias and of reporting evidence fairly and objectively; the low level of the basis for scientific generalisation of results; and the long time-scale needed to conduct the research, which can result in unmanageable amounts of amassed data. Denscombe (1998) also questions the credibility of generalisations arising from case study research, which is often perceived as producing 'soft' data. He notes the difficulties in defining boundaries to the object of study, in negotiating access and maintaining confidentiality, and in avoiding distorted results due to the 'observer effect'.

It was recognised here from an early stage that the results from the limited number of case study sites could not offer a high degree of generalisability. However, it was anticipated that the insights obtained from the individual case study sites would be useful in terms of illuminating specific aspects of the policy formulation *process* within the institutions concerned. By concentrating on policy formulation with regard to a single specific issue (the regulation of access to Internet content) it was possible to define the boundaries of the study with a reasonable degree of clarity.

All interviewees were assured that their comments would be reported anonymously, and that the identity of the institutions under investigation would

not be generally disclosed. Although it is indeed hard to ensure that results are not distorted as a result of the 'interview effect' the researcher was impressed by the apparent frankness and openness with which interviewees responded to her questions. The use of a semi-structured question framework with open questions was intended to ensure that the 'voice' of interviewees was heard, without undue leading from the researcher. The verbatim transcription of interviews ensured that the data was recorded in an unbiased and accurate fashion.

It is important to ensure that every case serves a specific purpose within the overall research study (Yin, 1994), and is genuinely worthy of study (Creswell, 1997). In deciding on which cases to select for study, Denscombe (1998) stresses the importance of ensuring that the selection of individual cases is suitable for the research purpose. The researcher should have a clear idea of what the case is intended to explain, before selecting a specific case for study. Creswell (1997) suggests that a case should be selected on the basis of its ability to demonstrate different perspectives on a problem, process or event; on its accessibility; and by the extent to which it represents either a very ordinary example of a phenomenon, or a particularly unusual example of the same phenomenon. In the context of the current study, apart from the issue of access, the sites were chosen on the basis that they would offer a range of types of institution at different stages of maturity. It was hoped that this would enable comparison of a variety of policy formulation models.

With reference to data collection, a variety of research methods are appropriate for case study research, including interviewing (in person or by telephone, on a one-to-one basis or via focus groups), observation (including, where appropriate, participant observation), documentary analysis and questionnaire surveys. Whatever methods are chosen, it is to be expected that most case study research will involve a range of different data sources, chosen for their anticipated relevance to the research question. For this study, the methods chosen involved a combination of face-to-face semi-structured interviews, non-participant observation and documentary analysis. The data obtained was further

supplemented with the findings from a questionnaire survey conducted with a selected group of undergraduate students at each of the case study sites (see **2.4**).

Prior to the commencement of data collection a case study protocol was prepared (Appendix One) which provided an overview of the project covering details of the research questions to be investigated, proposed field procedures and ethical issues such as confidentiality and anonymity. In addition to assisting the researcher in compiling question frameworks and guiding data collection, this protocol was used to provide information about the study for those responsible for granting access to the case study sites. It was also circulated in advance of interviews to respondents to provide them with information concerning the nature and purpose of the study. The first case study site (Institution A) was initially regarded as a pilot site for testing the research instruments, but as these were found to require no further modification, data from this site was regarded as reliable and is included in the discussion of the findings of the case studies.

A matrix detailing interviews carried out and documents obtained at each site was completed (Appendices Two and Three). In addition, a journal recording field notes, observations and reflections was maintained. Interviewees were selected according to their role in the institution, as detailed in the case study protocol. Efforts were made to ensure that a similar sample of personnel was interviewed at each institution, although roles were not always exactly matched. Some use was made of the 'snowballing' technique in identifying the most relevant personnel for interview, as the organisational structure and allocation of responsibilities did vary for each institution.

The question framework, although based on the research questions identified in the case study protocol, was modified somewhat for each interview according to the role of the interviewee. Thus, for example, systems personnel were questioned in greater depth on the technical aspects of network regulation, whereas academic staff were asked more questions about their day-to-day use of the network and what effects institutional policies appeared to exert on this. Interviews were recorded and transcribed. In two instances, the interviewees requested a copy of

the question framework in advance. In another instance, the recording failed; this experience showed the value of making a simultaneous hand-written record of responses alongside tape recording. In this instance, the answers were written up shortly after the interview had taken place to ensure maximum recall, and the transcript submitted to the interviewee to check whether it represented a true recording of his responses.

Data from the case studies were analysed on both a within-case and cross-case basis. Specific themes emerging from the data relevant to the research questions were identified in order to obtain a picture of the policy formulation process at each institution, and of the impact of policy decisions on freedom of enquiry. Alternative perspectives of control and freedom of information, different policy formulation models and differing governance structures at each of the institutions were considered in the final analysis. These results are described in Chapter Five of the thesis and their implications discussed in Chapter Seven.

2.4 Questionnaire survey

The third component of the research project was intended to supplement and triangulate the data obtained from the case studies by allowing the voice of students at each of the institutions to be heard. The methods used in the case study approach had thus far provided a substantial insight into the policy formulation process and the impact of policy measures on academic and support personnel at each case study site. However, it was less clear what effect policy measures were having on the student experience. Interviews with a very small number of students were not seen as being a reliable method of gaining an insight into the student experience and it would not have been practical to conduct large numbers of student interviews. Thus it was decided to use a questionnaire to explore the use of university computer networks and the opinions of a wider group of students at each site than would have been possible from personal interview. Even so, the numbers of respondents at each site were not considered to be sufficient to allow for a high degree of generalisation to the student body in total. The purpose of the survey was therefore limited primarily to determining whether the implementation

and promotion of Computer Use regulations and policies could be seen to have any discernible impact on the targeted group of students' use, and misuse, of university computer network facilities, including their freedom of enquiry and freedom of access to information.

Harvey and MacDonald (1993, p.100) suggest that a common feature of questionnaires as a research strategy is that they 'all involve asking people questions and summarising the answers in quantitative terms'. It is appropriate as a strategy for measuring and recording empirical data (Denscombe, 1998) and can be useful as a means of comparing and relating data, but is less suited to proving causal relationships. This can lead to a tendency towards empiricism whilst neglecting the implications of the findings. It does have the advantage of being a relatively cost-effective and quick strategy, offering wide and inclusive data collection, although the results tend to favour breadth rather than depth (Ibid). The accuracy of the results are dependent on the degree of honesty with which informants respond, and, unless the survey is repeated over time, it offers a "frozen image" (Harvey and Macdonald, 1993, p.136) that does not provide a longitudinal insight into the phenomenon under investigation.

In the current context it was hoped only to be able to get a "snapshot" of what was happening with regard to students' awareness of policy measures in place at their university, the effects of such measures on their computer use and their attitudes towards these measures. Thus it was felt that, despite the disadvantages outlined above, the survey method would be a reliable and valid strategy for data collection. The quantitative nature of the data obtained would be supplemented by the qualitative data obtained from the case study approach. It was not considered relevant or appropriate to take a longitudinal approach to this area of data collection. With regard to honesty, it was felt that the anonymous nature of the data collection and the creation of a 'safe' environment (Belson, 1986, p.19) would encourage honesty and openness in responding to what were, in some cases, relatively sensitive and personal questions.

A copy of the questionnaire is provided as Appendix Four. The questionnaire design was based on a significantly modified version of that used by Prior (2001) in her study into the decision-making process involved in the introduction of CCTV into a university environment. The specific questions to be asked were based on the original research questions, which were further broken down into dimensions with a number of variables. Thus questions related to:

- The purposes and nature of usage of university network facilities (Q.1, 5, 6);
- Awareness of university policies and regulations relating to computer use (Q.2);
- Awareness of blocking or filtering of website access (Q.3);
- Awareness of monitoring of website access or email usage (Q.4);
- Experience of offence as a result of other users' computer usage (Q.7).

In addition, a simple Likert scale was used to explore students' attitudes to:

- Monitoring of web access and email usage (Q.8, 10);
- Blocking of access to offensive content (Q.9);
- The protection of their privacy whilst online (Q.11);
- The ability of students to bypass measures to control their network use (Q.13);
- The extent to which they felt they have a right to be informed or consulted about measures taken by the university to control or monitor their network use (Q.14).

In order to challenge their thinking about the issues involved, they were also asked about what their expectations of their rights would be if they were in charge of university computing facilities. The Likert scale was used to rate their agreement with a range of statements relating to whether, in such circumstances, they would expect to have the right to:

- Block access to offensive (but legal) content (Q.14);
- Block access to illegal content (Q.15);

- Monitor email content (Q.16).

The final question using the Likert scale (Q.17) concerned their attitudes towards the rights of government to monitor email and web use, in the interests of national defence and security. This question was felt to be important in the context of the monitoring of policy measures at macro level, particularly as the fieldwork was carried out at the time that legislative measures such as the *Regulation of Investigatory Powers Act 2000* (Parliament, 2000a)[31] and the *Anti-Terrorism, Crime and Security Act 2001* (Parliament, 2001)[32] were receiving considerable media attention.

Finally, the respondents were given the opportunity to add any further comments that they wished to make by the use of an open question (Q.18). They were also asked to provide information on their course, which year of their course they were in, their gender, and their age bracket. These last variables were used only as a means of verifying the character and inter-institutional comparability of the student groups.

It was anticipated that the choice of closed questions, and the use of a well-tested scale such as the Likert Scale, would enhance the reliability of the data collection and analysis, whilst validity would be achieved by defining the questions through reference to the theoretical constructs of the overall research questions. Efforts were made to ensure that the questions followed a logical sequence, and in particular, that the more difficult, sensitive or personal questions came later in the sequence. Other principles guiding the framing of questions were that they should make sense to respondents; they should avoid the use of jargon; they should be unambiguous; they should be short and clear; and leading questions should be avoided.

[31] <http://www.legislation.hmso.gov.uk/acts/acts2000/20000023.htm> [Last accessed 5/7/2004]

[32] <http://www.hmso.gov.uk/acts/acts2001/20010024.htm> [Last accessed 5/7/2004]

Because of the sensitive nature of some of the questions, and in order to assess content validity, the questionnaire was submitted for review by the Research Supervisor and Research Director of the project to ensure that it was considered to be ethically acceptable as well as valid in its approach. This led to one or two minor alterations. It was then piloted with a small number of students prior to full administration. The data obtained from these pilot surveys was not included in the formal data collection, and again, the piloting led to minor amendments to overcome some ambiguities in the wording of questions.

It was decided that it would be preferable to administer the questionnaire in a controlled environment and the start of formal student tuition sessions were identified as suitable for this. This was intended partly to ensure a good response rate, but given the nature of the specific questions it also gave an opportunity to ensure that respondents understood the confidential and anonymous nature of the exercise. Administration of the questionnaire by the researcher herself, rather than by their tutors, was considered essential to emphasise distance from university officialdom and thereby to promote honesty on the part of student respondents. The need to gain access to students during class contact time meant that sampling was based on the use of 'random cluster samples' (Harvey and MacDonald, p.118). No attempts were made to control for variables such as gender. Whilst this approach could not be considered sufficiently rigorous to allow for generalisation to the whole student population, this was not the intention of the survey and therefore this sampling method was considered acceptable in the specific context.

In order to analyse the data a coding frame was designed (Appendix Five), and the SPSS software package was used to record the variables for each respondent and to conduct the subsequent data analysis. Since the intention was only to provide a descriptive outline of students' awareness of policies relating to computer use, their actual use of network facilities and their attitudes to regulation of this use, the statistical analysis was kept simple. Thus frequency tables and percentages were calculated for each question, but correlations between variables were not generally explored.

2.5 Scope of the research

Limitations to the scope of the research have already been highlighted, and the rationale behind such limitations discussed, so they will only be summarised here. Thus, with regard to the policy monitoring, the scope was limited in respect of

- Chronological period – this was limited to the period between 1998 and 2003, although some limited reference to earlier policy measures is made in order to contextualise subsequent developments;
- Geographical and political coverage – this was limited to policy formulation within the UK, the Council of Europe and at European Union level;
- Content – despite the potential impact on freedom of access to information and freedom of expression on the Internet of other measures such as data protection legislation, the monitoring focused on policy specifically aimed at controlling access to illegal, offensive or harmful Internet content.

With regard to the academic case studies, these were limited to three Higher Education Institutions. It is recognised that this does not allow for generalisation of the results of the study across the UK higher education sector. However, it was not the intention of the researcher to obtain generalisable data. Instead, it was hoped to gain an insight into policy formulation processes in order to enhance the understanding of the theoretical basis of decision-making and the impact of policy measures at each institution, at a specific point in time. This is equally true of the data obtained through the questionnaire survey, which was used to obtain a "snapshot" of students' use of computer networks and their attitudes towards regulatory measures.

2.6 Ethical considerations of the research strategy

With regard to the longitudinal monitoring of policy initiatives at UK, EU and Council of Europe levels that was conducted through documentary analysis, no ethical issues were identified; all sources used were publicly available for

consultation. Similarly, it was not considered that there were significant ethical issues attached to the researcher's involvement in the Council of Europe policy formulation process.

However, with regard to the institutional case studies and the involvement of student respondents in the questionnaire survey, there were significant issues of confidentiality and anonymity to be considered. At institutional level, a concern on the part of university administrators not to risk their institutions being portrayed in a negative light meant that assurances of institutional anonymity had to be given. Similarly, at the level of individual respondents, guarantees that their contributions would not be openly attributed were a necessary requirement in order to ensure their openness with the researcher. The same was true of student respondents to the questionnaire survey: in many cases they were, in effect, acknowledging their involvement in illegal activities and their confidence in the confidentiality and anonymity of their responses was crucial.

2.7 Conclusion

This chapter has discussed the different methods used in the overall research strategy that was adopted. In particular, it has aimed to present the rationale for the use of these methods, and to consider their appropriateness with reference to the extensive methodological literature available. It has also aimed to make explicit the linkage between the different components of the overall study. Limitations in the scope of the research have been identified and specific ethical issues attached to carrying out the research have been discussed. Chapter Seven will include discussion of the appropriateness of the research strategy in practice, and will consider any ways identified in the course of the research in which it was felt that the research strategy could have been improved.

The next three chapters will present the findings of the different elements of the research, the implications of which will then be discussed in Chapter Seven.

CHAPTER THREE: POLICY CONTEXT AND POLICY PROCESS – THE EUROPEAN UNION AND THE UNITED KINGDOM

> *The Internet has already thrown up a host of legal and political conundrums, but these are only a small foretaste of the dilemmas – about privacy, security, intellectual property and the nature of government itself – that will have to be faced over the coming decades.*
>
> (Manasian, 2003)

3.1 Introduction

This chapter presents the findings of the longitudinal policy monitoring at European Union (EU) and UK national levels, focussing on the debate about what governments, regulators or societies in general should 'do' about Internet content (Newey, 1999). The investigation was guided by the 'distributive perspective', with a concern on the part of the researcher to identify and uncover policy developments that constrain access to information on the Internet, and that have an inhibitory effect on the ability to express oneself freely online in accordance with one's own beliefs and values.

Discussion of EU policy initiatives has been placed before that of UK measures, as much of the policy and legislation in this context in the UK has been influenced by, or derived directly from, that developed at EU level. The chapter includes an initial discussion of the scope and definition of information policy in general, before considering the relevance of information policy specifically as it applies to the Internet. The findings of the policy monitoring with regard to Council of Europe initiatives will be presented in the next Chapter.

Discussion of the implications of the findings of the policy monitoring and analysis at all levels will follow in Chapter Seven of the thesis, in the context of the policy process models introduced previously.

3.2 Information policy – some definitional dilemmas

> *Information policy is the set of all public laws, regulations and policies that encourage, discourage or regulate the creation, use, storage and communication of information.*
>
> (Weingarten, 1989)

'Information Policy' itself is a concept that suffers from a lack of any common, accepted definition (Browne, 1997a). Although the above definition encompasses all aspects of information policy in the broadest sense, it is particularly useful to the current study on account of its emphasis on regulation of the use and communication of information. Burger defines information policy in even wider terms as those 'societal mechanisms used to control information, and the societal effects of applying those mechanisms' (Burger, 1993). Thus recognition is given to the two-way policy process: policy is not only embedded in, and influenced by, the social, political and cultural environment in which it is formulated, but it also acts to modify that environment. This bi-directional effect is particularly evident with respect to the Internet, as noted by Slevin: the Internet both affects, and is affected by, government regulation (Slevin, 2000).

Moore identifies a value-driven goal of information policy as comprising 'the development of a legislative and regulatory framework within which the use and exchange of information is encouraged, while protecting intellectual property and other rights', thus achieving a balance between the rights and responsibilities of individuals and institutions (Moore, 1993, p.284). He also notes the importance of formulating policies capable of accommodating the changing requirements of rapidly developing Information and Communication Technologies (ICT).

Overman and Cahill (1990) distinguish between two competing perspectives in information policy, those that are primarily restrictive in purpose (for example, policies protecting security and ownership of information), and those that are distributive in intent (thus, for example, freedom of information and expression). They cite the value of privacy as potentially belonging to either perspective, depending on context: thus policies that protect the privacy of an individual to

access information without surveillance would be distributive in effect, whereas those aimed at protecting the privacy of personal data would be restrictive. The tensions inherent as a result of these competing normative and moral assumptions that underpin practices in the sphere of information management lead to what Overman and Cahill (Ibid) describe as a 'policy impossibility'.

3.3 Information policy and the Internet

> *The Internet interprets censorship as damage, and routes around it.* [33]

Although many national governments, and indeed supranational organisations, were initially slow to understand the relevance of the development of the Internet to the public policy arena, there has more recently been a widespread enthusiasm for implementing measures that encourage or constrain the growth of Internet use within their jurisdictions. Lan and Falcone (1997) provide a compelling argument justifying the formulation of national policies on Internet access. Their argument is as follows: if it is true that 'information is power'[34] then complete access to all information by all people would ensure the equalization of the distribution of power. The Internet is a mechanism that could theoretically provide access to all information by all people.

However, governments do not always see universal access to perfect information as being in their own best interests. Indeed, the early history of the Internet has shown its potential as an instrument of subversion and resistance. An example of the democratising powers of communications technologies that are not easily

[33] This quotation has been attributed to John Gilmore (Electronic Frontier Foundation). [Gilmore states: "I have never found where I first said this. But everyone believes it was me, as do I." Also in New York Times 1/15/1996, quoted in CACM **39**(7):13. From <http://cyber.law.harvard.edu/people/reagle/inet-quotations-19990709.html>, accessed 5/7/2004]

[34] Adapted from Francis Bacon 'Nam et ipsa scientia potestas est' [Knowledge itself is power] *Religious Meditations of Heresis.n.d*
.

subject to authoritarian control can be found in the dissolution of the former Soviet Union, as described by McGowan (1991) who suggests that 'Telecommunications played as much of a role as pickaxes and shovels in bringing down the Berlin Wall and the barbed wire of the Iron Curtain'. There are many examples of the use of the Internet to effect the 'globalisation of opposition' (Vidal, 2000) and resistance to authoritarian or unpopular regimes. Examples of such use have been offered by, among many others, Castells (1997); Sussman (1997); Barkham (1998); Hill and Hughes (1998); and Vidal (op. cit.).

Nevertheless, attempts by governments to censor Internet content are bound to encounter difficulties, not least as a result of the architecture of the technology itself. Designed originally to withstand attack, it could be suggested that the Internet is inherently resistant to conventional forms of governance. Globalisation of the Internet also brings with it problems arising from differing cultural, legal and social norms. Despite this, the Internet in itself is not a democracy, and even in cyberspace it could be argued that power does not reside with those who seek access to information but rather with those who determine what information will be available and who will have access to it. An alternative perspective resulting from the 'knowledge is power' observation was offered by Line in his 1990 Library Association presidential address in commenting 'That knowledge is power has been recognised as a commonplace since Bacon uttered it. Control over who has knowledge and how much is available is perhaps an even greater source of power than knowledge itself' (cited in Curry, 1997, pp.204-205). A similar argument has been put forward by Sturges (1998) who suggests a reversal of Bacon's dictum to reflect a reality where 'Power is information', as it is power that defines and delimits information, that governs its availability and that determines its effects.

Thus, despite the inherent difficulties of 'censoring' the Internet, attempts by governments and other bodies to impose regulatory authority on the Internet mean that it cannot accurately be described as the 'lawless zone' that many of the original pioneers envisaged it to be (Reidenberg, 1996; Valauskas, 1996; O'Toole, 1998; Henley, 2000; Campbell and Machet, 1999; Walker, Wall and Akdeniz,

2000). This is partly because, although implementation may be fraught with difficulties, cyberspace is not exempt from the existing 'terrestrial' laws operating in a particular jurisdiction. The norms promoted by the early Internet pioneers that led to a 'code of practice' for cyberspace[35] also gave rise to the Internet being described as 'one of the most self-regulated and self-protected places in the world' (Valauskas, 1996).

In addition, a number of amendments to existing legislation to accommodate the changed electronic environment, as well as new policy and legislative initiatives specifically aimed at the regulation of cyberspace at both national and international levels, have been adopted in attempts to increase the accountability and control of Internet use. The relative lack of Internet connectivity in the Arab States region is given by Lan and Falcone (1997) as an example of the deliberate control that can be exercised to prevent access to information. This kind of control not only has a constraining effect on individual freedom, but also risks hindering the development of the Internet and the ability of Nation States to derive economic and social benefits through the development of e-commerce (Wall, 2000). Economic constraints and lack of network infrastructure have already created a 'digital divide' that denies Internet access to a substantial proportion of the world's population[36] and that 'allows a partial commodification of political debate by the relatively rich and powerful' (Walker, 2000, p.146).

3.4 European Union policy development towards the Internet

The following sections describe the outcomes of the monitoring exercise analysing the common characteristics of policy initiatives towards Internet regulation that have prevailed within the EU policy-making arena. The results of a retrospective

[35] These 'virtual rules of conduct' have been outlined as: 1. Do nothing that would in any way harm the Internet functionally; 2. Take care in communicating with others over the Internet (observe 'netiquette'); 3. Respect bandwidth. *Cited in* Valauskas (1996).

[36] In 2000, 93% of the world's population had no online access (Castells, 2001, p.261).

policy study covering the years 1996-1998 inclusive will be presented initially in order to set the context for the analysis of subsequent policy development. It should be noted that the scope of the study does not allow for a comprehensive analysis of the institutional structure and organisation of the various consultative and decision-making organs of the EU[37], but concentrates rather on the impact of factors seen to be having a direct impact in shaping policy towards the regulation of Internet access and content.

A wide range of social and political concerns with consequences for individual Internet content and access, including data protection, privacy, data retention and surveillance, have also received much policy attention within the EU and beyond, and these are discussed briefly. However, despite the obvious relevance of such measures to freedom of expression and freedom of access to information, the emphasis of this analysis was on policy measures that have an explicit objective of controlling Internet content and access.

3.4.1 The beginnings of the EU debate on Internet content

During the early 1990s the EU focussed much of its ICT policy on the competitiveness of European information technology products and the creation of the 'Information Society', albeit with a recognition that

> *The notion of a European Information Society comes closer than the information superhighway metaphor in reflecting the Commission's belief that the political and social consequences of using modern ICTs go far beyond just economic or technological reforms. These innovations are changing societies as a whole…the way in which we live, learn and work.*
>
> (Bangemann, 1995)

[37] However, an abundance of useful information on the EU institutions can be found on the EU website <http://europa.eu.int> [Last accessed 5/7/2004], or in publications such as Bainbridge (1995) and Borchardt (2000).

The concept of a 'European Information Society', with its emphasis on the market, economic growth and the liberalisation of the telecommunications sector, firmly established the context of subsequent initiatives with regard to the Internet. Although there was an acknowledgement of the importance of the potential political and social impact of the new technologies, much of the emphasis of early EU information policy had been heavily biased towards funding Research and Development activity to enhance competitiveness, and to address high unemployment, rather than on fundamental policy-making (Mahon, 1997; Dearnley and Feather, 2001).

The EU was much slower to address issues of Internet content than was the US, and the debate in Europe has been more fragmented than it has in the US (Charlesworth, 2000a). This is in part a result of the cultural and linguistic diversity of Member States, and in part through the lack of an overriding First Amendment protecting freedom of speech. The slower initial penetration of the Internet in Europe was another cause of the relatively late entrance of the EU into the content regulation forum (Campbell and Machet, 1999). However, this may also have been driven by a common-sense intention to approach the issue with due thought and consideration: a Commission communication of 1996 argued that 'Over-hasty legislation should be avoided until it is clear where and what type of intervention is required' (European Commission, 1996a, cited in Campbell and Machet, 1999).

In addition to this initial caution on the part of the Commission, individual Member States have also tended to delay implementing legislation in accordance with EU policy relating to Internet regulation. According to Charlesworth (Ibid) this can be attributed to:

- Resistance from entrenched commercial interest groups to perceived threats to their existing rights;
- The fear of national governments of losing their autonomy to control online activities;

- A lack of understanding of the technical workings of the Internet and its implications for societal norms on the part of legislators;
- The rapid pace of technological development, of which national governments and legislators have been unable to keep abreast.

The principle of subsidiarity[38] has traditionally favoured leaving the regulation of broadcasting and other mass media largely in the hands of national authorities (Cincera, 1999). However, the advent of new technologies, increased technical and economic convergence, the increasingly 'trans-frontier' reach of media such as the Internet and cable and satellite broadcasting, together with the widening scope of the EU project beyond the creation of a 'common market' – for instance, the ambition to 'promote cultural policies, and to stimulate the creation of consensus between European cultures' (Ibid, p.75) – have all led to a greater level of EU intervention in the media arena. In particular, Pillar Three of the Maastricht Treaty (European Commission, 1992), allowing for co-operation in the field of justice and home affairs, provides a basis for the Commission's involvement in co-ordinating the efforts of national law enforcement agencies with regard to illegal content on the Internet (Campbell and Machet, 1999, p.145; Akdeniz and Walker, 2000, pp.345-6).

And so by the mid 1990s the EU had started to express interest in the control of 'harmful' and illegal Internet content, particularly with a view to protecting the interests of minors. The debate was initiated by the Commission in 1996, with the Commission's *Communication Paper on Illegal and Harmful Content on the Internet* (European Commission, 1996b), which set the scene for the subsequent *Action Plan* (European Commission, 1997a). The *Communication Paper* proposed that the solution to controlling access to illegal and harmful content lay in

[38] This stipulates that for areas of joint competence the EU should only take action where the scale or effects of a particular policy area makes action at the EU level more effective than individual action by Member States.

> *…a combination of self-control of the service providers, new technical solutions such as rating systems and filtering software, awareness actions for parents and teachers, information on risks and possibilities to limit these risks.*
>
> (European Commission, 1996b)

This initial debate identified several key themes that have continued to characterise the approach of the EU to the issue, namely that self-regulation would play a central role in content control; that, given the diversity of the Member States, 'illegal content' would be easier to categorise than 'harmful content'; that, to be effective, any system of Internet content regulation would have to be global; and that responsibility for content should rest with producers and distributors, and not with intermediaries such as ISPs (Charlesworth, 2000, pp.59-60). It does have to be noted, however, that the latter principle has not been without subsequent challenge in some Member States[39].

In April 1997 the European Parliament adopted a Resolution on the Commission Communication that supported the initiatives undertaken by the Commission and stressed the need for international co-operation to be initiated and co-ordinated by the Commission. In particular, it called on the Commission to propose, after consultation with the Parliament, a common framework for self-regulation at EU level. The framework was to include

1. Objectives in terms of the protection of minors and human dignity;
2. Principles governing the representation of the industries concerned and the decision-making procedures;
3. Measures to encourage private enterprise to develop message protection and filtering software;

[39] As for example in the 1998 case in Germany of Compu-Serve Chief Executive Felix Somm (see Traynor, 1998) and the UK court case between Demon Internet Ltd and Godfrey (see Chapter Three, p.92-).

4. Appropriate measures for ensuring that all instances of child pornography uncovered on computer networks are reported to the police and shared with Europol and Interpol.

The Resolution also calls on the Commission and the Member States to encourage the development of a common international rating system compatible with the PICS (Platform for Internet Content Selection) protocol, and sufficiently flexible to accommodate cultural differences. In addition, it calls upon the Commission to submit proposals for a common regulation of liability for Internet content (European Commission, 1997b).

3.4.2 Green Paper on the Protection of Minors and Human Dignity

In October 1996, at much the same time as the Commission Communication was being debated, a *Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services* (European Commission, 1996c) was adopted by the Commission. The *Green Paper* was intended to 'stimulate public debate in order to identify the main problems posed by new information services and to identify measures needed' (European Commission, 1997b). The *Green Paper* culminated in a *Proposal for a Council Recommendation* (European Commission, 1997c), which stated that the role of the EU is to 'improve the effectiveness of national measures by ensuring a minimum level of coherence in the development of national self-regulatory frameworks and by encouraging co-operation at European level' (Campbell and Machet, 1999, p.151). The Council adopted the *Recommendation* in May 1998.

With regard to Internet content the *Green Paper* (and subsequent *Recommendation*) requested ISPs to develop codes of conduct so as to better apply and clarify current legislation. It also offered guidelines for the development of national self-regulation regarding the protection of minors and human dignity, based on three key elements:

- The involvement of *all* interested parties (Government, industry, service and access providers, and user associations) in the production of codes of conduct;
- The implementation of codes of conduct by the industry;
- The evaluation of measures taken.

Broad recognition was given to the role of the EU in co-ordinating the development of national self-regulation, and of the commitment of the EU towards ensuring that measures taken are consistent with observance of Articles 8 and 10 of the European Convention on Human Rights[40] (Council of Europe, 1950). Particular emphasis was placed on measures that support parental control and the promotion of access to high quality content, including the further development of technology-supported measures such as content rating and filtering systems.

A particularly interesting response to the consultation on the *Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services* (European Commission, 1996c) and on the earlier *Communication on Illegal and harmful content* (European Commission, 1996b) was made by the European Commission Legal Advisory Board in early 1997 (European Commission Legal and Advisory Board, 1997). This endorsed a number of important principles set out in the documents, and raised some additional points for consideration. Among those that it emphasised were:

- Existing general rules such as laws intended to protect minors and human dignity should apply equally to all media – the Internet is not a "sphere apart" subject only to self-regulation and exempt from national law;
- The Internet is 'a positive instrument, empowering citizens and educators, lowering the barriers to the creation and distribution of content and offering universal access to ever richer sources of digital information' – thus any action taken to deal with 'atypical' use should not have a disproportionate impact on Internet users and the industry as a whole;

[40] Relating to the rights of privacy and of freedom of expression (see Chapter Four, pp.108-110).

- Responsibility for prosecuting and punishing those responsible for illegal content remains with national law-enforcement agencies;
- The potential empowerment of users through increased transparency of government and availability of public sector information should be at the forefront of the debate;
- ISPs are responsible for their own content that they make available for use, but they are not responsible for third party content to which they merely provide access for use, unless they can 'reasonably be said to have had knowledge about its possibly illegal or harmful content and blocking its use is both technically possible and can be reasonably expected';
- Information on the Internet should be allowed the same free circulation as paper-based information. The requirements of Article 10 of the European Convention on Human Rights (Council of Europe, 1950) should guide decisions on the proportionality of any measures restricting freedom of expression and any regulatory approach to control harmful content should abide by the terms of Article;
- It is important to recognise the distinction made in the *Green Paper* between measures to control content defined as illegal by national legislation, and that which is regarded as possibly harmful;
- Anonymous communication is part of the basic right of freedom of communication and necessary to protect an open political process – effective technical means to protect this right on the Internet should be ensured;
- Where content rating is used, the criteria and procedures for rating content should remain transparent. With regard to filtering services, information access providers should make their use of such devices transparent to their clients; they should not oblige their users to use a particular filtering service, and they should respect the right to privacy;
- ISPs and Internet access providers should make software available that allows parental control, and should make information about the software available to parents and teachers.

(European Commission Legal Advisory Board, 1997)

The paper concludes with a further two 'guiding principles' that the Legal Advisory Board felt should underpin the debate. Firstly, that the focus should be on practical co-operation rather than on attempts to find a new specific legislative solution for the Internet. Secondly that, although consensus in the broader international context is desirable, international discussions should bear in mind that 'an issue is being discussed which although having obvious economic implications is mainly an issue of the effectiveness of human rights, cultural values and balances between state authority and citizens' rights' (European Commission Legal Advisory Board, 1997). This response thus gives much stronger emphasis and support for the values of freedom of expression and freedom of information than the does the original Commission document, as well as a clear endorsement of the liberating and democratising potential of the Internet.

In July 2001 the Council of the EU adopted the conclusions of an evaluation report produced by the Commission on the application of the *Green Paper*'s recommendations (European Commission, 2001). An overwhelming endorsement of the report by Members of the European Parliament (MEPs) in April 2002, with 460 votes in favour of the Commission's approach, 3 abstentions and no votes against, followed this. In particular, the Parliament endorsed the principle that children's welfare is primarily the responsibility of their legal guardians. The adoption of a self-regulatory approach rather than the use of blocking technologies was also strongly commended (European Parliament, 2002), although there was little evidence otherwise of the impact of the Legal Advisory Board's response.

A further evaluation report, analysing the effectiveness of measures of the *Recommendation* that have been implemented in Member States and at EU level since 2000, was adopted by the European Commission in December 2003 (European Commission, 2003a). At the same time, it was announced by the European Commissioner in charge of Education, Culture and Audiovisual Services that the Commission intends to follow up the evaluation report by proposing an update of the *Recommendation* during the first quarter of 2004. In particular, the update would concentrate on the right to reply; media literacy; the harmonisation

of ratings descriptors; and measures against discrimination and incitement to hatred on the grounds of race, sex or nationality in online media (Ibid).

3.4.3 Action Plan on Promoting Safe Use of the Internet

Meantime, a parallel initiative was also being developed by the Commission. The four-year *Action plan on promoting safe use of the Internet* (European Commission, 1997a) was originally intended to cover the period 1998-2001 inclusive, and was adopted in November 1997 with a budget of 25 million Euro. The *Action Plan* was intended to be complementary to the *Recommendation*, and was shaped by the same underlying principles based on a self-regulatory approach. However, whereas the *Recommendation* was a legal instrument providing guidelines for national legislation, the *Action Plan* was intended as a mechanism for targeting financial support towards implementing actions. Following the themes identified in the *Communication on illegal and harmful content* (European Commission, 1996b) it proposed four main action lines to 'create a safer environment' by combating illegal and harmful Internet content:

- Industry self-regulation – for example, through the creation of a European network of "hotlines" to allow users to report content that they consider to be illegal, and through the development of industry codes of conduct;
- Technical measures, such as the development of filtering and rating systems to make harmful content easier to identify;
- Raising user awareness, for example by developing material for use in the education sector;
- Support actions, such as those aimed at identifying the legal implications of actions taken under the *Action Plan.*

(European Commission, 1997a)

The *Action Plan* recognised the need for co-ordination and co-operation across Member States if actions were to be successful. Illegal use that it considered should be controlled included 'actions or speech that may be prejudicial to national

security; content that threatens the protection of minors (in particular child pornography) and the protection of human dignity (in particular race-hate speech); actions prejudicial to economic security (e.g. fraud) and information security (such as hacking); and actions liable to damage the protection of privacy, reputation or intellectual property' (European Commission, 1997a). It advocated that illegal content be dealt with at source by law enforcement agencies, aided by industry self-regulation (for example, by the use of hotlines to alert ISPs to potentially illegal content). Content deemed harmful (that is, content that is potentially offensive but not illegal) should be controlled via access restriction (such as filtering and ratings technologies) and by raising parental and user awareness, but should not be removed on the grounds of allowing freedom of expression. It noted that 'a definition of 'harmful' content will always be subject to the cultural differences inherent in the Member States' (Ibid).

During Parliamentary debate on 1 July 1998 it was noted that, while the *Action Plan* is 'a step in the right direction', the fact that EU legislation does not cover criminal law makes the promotion of safe Internet use a difficult task. Indeed

> *It was the unanimous view of the House that illegal and harmful content on the Internet could be damaging to the mental health, safety and economic interests of consumers and thus affect the creation of an environment conducive to sound ethical standards. But combating Internet content liable to prosecution was a matter for the member states. In practice, this was made considerably more difficult by the fact that there were not even identical or at least comparable legal standards governing important issues in this area throughout the EU.*
>
> (European Parliament, 1998b)

There was here a clear statement that the driver for legislation to control Internet content was the desire to promote an environment that favoured the development of e-commerce and a growth in Internet use as an impetus to economic development. On its second reading at the Parliament several amendments to the *Action Plan* were tabled: that support should be given under the *Action Plan* to organisations active in the protection of human rights and in counteracting abuse of women and children; the most effective means should be used for disseminating

information to raise user awareness; Internet providers who voluntarily keep to a code of conduct agreed within the industry on undesirable website content should be able to apply to the Commission for a 'quality' label; and, potentially the most far-reaching proposal of all, civil and criminal law within the EU should be harmonised with the aim of ensuring safer use of the Internet (European Parliament, 1998c).

In order to pursue the aims of developing technical means of content regulation the European Parliament awarded a contract to Smith System Engineering to investigate the technical feasibility of software to block pornography and racism on the Internet. Working with legal and social policy experts, the engineering consultants were charged with providing a study to be used as a briefing document for Members of the European Parliament (MEPs) expected to form the basis of future policy (Taylor, 1997). The resulting report *Feasibility of censoring and jamming pornography and racism in informatics* (Pitman, 1997) identified possible solutions such as the use of labelling and rating standards such as PICS and filtering software such as Net Nanny, CyberPatrol and Cybersitter (Craven, 1998). The Open Information Interchange (OII) of the European Commission published a guide to labelling of electronic data, and rating and filtering as a function of labelling (European Commission, 1998a). However, despite much subsequent investment into the development of technical solutions, they have so far failed to meet the hopes and expectations vested in them (see Chapter One, pp.22-29 for further discussion on this issue).

Following an intermediate evaluation of the results of implementing the *Action Plan*, carried out between November 2000 and April 2001, the Commission published a *Communication Paper* on the follow-up to the *Action Plan* with a proposal that it should be extended for a further two years until 31st December 2004 (European Commission, 2002a). In addition to proposing future directions for EU strategy on content regulation, the *Communication Paper* was useful in providing a detailed account of projects funded to date under the original *Action Plan.* The intention of the new proposal was to 'adapt [the scope and implementation of the *Action Plan*] to take account of lessons learned and new

technologies, and to ensure co-ordination with parallel work in the field of network and information security' (Ibid). In reality, the proposed 'adaptation' of scope comprised a significant extension of application, both in terms of the technologies to which the coverage would apply and the nature of the content to be controlled. Thus, in future proposed actions would apply to 'mobile and broadband content, online games, peer-to-peer file transfer, and all forms of real-time communications such as chat rooms and instant messages' (Ibid). Relevant content would now encompass racism and violence.

The Commission still claimed the underlying rationale of the *Action Plan* as being that of user empowerment, with the Commission acting as facilitator for, and contributor to, European and global co-operation in this arena. EU actions were promoted by the Commission as complementary to national initiatives, with the aim of achieving a considerable degree of decentralisation through a network of national co-ordinators. Four areas still requiring action were identified in the proposed extended *Action Plan*:

- Support for hotlines to enable users to report illegal content;
- Continuing promotion of self-regulation;
- User empowerment through filtering software;
- Increasing awareness about safer use of the Internet.

(European Commission, 2002a)

It was acknowledged that the focus of the new programme should be on self-regulatory and non-regulatory aspects of safe Internet use, with an emphasis on actions intended to raise awareness of safe use, particularly in countries that currently lacked appropriate experience and infrastructure. It was also suggested that part of the new initiative should include support for the creation of high quality European content intended specifically for children (Ibid). Enhanced networking was to be encouraged among all those involved in the field through the establishment of a Safer Internet Forum, and more active involvement of the media and content industries was promoted as desirable.

In response to the *Communication* from the Commission, the European Economic and Social Committee (EESC) proposed a more restrictive approach. The Committee recommended adopting a legal framework that ensured co-legislation rather than the self-regulation proposed by the Commission. It also advocated stronger government and industry support for ratings and warning schemes, particularly with regard to chatrooms, and the adoption of a stronger line against racism on the Internet, which 'should not be condoned on the grounds of protecting freedom of expression' (European Economic and Social Committee, 2003).

On 16th June 2003 the Parliament and Council agreed to the original communication proposal by taking *Decision No 115/2003/EC amending Decision No 276/1999/EC adopting a Multiannual Community Action Plan on Promoting Safer Use of the Internet by Combating Illegal and Harmful Content on Global Networks* (European Commission, 2003b). In addition to the changes already described, the Decision amended the title of the Plan to that of the '*Multiannual Community Action Plan on Promoting Safer Use of the Internet and New Online Technologies by Combating Illegal and Harmful Content Primarily in the Area of the Protection of Children and Minors*' to reflect new emphases. In its communications the Commission appears to have adopted the abbreviated title of the '*Safer Internet Action Plan'* (SIAP) in referring to the new Plan; it is also referred to as the 'Action Plan second phase'. An additional sum of 13.3 million Euro has been made available for implementing the extended actions. The draft Work Programme and initial draft Calls[41] were made available in July 2003.

In August 2003 the European Commission announced that, in addition to the extension of the Action Plan to 2004, it was making preparations for a follow-up programme, the Safer Internet Plus programme[42], to cover the period 2005-2008

[41] <http://www.europa.eu.int/information_society/programmes/iap/index_en.htm> [Last accessed 5/7/2004]

[42] See <http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/04/333&format=HTML&aged=0&language=EN&guiLanguage=en> [Last accessed 5/7/2004]

(Swetenham, 2003). The overall objective of this programme remained the promotion of safer use of the Internet and other new technologies, particularly by children, and to continue the fight against illegal content and 'content unwanted by the end user' (Ibid). The stated intention this time was to focus on the end-user, in particular parents, educators and children. In addition to building on the achievements of existing actions, the programme was to be opened up to other new media, and to new issues such as the control of 'spam'[43] and the expansion of network infrastructure to accession countries. The role of different stakeholders would be analysed to determine the role that they could play in the fight against illegal, harmful and unwanted content.

3.4.4 The Information Society, the management of the Internet and democracy

Reflecting a rather more positive and distributive perspective than that evidenced in other EU initiatives, the European Parliament acknowledged in a *Resolution on the Information Society, the management of the Internet and democracy* (European Parliament, 1998a) that freedom of expression is one of the foundations of democratic societies, and that use of the Internet 'could open the way to strengthening democracy by increasing transparency'. It also recognised that 'globalisation of the Internet requires an international regulatory framework…including the protection of cultural and linguistic diversity and the protection of human dignity and minors'. The resolution 'calls on Member States to ensure that the [Internet is] used to promote freedom of speech and information, exchanges between cultures, education and civic participation in public life, in particular in relation to EU enlargement or international contacts with countries whose peoples live under authoritarian and repressive regimes' (Ibid). This statement represented a much stronger endorsement of the potential of the Internet as a tool to support and enhance democracy, and located the role of national states

[43] Unsolicited email, usually of a commercial nature, sent to multiple email users.

as being the promotion and strengthening of the positive benefits of the Internet as opposed to a preoccupation with its potential for harm.

3.4.5 The role of libraries in the Information Society

In October 1998 the European Parliament adopted a report (Ryynänen, 1998) that also evidenced a more liberal, distributive perspective. This reported on the *Green Paper on the Role of Libraries in the Information Society*, which had explored the issue of public access to the Internet via libraries. The report called for greater co-ordination of policy measures by the Member States in providing access to knowledge and information via libraries. It recommended that the Member States provide libraries with modern equipment and Internet connections, together with 'adequate funding to take advantage of the Information Society' (Ibid).

It also proposed that the means should be made available to train library staff to 'filter out required material' from the massive volume of information available. Noting the poor performance of software filters, and the difficulties posed by varying cultural approaches to content control, it considered that 'there is a manifest need for selective and sustained search services which provide access to material on the basis of professional librarians' definitions of acceptable network material' (Ibid). It thus identified the control of access to Internet content as being a matter best resolved through human judgement, and in particular saw such judgement as being part of the intrinsic role of information professionals. However, such bold declarations appear since to have received scant attention compared with the more restrictive calls for industry-led content control contained in initiatives such as the *Action Plan.*

3.4.6 The Framework Programmes for Research

Alongside the measures already outlined, the EU Framework Programmes for Research have paid considerable attention to the information services sector.

These Framework Programmes for Research, Technological Development and Demonstration Activities set out the priorities for EU investment in research and development over five-year periods. The Fifth Framework Programme, which covered the period 1998-2002, included the creation of a 'User-friendly information society' as one of four major themes, with a budget of 3,600 million Euro, the single largest budget allocation of the four themes (European Commission, 2000a). This emphasis was largely driven by the convergence of the computing, communication and content industries and the global nature of the information marketplace, which led to recognition of the importance of a coherent approach to addressing the development of the Information Society. This theme is also reflected in the priorities of the Sixth Framework Programme, which runs from 2002 to 2006 (European Commission, 2002b). In both these programmes, however, activities funded have tended to concentrate on issues of competitiveness and the needs of business and industry, leaving issues of Internet regulation and the development of content control technologies largely to the *Action Plan.*

3.4.7 The European Internet Co-regulation Network

At the World Summit for the Information Society, held in Geneva in December 2003, European Commissioner Erkki Likkanen announced the launch of the European Internet Co-regulation Network[44] (Forum des Droits sur l'Internet, 2003). Supported by the European Commission and the French government, through its Forum des Droits sur l'Internet[45], the Network aims 'to promote co-regulation as a means of gaining the co-operation of all the stakeholders in the building of rules on Internet rights and usage issues' (Ibid). At the time of its launch the network had seven members: Austria, Belgium, France, Hungary, Italy, Sweden and the UK, the latter being represented through the Internet Watch Foundation and the Oxford Internet Institute. Although it is portrayed as having a

[44] <http://www.internet-coregulation.org> [Last accessed 5/7/2004]

[45] <http://www.foruminternet.org> [Last accessed 5/7/2004]

predominantly co-ordinating role, rather than a regulatory role, it is too early to gauge the exact role the Forum will play or what influence it will exert in the Internet control arena.

3.4.8 The EU and e-commerce, privacy, interception and surveillance

By 1998 the development and promotion of e-commerce, with the subsequent need to create a favourable and appropriate regulatory framework to instil confidence in business and consumers alike, began to climb higher on the EU agenda. An initial proposal was put forward in November 1998 (European Commission, 1998b), culminating in the adoption by July 2000 of a *Directive of the European Parliament and the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market* ("the E-commerce Directive") (European Commission, 2000b). In order to stimulate, rather than hinder, the development of e-commerce, the Directive adopted a light-handed approach with an emphasis on self-regulation that mirrored its approach towards issues of content regulation. Following an Amendment made during the consultation phase, the Directive included a specific reference to the protection of minors and human dignity, and assured the rights of Internet users to confidential electronic communication by using encryption services, should they so choose.

However, the relatively light-handed approach based on self-regulation that had characterised EU involvement in regulating the Internet came under threat with the terrorist attacks that took place in the United States on September 11th 2001. The period since then has seen a wave of initiatives aiming to increase the powers of law enforcement agencies to monitor and intercept electronic communications. Thus, for example, in May 2002 the European Parliament approved legislation[46] that gave police the power to access the communications records of all telephone and Internet users (Millar, 2002a). Regardless of the privacy protections afforded

[46] Electronic communications: Processing of personal data, protection of privacy. The Final Act was published in the *Official Journal of the European Union,* L201, 31/7/2002.

by the Data Protection Directive (European Commission, 1995) the new measure allows governments to require telephone and Internet companies to retain detailed logs of their customers' communications for a minimum of 12 months and a maximum of 24 months. In a further direct conflict with the Data Protection Directive (Ibid), under the new measure individuals have no right to check whether information held about their personal communications is accurate, nor are they entitled to legally challenge decisions made about its use by EU authorities (Norton-Taylor and Millar, 2002). Ironically, the measure was contained in an amendment to a bill that was originally intended to improve the security of e-commerce transactions and personal privacy.

Such measures were initially explained by national governments and the European Parliament by the need to fight terrorism. However, this justification is now being extended to include the demands of fighting all crime, including paedophilia and racism (Norton-Taylor and Millar, 2002). Much of the driving force behind the measure came from the UK government (Millar, 2002a; Ahmed, 2002), which had already imposed data retention obligations on ISPs in the UK via the Anti-Terrorism, Crime and Security Act (Parliament, 2001) rushed through the UK Parliament in 2001. This was in addition to the *Regulation of Investigatory Powers Act* (Parliament, 2000a), which had already established the right of a range of public bodies in the UK to intercept, monitor and access communications data.

3.5 Policy development in the United Kingdom

3.5.1 UK approaches to information policy

In a number of significant initiatives, the UK has embraced the emphasis placed by the EU on the development of the Information Society as a tool of economic growth and competitiveness, with a secondary proclaimed goal of enhancing social cohesion and inclusion. The government gave recognition to the importance of support for the development of e-commerce with the statement that 'The Government's policy is to encourage electronic commerce, with the ambition of

making the UK the best place in the world for electronic trading' (Department of Trade and Industry, 2003). To date, this support has been applied most actively to the issue of how to build trust and security into e-commerce activities (Saxby, 2000, p.44) and has been implemented through the *Electronic Communications Act 2000*[47], which established the legality of electronic signatures and an approvals scheme for cryptography support services (Ibid). In addition to the *Electronic Communications Act*, in 2002 the government also incorporated the EU *E-commerce Directive* (European Commission, 2000b) into UK law following a wide consultation exercise. However, UK government approaches to e-commerce have also been influenced by a recognition that the availability of offensive Internet content may 'lead to lack of confidence for the development of e-commerce within the UK' (Cabinet Office Performance and Innovation Unit, 1999).

Despite the recognition of the importance of e-commerce, Bellamy and Taylor note that the UK was relatively slow to adopt the widespread use of Information and Communication Technologies, or to adapt its practices towards the context of the new Information Age (Bellamy and Taylor, 1998). Rowlands (1997, p.48) and Oppenheim (1998) have both noted the highly decentralised and fragmented nature of UK national information policy, involving as it does a wide range of actors and an amalgam of statutory law, common law, social norms, administrative practice, market forces and international agreements and treaties. Going a step further, Oppenheim (Ibid) has suggested that 'the UK's information policy is, in most cases, to have no policy'.

This lack of a national information policy was also acknowledged in a policy report prepared by the Library and Information Commission in 1999 which stated that 'a UK National Information Policy is urgently required if we are to remain competitive in the global information society' (Library and Information Commission, 1999). However, despite progress made with regard to specific

[47] <http://www.hmso.gov.uk/acts/acts2000/20000007.htm> [Last accessed 5/7/2004].

policy issues, by 2003 there was still evidence of an overarching lack of co-ordination or clear line of responsibility for information policy formulation.

3.5.2 Improving access to the Internet – the People's Network

A 1997 Library and Information Commission report, *The New Library: The People's Network,* commissioned by the Department for Culture, Media and Sport, recognised the potential of the new communications technologies for enhancing education and lifelong learning; supporting training, employment and business to foster economic prosperity; and nurturing social cohesion (Library and Information Commission, 1997). In addition to a commitment to extending Internet access to all public libraries in the UK, the report placed emphasis on the role of the librarian as intermediary in the networked environment and recommended that £3 million be provided over five years to support public libraries in developing controlled gateways to high quality resources in specific subject areas (Ibid).

As a result of the report, the New Opportunities Fund (NOF) was established, funded by the National Lottery and managed by the Library and Information Commission's successor, Re:source[48]. The aim of the NOF was to implement the Government's commitment to 'give everyone in the UK the opportunity to use computers and access the Internet' (The People's Network, 2002). By December 2002 the People's Network reported that 100% of all UK public libraries were connected to the Internet[49].

[48] Since renamed Museums, Libraries and Archives Council (MLA). See <http://www.mla.gov.uk/index.asp> [Last accessed 5/7/2004]

[49] Figures obtained from <http://www.peoplesnetwork.gov.uk/progress/libraries.asp> [Last accessed 5/7/2004].

3.5.3 UK approaches to Freedom of Expression

Prior to the accession into British law in November 1999 of the *Human Rights Act 1998*[50] (Parliament, 1998a) there was no statutory general right of freedom of expression within the UK, only legislative measures that imposed restrictions on such freedom. These measures included the *Obscene Publications Acts* of 1959 and 1964 (Parliament, 1959; Parliament, 1964); the *Race Relations Act 1976* (Parliament, 1976); the *Video Recordings Act 1984* (Parliament, 1984); the *Malicious Communications Act 1988* (Parliament, 1988a); the *Official Secrets Act 1989* (Parliament, 1989); the *Broadcasting Act 1996* (Parliament, 1996a); the *Criminal Justice and Public Order Act 1994* (Parliament, 1994a) (involving incitement to racial hatred); and the *Defamation Act 1996* (Parliament, 1996b).

The *Human Rights Act 1998* (Parliament, 1998a) is the instrument that incorporates the provisions of the *European Convention on Human Rights* (ECHR) (Council of Europe, 1950) into UK law. In line with the ECHR, Article 10 of the *Human Rights Act* contains the statement that:

> *Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.*
>
> (Parliament, 1998a)

Thus, for the first time, UK citizens had a right to freedom of expression enshrined in a Parliamentary Act. However, the rights conferred through the Act are not without limits. As with the ECHR, in addition to reserving the right of the State to require the licensing of radio and television broadcasting, and of cinema enterprises, the Act also states that:

[50] <http://www.hmso.gov.uk/acts/acts1998/19980042.htm> [Last accessed 5/7/2004]

> *The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.*
>
> (Ibid)

There remains, therefore, considerable scope for the government to impose constraints on the right to freedom of expression, and this right has indeed already met with considerable challenge particularly in the light of the 'war on terrorism' of the early Twenty-first Century.

3.5.4 UK approaches to Internet content control

In line with the EU and the Council of Europe, the preferred measure with regard to the issue of Internet content control within the UK has been that of voluntary self-regulation (Barrett, 1996; Akdeniz, 1997b), together with support for the development of technological solutions such as rating and filtering systems. Support for a self-regulatory approach was stated quite clearly in a Select Committee on Science and Technology report in 1996 that stated:

> *Even if it were desirable, it is unlikely that censorship of Internet content will ever be possible, partly on technological grounds, partly because of its global nature. The best hope of controlling the circulation of undesirable material on the Internet is self-regulation.*
>
> (Parliament: House of Lords, 1996, para.5.50)

This contrasts with the US where, despite the provisions of the First Amendment, repeated (and mostly unsuccessful) legislative attempts have been made to control Internet content. Within the UK the main responsibility for Internet content issues rests with the Department for Trade and Industry (DTI) supported by the Department for Education and Skills (DfES) and the Home Office (Akdeniz,

2001). Self-regulation in the UK has been implemented via the Internet Watch Foundation (IWF) in co-operation with the Internet Service Providers Association (ISPA) and the Home Office.

3.5.5 The Internet Watch Foundation

In the UK the active involvement of the ISPs in controlling Internet content was called for in a letter sent in August 1996 to all ISPs by Chief Inspector Stephen French of the Clubs and Vice Unit of the Metropolitan Police. The letter contained a list of newsgroups that the Vice Unit believed to contain 'offensive material', and stated that 'we are looking to you to monitor your newsgroups identifying and taking necessary action against those others found to contain such material' (Watson, 1996a). This move was resisted by the ISPs for a number of reasons, not least on account of the ethical and practical difficulties that implementation would incur. The problems involved in attempting to target specific groups were clearly illustrated by the Metropolitan Police's own list of 'offensive' sites: this included the UseNet group 'alt.sex.paedophilia', which was in fact a forum for discussing methods of identifying, treating and helping paedophiles and their victims (Ibid). Overall, UK ISPs considered that the approach of the Metropolitan Police 'had been founded on a misunderstanding of the technology involved' (Watson, 1996b) and that moves to impose content censorship of the Internet should be debated in Parliament rather than randomly applied by law enforcement agencies (Akdeniz, 1997a).

Instead of co-operating with the terms of the Metropolitan Police's letter, ISPA[51] requested a meeting with the Metropolitan Police and other interested parties, leading to the establishment of the Safety-Net Foundation[52] in September 1996. The Foundation was set up as an independent organisation to implement proposals

[51] <http://www.ispa.org.uk> [Last accessed 5/7/2004]

[52] This subsequently became the Internet Watch Foundation (IWF), <http://www.iwf.org.uk> [Last accessed 5/7/2004]

for controlling Internet content that were jointly agreed by the government, the police and the Internet Service Provider associations (ISPA and LINX[53]), including the drafting of a Code of Practice for the industry. The initial self-regulatory focus of the IWF was on child pornography, with ISPs agreeing to exclude clients who hosted illegal pornographic or paedophile images or messages, wherever this was brought to their attention. A hotline was set up to enable Internet users to alert the IWF to sites that they suspect contain illegal materials and, if found to be so, IWF alerts any ISP hosting the site. Only if the ISP does not co-operate in removing the content at this stage would it be liable for prosecution. During its first year of operation the IWF hotline led to more than 2,000 items being removed from UK Service Providers (Library Association Record, 1998b). The statistics for the year 2002 revealed that the total number of reports made to the IWF had risen to 21,341, leading to 3,774 items being removed – 3,768 for child pornography content, five for having 'adult obscene' material, and one for being 'criminally racist' (Internet Watch Foundation, 2003).

In addition, the IWF established an Advisory Board including representatives of children's charities, content providers, regulators from other media, ISPs and civil liberties groups to develop a rating system 'appropriate to the needs of UK Internet users' (European Commission, 1997d). The IWF was also instrumental in bringing together a group of interested parties within Europe to develop the INCORE (Internet Content Rating for Europe), under commission from the EU. The primary aim of INCORE was to investigate a means of rating Internet content that identified illegal material and allowed for the classification of legal material. The latter action was to be based on consumer research as to users' expectations regarding the Internet and the kind of material to which they would consider the application of ratings to be appropriate (Ibid).

In 1998 it was announced that there would be a governmental review of the IWF, with a view to expanding its role to include the control of defamatory material and

[53] <http://www.linx.net> [Last accessed 5/7/2004]

copyright breaches on the Internet (Library Association Record, 1998c). In addition, the Foundation joined forces with the International Working Group on Content Rating (IWGCR), a coalition of national and international watchdog organisations, to establish an international rating system for legal material that would allow the end user to define the categories of content that they wished to exclude. This group subsequently led to the formation of ICRA, the Internet Content Rating Association[54]. It also began working on the development of screening software intended to facilitate the monitoring of UseNet articles to aid the identification of illegal content, and has developed its role in terms of promoting awareness and education with regard to Internet content issues.

The *Public Order Act 1986* (Parliament, 1986), as amended by the *Criminal Justice and Public Order Act 1994,* makes it an offence 'to publish material designed or likely to stir up racial hatred' (Parliament, 1994a). In January 2000 it was announced that the remit of the IWF was to be expanded to include the policing of such 'criminally racist' material (Travis, 2000). However, the definition of what material can be considered as 'criminally racist' is more complex than the identification of materials involving child pornography, and since simple possession of the material is not in itself illegal, prosecution can only follow evidence of the intention to 'publish' the material to others. The Home Secretary at the time, Jack Straw, defended the proposed extension of the remit of the IWF by stating that 'the Internet cannot exist in an anarchistic free speech environment' (Ibid).

In co-operating with the approach of self-regulation via the IWF, participating ISPs have taken on some responsibility towards prevention of use of the Internet for illegal purposes, whilst managing to ensure that end users are responsible for the content they post and responsibility for law enforcement remains with the police (Watson, 1996b). However, they have done so partly in response to the threat of enforced regulation, seeing self-regulation as a means of protecting

[54] <http://www.icra.org> [Last accessed 5/7/2004]

freedom of expression from the imposition of more authoritarian measures[55]. This latter point was vividly illustrated by the comments of the then Commander of the Metropolitan Police Clubs and Vice Unit, Mike Hoskins, at a meeting held in August 1996 between Scotland Yard and ISPA. This was immediately prior to the letter sent to the ISPs that requested removal of access to named UseNet discussion groups. Hoskins stated at the meeting 'either the industry takes it upon itself to clean up the Net or the Police intervene' (cited in Akdeniz, 1997b). The letter itself included the sentence 'We trust that with your co-operation and self-regulation it will not be necessary for us to move to an enforcement policy' (cited in Campbell, 1998b).

However, critics of the IWF approach have raised doubts about the ability of a non-public body to maintain sufficient standards of transparency and accountability. Akdeniz has claimed that the UK policy of reliance on the IWF forces ISPs 'to be defendant, judge and jury' and that removal of content by the IWF in the absence of a court order amounts to 'censorship by the back door'[56]. It has been argued that locating regulatory initiatives into the private rather than the public sector risks not only a loss of accountability, but also the probability that commercial pressures may induce a more proactive involvement with content regulation (Akdeniz and Strossen, 2000).

3.5.6 Legal liability of ISPs in the UK

The main impetus for the ISPs to co-operate with measures to control illegal content on the Internet was uncertainty with regard to their potential liability for such content. Although the ISPs have always maintained that they are 'common carriers' and should be no more responsible than telephone service providers or the

[55] From comments made by David Kerr, Chief Executive of IWF, at an Oxford Union Debate *Beyond Control or Through the Looking Glass* held in April 2000.

[56] From comments made by Yaman Akdeniz of Cyber-Rights and Cyber-Liberties, at an Oxford Union Debate *Beyond Control or Through the Looking Glass* held in April 2000.

Post Office for the material they carry, it has also been argued that they should be held liable for content in a similar way to broadcasters or publishers. The actions of the Metropolitan Police in suggesting that they would 'move to an enforcement policy' (Campbell, 1998b) if the ISP industry did not impose a satisfactory regime of self-regulation certainly aroused concern among ISPs about their own liability. This concern was exacerbated in September 1998, when 30 police officers launched a dawn raid on a major ISP as part of the child pornography investigation 'Operation Cathedral', seizing computer logs and arresting a member of staff (Ibid).

Concern regarding the legal liability of ISPs in the UK intensified when ISP company Demon Internet Ltd were found liable for damages and costs in a court settlement to physicist Laurence Godfrey. Godfrey claimed that he had been defamed by two anonymous postings on newsgroups hosted by Demon, and that Demon had ignored his request to have the postings removed. The case is significant in that it suggested that if ISPs do not respond to requests to remove allegedly defamatory content then under Section One of the 1996 *Defamation Act*[57] (Parliament, 1996b) they cannot claim 'innocent dissemination' but instead are responsible as the 'publisher' of the content (Gringras, 2003, p.127). The Godfrey v Demon Internet Ltd case[58] thus highlighted the issue of potential liability for libellous content on the part of ISPs.

Following the case, other ISPs, concerned about its implications, responded to claims about potentially libellous content by removing the content concerned as a precautionary measure. Examples included the removal of a radical gay magazine's website, an anti-censorship site and a site that highlighted miscarriages of justice (Wells, 2000a; Wells, 2000b). As there is no onus to prove that statements complained about are malicious or false before threatening prosecution, ISPs are likely to respond to the threat of legal action by removing content without

[57] <http://www.hmso.gov.uk/acts/acts1996/96031--a.htm#1> [Last accessed 5/7/2004].

[58] Godfrey v Demon Internet Ltd [2001] QB 201, [1999] 4 All ER 342.

waiting for a judicial verdict on the content. This "chill factor" (Wells, 2000b) has potentially serious implications for freedom of expression on the Internet.

In another case involving Demon Internet Ltd, Judge Butler-Sloss ruled in July 2001 that ISPs would not be held responsible if their users revealed the whereabouts or new identities of Jon Venables and Robert Thompson, who murdered James Bulger in 1993 (Dunne, 2001). Butler-Sloss ruled that 'ISPs were protected if contemptuous material was posted on web pages – as long as they took "all reasonable steps" to prevent the publication of such material' (Ibid). It would seem that, in line with the self-regulatory policy of the IWF, this means that ISPs will be liable for prosecution only if they are informed about an illegal site and subsequently fail to remove it. This removes the onus of 'policing' content on their servers from the ISPs. However, it is unclear whether this ruling means that they should respond to requests from anyone who wants them to remove content that (in the absence of a court decision) the complainant regards as defamatory to their reputation.

This lack of clarity was further illustrated in 2002 when ISP Host Europe responded to a request from the police to remove the satirical site www.thinkofthechildren.co.uk from its server, following a complaint by a member of the public (Left, 2002). Despite no court ruling on the legality, or otherwise, of the site's content, Host Europe shut down the site, fearing that the company could be held criminally liable. The site was subsequently reinstated, albeit with the 'suspect' content removed (Ibid).

3.5.7 Rating systems and filtering software in the UK

In line with the EU, rating systems and filtering software have consistently been promoted by UK policy makers as a potential solution to the problem of access to 'harmful' (as opposed to illegal) Internet content, particularly where this access applies to minors. Unlike the approaches of the US or Australian authorities, however, there have been no attempts to implement legislation compelling ISPs,

schools or libraries in the UK to install filtering software. With specific regard to public access to the Internet within UK public libraries, the Networked Services Policy task group of Project EARL was set up in 1996 with a brief 'to assist public library authorities to shape and develop their own public access strategies' (Everall, 1996). The chief concern of the project was focussed on illegal material available on the Internet, in particular hardcore pornography, and the ability to create and send offensive materials to others. At the time of the study, the Group found little support among public librarians for filtering software. However, there was a broader level of support for actions such as selecting an ISP that filters at server level; supervised access for children; and the establishment of Acceptable Use Policies requiring users to sign an undertaking not to abuse the service (Ibid).

Acceptance of technical solutions among librarians appears since to have increased: an unpublished survey by Manchester Metropolitan University carried out in 2000 found that 71 per cent of libraries had some form of technical control, with half of these opting for filters as their favoured solution (Library Association Record, 2001). A People's Network survey carried out in June 2002 reported that 65.71% of Library Authorities used filtering software for public library Internet access; in addition, 86.67% of Library Authorities had an Acceptable Use Policy in place[59].

The UK Library Association, prior to its amalgamation with the Institute of Information Scientists to form CILIP, did not endorse the use of filtering, although they did accept that libraries may be obliged to use such software (Willson, cited in Library Association Record, 2001). However, it was recognised that the issue of filtering software in public libraries is contentious, especially with regard to children's use of network facilities. Thus, at the time of writing (2004), the new organisation has not yet determined its policy, preferring to 'look at the issue again

[59] Figures available from <http://www.peoplesnetwork.gov.uk/progress/libraries_uk.asp> [Last accessed 5/7/2004].

from scratch'[60]. To this end it has appointed a Freedom of Information panel that will have responsibility for developing policy in this area.

3.5.8 UK educational initiatives

The UK government has also put considerable emphasis on educational measures targeted at minors to promote an awareness of safe Internet use. In 1999 the then Education Secretary, David Blunkett, launched an information pack entitled 'Superhighway Safety' containing practical advice for parents and teachers on how to reduce children's exposure to 'unacceptable' information (Smithers, 1999). The information pack recommended schools to use written contracts whereby pupils pledge to use only specified websites, backed up by regular checks by teachers. Schools are also advised to use "walled gardens" and firewalls to block banned sites. Parents are advised to supervise the home Internet use of their children, who should be warned not to give out personal details online (Ibid).

The benefits of an approach based on educating children about responsible online use were reflected in the publication of a 2001 report by the Institute of Public Policy Research (IPPR), an influential Think Tank with close links to the government (Livingstone, 2001). This proposed that children should take a 'surfing proficiency test' at the age of eleven; students who passed should then be allowed less restricted access to the Internet than schools currently allow. They would be able to take a one-week summer course to prepare for the test, which, in addition to educating them about avoiding potential dangers online, would also help them to develop their skills in using the Internet constructively to find information. However, the proposal was received with some scepticism by the General Secretary of the Secondary Heads Association who maintained that 'A proficiency test as a passport for unsupervised use of the Internet would simply give [children] even more knowledge of how to find sites that they shouldn't be seeing' (reported by Woodward, 2001). To date (April 2004) the initiative has not

[60] Email communication to the author from Guy Daines, Principal Policy Advisor, CILIP, 2/9/2003.

been implemented, although it is still being promoted for potential adoption by the IPPR[61].

However, in January 2003 the government did launch a £1million advertising campaign, using television, radio and website messages to warn of the dangers of paedophiles using the Internet, and aiming to make parents and children aware of how to surf the web safely (BBC, 2003a). The government's approach in this respect appears to be constructive and positive. At the launch of the campaign, Home Office Minister Hilary Benn said that he hoped the campaign would give parents and children basic safety information without demonising the Internet:

> *The Internet is a great tool, it opens up all sorts of possibilities and we don't want to scare people about using it, we just want to make sure that when you use the Internet you do so safely.*
>
> (Cited in BBC, 2003a)

The advertising campaign was accompanied by the production of a new set of guidelines for ISPs who offer chat and instant messaging services, including the recommendation of using clear warning information on their sites and ways for children to report problems encountered online.

Other UK organisations have also been involved in promoting 'safe use' initiatives for children, a good example being the NCH Action for Children booklet '*Children on the Internet: Opportunities and Hazards*' (NCH Action for Children, 1998).

3.5.9 Privacy, surveillance and monitoring

Although a comprehensive analysis of UK public policy measures relating to privacy, surveillance and monitoring of Internet use is outside the scope of this

[61] See <http://www.ippr.org/research/index.php?current=25&project=72> [Last accessed 5/7/2004]

thesis, a brief outline of some of the major recent initiatives in this area is appropriate, on account of the importance of their potential impact on freedom of expression and freedom of access to information.

The events in the US on 11th September 2001 and the subsequent 'war on terrorism' have been used to justify a range of measures restricting rights to privacy in the online environment in the UK. However, the initial steps to implement these measures can be traced back as far as at least early 1997, when the National Criminal Intelligence Service (NCIS) requested urgent action to introduce legislation enabling police to intercept and monitor emails (Campbell, 1998b). This was put on hold because of the General Election of 1997, but was resurrected in June 1998 when the Association of Chief Police Officers (ACPO) agreed a 'memorandum of understanding' with ISPs, that would enable police to monitor customers' emails, and Web-usage logs on demand (Library Association Record, 1998d, p 457; Campbell, 1998b). The Memorandum also obliged ISPs to retain logs of user transactions for a minimum of six weeks (Arthur et al, 1999). Concern was expressed by legal practitioners and civil liberties organisations that the agreement lacked the normal legal safeguards, as police interception would not require a warrant. The Data Protection Registrar at the time, Elizabeth France, expressed strong reservations:

> *We say it time and time again – [under the Data Protection Act] information can only be released on a case by case basis. Fishing expeditions are not allowed…It is important that [email] has the same level of protection for individuals as for any other communications – mail and telephone calls.*
>
> (Cited in Campbell, 1998b, p.2)

Subsequent legislation, the *Regulation of Investigatory Powers Act 2000*[62] (Parliament, 2000a), clarified the electronic interception powers of public authorities in UK law, when it superseded the *Interception of Communications Act 1985* (Parliament, 1985) in July 2000. It also implements Article 5 of the EU

[62] <http://www.hmso.gov.uk/acts/acts2000/20000023.htm> [Last accessed 5/7/2004].

Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector[63] (JISC, 2001). Introduced by the government as an instrument for controlling the powers of public authorities to monitor and intercept communications under a single regulatory regime in compliance with human rights legislation (Pallister, 2003), implementation of the Act arguably led to an extension of these powers, and imposed additional responsibilities onto ISPs. In addition to the authority of the Home Secretary to issue warrants for the interception of communications, the Act allows any public authority designated by the Home Secretary to access 'traffic data' (i.e. source, destination and type of any communication) without a warrant (EPIC and Privacy International, 2002). Under the Act ISPs are required to provide a 'reasonable interception capability'; every UK ISP is responsible for installing remote-controlled equipment that relays all data passing though its computers to a special monitoring centre in MI5's headquarters (Greenslade, 2000). In addition, it allows senior members of the civilian and military police, customs authorities and members of the judiciary to demand the plain text of encrypted material, or, in certain circumstances, actual decryption keys (EPIC and Privacy International, 2002). In the event of refusal to provide the decryption key or password to his or her computer files, anyone who is unable to prove that it has been lost or destroyed will be liable to up to two years imprisonment (Ibid). Anyone who discloses that they have been served with an order to surrender decryption keys or passwords is liable for a five-year jail term (Greenslade, 2000).

The ISP industry has expressed reservations concerning the financial costs to them of compliance with the 'reasonable' provision to facilitate interception required under the Act, and the potential impact that such costs, together with the loss of privacy afforded to the UK online environment, may have on e-commerce. The ISPA estimated in 2000 that RIPA was likely to lead to the interception of around one in every 500 Internet communications (Sommer, 2000). There is also a potential for conflict between compliance with the terms of RIPA and with those

[63] <http://europa.eu.int/ISPO/infosoc/telecompolicy/en/9766en.pdf> [Last accessed 5/7/2004].

of the *Data Protection Act 1998* (Parliament, 1998b) and the *Human Rights Act 1998* (Parliament, 1998a).

However, the provisions of RIPA did not meet all the demands of the police, security and intelligence agencies who subsequently requested the Home Office to enact legislation that would require all telecommunications companies and ISPs to retain all communications data originating or terminating in the UK, or routed through UK networks for a period of up to seven years (Norton-Taylor, 2000). The terrorist attacks on the Twin Towers in New York in September 2001 gave added legitimation and public support to government initiatives to extend monitoring and interception powers. However, these powers were not limited to anti-terrorism investigations, but also to police investigating minor crimes, as well as to tax collection and public health authorities (Millar, 2001b). Indeed, in November 2001 the Home Office acknowledged that there were 'no plans to limit access [to communications data] to cases involving national security' (Ibid).

In December 2001, after an unusually fast passage through Parliament, the *Anti-Terrorism, Crime and Security Act 2001*[64] (Parliament, 2001) came into force – the fast-tracking was such that only two days were given to the Committee Stage, a process that would normally extend over a period of weeks (Fisher, 2002, p.17). At the time the House Affairs Select Committee was critical of the fact that the Bill should be 'passed by the House in such a short period and with so little time for detailed examination' and stated the opinion that 'the balance between freedom and security in the Bill has not always been struck in the right place' (Ibid, 2002, p.15).

Part 11 of the Act relates to data retention on the part of ISPs and telephone service providers, who will be subject to a voluntary Code of Practice on Data Retention (this was issued by the Home Secretary in September 2003): the Code calls for the retention of user logs for 12 months. The data to be retained includes

[64] http://www.hmso.gov.uk/acts/acts2001/20010024.htm [Last accessed 5/7/2004]. For a detailed account of the legislative process leading to the Act's introduction see Fisher, 2002.

the names and addresses of customers, the source and destination of emails received and sent, and the addresses of websites visited, all of which would be available to the authorities without the need for a judicial or executive warrant (Millar, 2002d). However, if the Home Secretary is not satisfied that the voluntary Code is working, the Act empowers him to enforce data retention. Two justifications are provided for extending data retention requirements, namely safeguarding national security, and the prevention and detection of crime (Parliament, 2001, Part 11, Section 102, 3(a) and 3(b)). In July 2002, the Director of NCIS indicated his dissatisfaction with reliance on a voluntary code, and his desire to see ISPs compelled to retain this data for a period of five years (Millar and Hopkins, 2002). At the same time, the Information Commissioner warned the Home Office that the data retention provisions of the Act may breach the *Human Rights Act 1998* (Parliament, 1998a), as data retained strictly for the purposes of national security could be accessed by police and intelligence officers investigating other crimes such as tax evasion.

In October 2002 ISPA announced that the industry was not convinced of the legality or justification of the data retention requirements and would not comply voluntarily with the Code of Practice (Millar, 2002d). In a letter to the Home Office, ISPA stated that ISPs were also concerned about the privacy and cost implications of retaining the required data. According to representatives of the ISP industry, the true cost to ISPs of storing the communications data required by the Code would be far in excess of the £20 million sum estimated by the government (Loney, 2002).

In June 2002 the Home Office announced that the list of government agencies allowed access under the *Regulation of Investigatory Powers Act* (Parliament, 2000a) to Internet traffic data without a warrant was to be extended to over 1,000 different government departments including local authorities, health and environmental organisations and trade bodies. Once again, the needs of crime and terrorism prevention were cited as justifying the proposal (Millar, 2002b). The ensuing complaints from the media, the public, civil liberties campaigners and representatives from ISPs led to the Home Secretary, David Blunkett, announcing

that he had 'blundered' and the proposal was withdrawn 'until the Autumn at the earliest' (Millar et al, 2002). It was reported widely in media coverage that this decision had been influenced by the Home Secretary's son, an IT specialist, telling his father that the proposal would be 'unworkable' for the Internet services industry.

In response, in March 2003 the Home Office issued a consultation paper, *Access to communications data: respecting privacy and protecting the public from crime*[65], which proposed to restrict the number of officials who can access communications data. The paper explained that the original proposal had failed to explain clearly the limitations that would have applied to public authorities' access to data. Alongside this consultation paper, the Home Office issued another on the retention of data requirements, proposing a code of conduct for ISPs and telephone companies allowing for a maximum period of twelve months for the retention of communications data. In comparison with the original proposals of June 2002, these proposals represented significantly decreased powers of monitoring and interception on the part of public authorities and clarified the situation of ISPs with regard to data retention. Nevertheless, civil liberties groups have expressed concern that data can be accessed without the requirement of a warrant from a judge (Pallister, 2003). Statistics published in 2003[66] suggest that the police and other authorities are making around one million requests each year under RIPA for access to data held by ISPs and telephone companies, although the accuracy of these figures has been disputed by the Home Office (BBC, 2003b).

These policy initiatives have wide-ranging potential implications for those responsible for managing and delivering library and information services, as illustrated by an incident that took place in a public library in Plymouth in January 2003. Having noticed a library user accessing web sites that displayed 'tall buildings', another library user contacted the police. The library web user turned

[65] <http://www.homeoffice.gov.uk/docs/consult.pdf> [Last accessed 5/7/2004].

[66] Compiled by the Foundation for Information Policy Research and cited in BBC, 2003b.

out to be a foreign student, and usage logs revealed that the 'tall buildings' were actually the logo used by an Internet radio station. The police subsequently asked library personnel if they could log Internet use made by asylum seekers. The request was refused by library authorities on the grounds of Data Protection and Human Rights legislation (Goddard, 2003).

A study on user privacy in the digital library environment carried out at Loughborough University between June 2000 and December 2001 investigated the attitudes and approaches to privacy of library users and library personnel in special, further education and higher education libraries (Sturges et al, 2003). Of the users of further and higher education libraries that were surveyed, 89% expressed 'no, or little, concern' about threats to privacy in using the library (Ibid). Three-quarters of the libraries' users accepted that 'the library should monitor the use of electronic services to prevent misuse' (Ibid). The findings of the study suggested that privacy issues were not high on the policy agenda of the respondent libraries, only 14% of which had a privacy policy in place. This contrasts with 81% of respondent libraries having an Acceptable Use Policy, 68% having an email policy and 64% having a Data Protection policy. The researchers suggested that this reflects a situation where libraries are more likely to formulate policy on an issue that generates a high level of public anxiety and media exposure, or as a response to the demands of legislation (Ibid). It should be noted that the fieldwork for this project was carried out prior to much of the media exposure given to the *Regulation of Investigatory Powers Act* (Parliament, 2000a) and the *Anti-Terrorism, Crime and Security Act* (Parliament, 2001), and it is likely, therefore, that there was little awareness on the part of either library users or personnel of legislative initiatives with regard to surveillance or interception of electronic communications.

As far as monitoring and interception of electronic communications in the workplace are concerned, the Information Commissioner issued a code of guidance for employers[67] in June 2003 (Dyer, 2003). The code advised employers

[67] <http://www.dataprotection.gov.uk/dpr/dpdoc.nsf> [Last accessed 5/7/2004].

that they must inform staff in advance if they intend to monitor their communications and employees must be told why the monitoring is being done. The code also recommended that employers carry out an audit to ensure that the benefits of monitoring outweigh the intrusion into privacy. Covert monitoring can only be justified in exceptional circumstances, such as the investigation of criminal conduct. In addition to compliance with the *Data Protection Act 1998* (Parliament, 1998b), employers should ensure that their monitoring and interception activities are in accordance with the *Regulation of Investigatory Powers Act 2000*[68] (Parliament, 2000a), the *Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000*[69] (Parliament, 2000b) and the *Human Rights Act 1998*[70] (Parliament, 1998a) (Information Commissioner, 2003).

A number of surveys have been conducted to determine the extent of monitoring of electronic communication carried out by UK employers. One example, carried out in June 2003 by Klegal and *Personnel Today,* found that 20% of firms carried out daily monitoring, and that disciplinary cases for email and Internet abuse at work in the previous twelve months exceeded the total of those for health and safety breaches, dishonesty and violence (Dyer, 2003).

3.6 EU and UK approaches compared – some conclusions

Regulation of the Internet has been shown to be a particularly problematic area in an already complex information policy arena. This study of some of the wide range of legislative and regulatory initiatives impacting on Internet content and access implemented at UK and EU levels demonstrates that the Internet is far from being an unregulated zone. On the contrary, it is subject to constraints imposed by a variety of legal instruments, technical architecture, self-regulatory mechanisms

[68] <http://www.hmso.gov.uk/acts/acts2000/20000023.htm> [Last accessed 5/7/2004]

[69] <http://www.hmso.gov.uk/si/si2000/20002699.htm> [Last accessed 5/7/2004]

[70] <http://www.hmso.gov.uk/acts/acts1998/19980042.htm> [Last accessed 5/7/2004]

and cultural norms; and of course, the ability to access network infrastructure. Policy measures implemented at both national and international level can be seen to have either a distributive purpose and effect (for example, the extension of network infrastructure); or a restrictive purpose and effect (for example, the implementation of filtering software).

Prior to the period under consideration, the main concerns of both national and international policy-making with regard to the Internet tended to focus on issues relating to infrastructure, regulation and deregulation of communications provision, and the obligations of service providers towards universal access. These concerns were driven primarily by the needs of commerce and promoting the competitivity of industry. Interest was also starting to be expressed in the potential offered by networked computer communications to areas such as lifelong learning, teleworking and enhancing citizenship. Where policies did address the regulation of content the overwhelming emphasis was on preventing access by minors to material with a sexual content, and the continuation – and indeed strengthening – of this emphasis was apparent in all regions in the subsequent policy study. However, there was already some evidence also of a broadening of scope, particularly with regard to the control of racist content.

The level of activity in developing and debating new initiatives within the EU in the period between 1996 and 1998 inclusive suggests that the issue of content regulation was high on the policy agenda of the EU. This is not surprising, as this was also the point in time when the media-generated 'moral panic' was at its zenith. However, the sheer volume of different initiatives that have followed, usually emanating from different Directorate Generals and with a different policy emphasis, has led to a fragmentation and lack of overall coherence that has arguably diluted the impact and effectiveness of the different measures.

The same fragmentation and lack of coherence is apparent in measures proposed and implemented within the UK. Indeed, approaches taken to the regulation of Internet content in the UK have closely mirrored those of the EU, in particular with regard to the priority given to self-regulation as a control mechanism. The

remit of the IWF reflects the action lines of the EU *Internet Action Plan*. Similarly, the priorities of the policy agenda at UK and EU levels have followed parallel lines, moving from an initial focus on developing infrastructure and technical expertise in order to promote economic growth and competitivity, to an increasing preoccupation with the control of illegal and harmful content; the promotion of a regulatory regime that aids the development of e-commerce; the promotion of social inclusion through access to Internet content; and finally to measures to fight crime and terrorism through communications traffic data retention, monitoring and interception. Where differences in approach have been identified, these have generally represented a subtle variation in the *balance* of priorities, for example the emphasis given in the EU to access to harmful content *by* minors, compared with a UK emphasis on the control of paedophiliac content.

In both policy arenas, difficulties and legal confusion can be seen to arise from the conflicting aims of legislative initiatives that aim to protect and promote information access, including the rights to privacy and to freedom of expression, and those whose primary aims are to control access to obscene or criminally racist content, or to fight crime and terrorism. Both the UK and the EU are hampered in this respect by the lack of an overarching, coherent information policy that could inform the priorities and balances of approaches to information access. There is evidence that content control is still a matter of concern to European and UK policy makers, particularly with regard to the notion of 'harm' to minors. Indeed the scope of content to be 'controlled' appears to be broadening, whilst the need to combat terrorism is being cited as justification for encroachments on the protection of privacy of electronic communication and online information access. Such measures promoting a more directive regulatory approach to the prevention of access to illegal and harmful content, to surveillance and to data retention are likely to conflict with the right to freedom of expression conferred through the European Convention on Human Rights (ECHR)[71] (Council of Europe, 1950).

[71] Relevant instruments of the ECHR are discussed in Chapter Four.

The policy issues that have presented themselves in the course of this study are further reflected in the investigations at Council of Europe level (presented in the next chapter) and those at institutional level with regard to HEIs (described in Chapters Five and Six). The interpretation and significance of these combined findings will be discussed in Chapter Seven, and final conclusions drawn together in Chapter Eight.

CHAPTER FOUR: THE COUNCIL OF EUROPE: PUBLIC ACCESS TO AND FREEDOM OF EXPRESSION IN NETWORKED INFORMATION: GUIDELINES FOR A EUROPEAN CULTURAL POLICY

4.1 Introduction

This chapter presents the findings of an investigation into policy formulation within the Council of Europe[72] with regard to public access to the Internet, and to freedom of expression in the online environment. Starting with some general background to the Council of Europe, and in particular to the relevant Articles of the *European Convention on Human Rights* (ECHR) (Council of Europe, 1950), it continues by outlining some of the characteristics of the Council of Europe's approaches to issues of freedom of expression. It then examines specific measures applied by the Council to regulation of the Internet, and illustrates this policy area by means of a case study of the formulation of *Guidelines for Public Access to and Freedom of Expression in Networked Information* (Sturges, 2000a). The author discusses her experience of involvement in this policy formulation through participation in an electronic consultation exercise and in an international conference attended by relevant policy makers.

Other relevant initiatives promulgated by the Council of Europe are also discussed, including the *Convention on Cybercrime* of 2001[73] (Council of Europe, 2001b). Although detailed consideration of the *Convention* is beyond the scope of this thesis, the relevant provisions that impact most directly on freedom of expression and freedom of access to information are analysed. A brief outline of the policy context in which the *Convention* was drafted and implemented is also provided, as it offers an interesting insight into the fragmentation, confusion and lack of

[72] <http://www.coe.int> [Last accessed 5/7/2004].

[73] <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm> [Last accessed 5/7/2004].

coherence that was found to be particularly characteristic of the Council's policy making processes.

4.2 Background to the Council of Europe

> *…although the Council of Europe has been eclipsed recently by the notoriety and clout of the European Union and its institutions, it remains the Continent's voice of conscience and carries immense moral authority on matters of its jurisdiction, primarily the monitoring and protection of human rights in member states and even beyond them.*
>
> (Baraschos, 1998, p.31)

The Council of Europe is not to be confused with the European Union (which, confusingly, has a body entitled the Council of the European Union): the Council of Europe is a quite separate and distinct organisation. Whereas the origins of the EU lay in economic co-operation, the Council of Europe had the protection and furtherance of human rights and fundamental freedoms at the core of its mission. The Council's stated aims are:

- To protect human rights, pluralist democracy and the rule of law;
- To promote awareness and encourage the development of Europe's cultural identity and diversity;
- To seek solutions to problems facing European society (such as discrimination against minorities, xenophobia, environmental protection);
- To help consolidate democratic stability in Europe by backing political, legislative and constitutional reform.

(Council of Europe, 2003a)

The Council does not, however, involve itself in military or defence matters, seeing these as the responsibility of NATO (Gomien et al, 1996).

The Council of Europe is an intergovernmental organisation, and any European state can become a member, provided 'it accepts the principle of the rule of law

and guarantees human rights and fundamental freedoms to everyone under its jurisdictions' (Council of Europe, 2003a; Gomien et al, 1996). There are currently 45 Member States[74]. The Council works towards achieving its fundamental aims through the adoption of conventions and recommendations; the dissemination of information about human rights; and the support of research in the area (Gomien et al, op cit, p.11).

It was founded in 1949, when the Treaty of London[75] establishing the Council of Europe was signed by the ten original founding member states. The following year, the *Convention for the Protection of Human Rights and Fundamental Freedoms*[76] (Council of Europe, 1950) was signed in Rome, as a legal instrument intended to guarantee civil and political rights. At the time of its founding, the Council decided to exclude economic, social and cultural rights from the Convention. According to Gomien et al (1996) this was in order to emphasise guarantees of respect for human rights, the rule of law and political democracy in a Europe that had been left devastated by war. It was also considered that some European countries were not yet in a position to implement full economic and social rights (Ibid). Robertson (1993, p.499) has suggested that its ideals were shaped by an awareness of the need for Western Europe to have in place a means of resistance against any future resurgence of fascism, as well as to strengthen those civil rights potentially endangered by the Communist regimes of Eastern Europe.

Economic and social rights were subsequently provided for via the *European Social Charter*[77] (Council of Europe, 1961), signed in Turin in 1961. Taken

[74] Correct as of August 2003. A list of Member States can be found at <http://www.coe.int/T/E/ Communication_and_Research/Contacts_with_the_public/About_Council_of_Europe/CoE_Map_ &_Members/> [Last accessed 8/8/2003].

[75] <http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm> [Last accessed 8/8/2003].

[76] More commonly referred to as the European Convention for the Protection of Human Rights (ECHR). Available at <http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm> [Last accessed 5/7/2004].

[77] <http://conventions.coe.int/Treaty/en/Treaties/Html/ 035.htm> [Last accessed 23/9/2004].

together, the Convention and the Social Charter provide a framework for a comprehensive guarantor to citizens of Council of Europe member states of most of the human rights set out in the Universal Declaration of Human Rights[78], as adopted by the United Nations in 1948. The Convention is enforced through the European Court of Human Rights, via a Commission on Human Rights and a Committee of Ministers. Any citizen of a member state who believes that his or her rights under the Convention have been infringed by a court ruling or by an administrative act, and who has exhausted all the possibilities of redress available through their national judicial system, may take their complaint to the European Court of Human Rights. Before the Court hears a case, the complaint must go before the Commission, which will gather and evaluate the facts of the case and present them to the Committee of Ministers or the Court. If an amicable solution cannot be found at the early stages, the Commission or the Council may refer the case to the Court, whose decisions are binding on member states. Of almost 26,000 cases petitioned to be heard by the Court between 1955 and 1998, approximately 1,900 only were deemed admissible for hearing and fewer than 500 were heard by the Court (Baraschos, 1998, p.45).

4.3 The Council of Europe and freedom of expression

The ECHR sets out a list of rights and freedoms that individual member states are obliged to guarantee to everyone within their jurisdiction. Thus, for example, in adopting the Convention in 1950 the Council of Europe guaranteed individual subjects of member states the right to freedom of expression. Article 10 of the Convention states:

1. *Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent states from requiring the licensing of broadcasting, television or cinema enterprises.*

[78] <http://www.un.org/Overview/rights.html> [Last accessed 5/7/2004].

2. *The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.*

(Council of Europe, 1950, Art.10, paragraphs 1 and 2)

Freedom of expression is thus not considered absolute, but is bound by duties and responsibilities towards both the national interest and the protection of the rights of others. However, any restrictions on Article 10 must meet all three conditions of prescription by law; the pursuit of a legitimate aim such as the prevention of crime or disorder; and necessity in a democratic society. Case law has demonstrated that the member states enjoy a certain 'margin of appreciation' in the interpretation of Paragraph 2, especially with regard to the 'protection of health or morals' as applied to restrictions on pornography and obscenity (Voorhof, 1995). However, it is for the European Court of Human Rights to determine whether measures taken at national level are justifiable in principle and proportionate. In the application of Paragraph 2, case law has demonstrated that judgement has depended less on the nature of the contested speech than on member states' justification for constraining that speech (Harris et al, 1995).

In addition to the restrictions imposed by paragraph 2, Article 15 of the ECHR permits member states derogation from the right of freedom of expression and information in times of war or other public emergency (Ibid). The freedom to publish and distribute materials inciting racial discrimination is also not protected by Article 10, and defamatory or blasphemous speech is afforded a lower level of protection (Ibid). Restrictions on freedom of expression and information may also be sanctioned under Article 6 (the right to a fair trial), for example on the grounds that media coverage may prejudice the opinions of jury members; Article 11 (the right to peaceful assembly); Article 16 (which permits restrictions on the political activities of foreigners); and Article 17, which prohibits reliance on Convention

rights where the aim is to subvert or destroy the freedoms that the Convention aims to secure.

Article 8 of the ECHR concerns an individual's right to privacy and family life as outlined in the following paragraphs:

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

2. *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

(Council of Europe, 1950, Article 8, paragraphs 1 and 2)

The Court has given recognition to the fact that there may be instances where member states have, to a limited extent, a positive obligation to interfere with the right to freedom of expression in order to protect the right to privacy under Article 8 of another individual, which may be violated by publications or revelations in the mass media. In such circumstances the State is expected to find a 'proper balance' between the two rights (Voorhof, 1995). To date, European Court of Human Rights case law has tended to give priority to the right to freedom of expression, recognising that, while privacy is important, freedom of expression is an essential safeguard of democracy (Travis and Dyer, 2000).

In addition to factual information, Article 10 provides protection for the expression of ideas, opinions and political speech. Information and ideas are given a particularly high level of protection when they are made public in the context of a political debate, on the grounds that freedom of expression in political and public debate 'is at the very core of the concept of a democratic society'[79]. This accords

[79] Lingens v. Austria, judgement of 8 July 1986, Series A, No.103, 8 EHHR 103 (1986), para.42, cited in Gomien et al (1996).

well with the Habermasian concept of promoting rational decision-making through conditions of 'ideal speech'. Particular attention has been paid to safeguarding the freedom of the press, which is seen as playing a vital role as 'public watchdog', and member states have been accorded very little margin of appreciation where restrictions on the press have been imposed (Copdel, 1999). Voorhof (1995) argues that Article 10 is particularly important for the protection of critical and non-conformist speech. This was clearly stated by the Court in the judgement of the case of Handyside[80] in 1976:

> *[Freedom of expression] is applicable not only to "information" or "ideas" that are favourably received or regarded as inoffensive or a matter of indifference, but also to those that offend, shock or disturb the state or any sector of the population. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no "democratic society".*
>
> (Cited in Gomien et al, 1996, p.274)

However, this level of tolerance may be lowered with consideration to the actual or intended readership of a publication, and the possible effect on that readership. This is especially true with regard to obscene or pornographic materials and their availability to minors. In the Handyside case cited above, despite the strength of the Court's defence of the principle of freedom of expression, the Court found in favour of the State's action in suppressing publication under the 'protection of morals' provision of Article 10, paragraph 2. Given that the publication in question, *The Little Red Schoolbook*, was specifically targeted at adolescents aged twelve to eighteen, the Court held that the nature of its content might have had harmful effects on the adolescents who would read it. The case was also instrumental in illustrating the importance placed by the Court on the margin of appreciation afforded to national states: the fact that the book had been published with impunity in a majority of member states did not preclude the necessity of restraining its publication in a minority of states if local circumstances justified this (Burnheim, 1997).

[80] Handyside v. United Kingdom, judgement of 7 December 1976, Series A, No. 24, 1 EHHR 737 (1979-1980), para.49.

Article One of the ECHR obliges member states to secure to everyone within their jurisdiction the rights and freedoms defined within the Convention. Case law has demonstrated clearly that this not only imposes an obligation on national governments to protect these rights, including that of freedom of expression, but also gives them a 'promotional obligation' to take positive action to ensure access to them[81] (Vitiello, 1997). Thus the state, in addition to not itself restricting freedom of expression in violation of Article 10,

> *…has a duty to secure the conditions which will ensure that the freedom of expression and information of the individual is not restricted by other private persons or private organisations in a way which violates Article 10 of the Convention.*
>
> (Voorhof, 1995, p.60)

The impact of the ECHR on protecting and enhancing civil liberties in the UK has arguably been much greater than any spontaneous national initiatives (Robertson, 1993, p.497). Between 1975 and 1993, prior to the adoption of the *Human Rights Act 1998* (Parliament, 1998a) which incorporated the provisions of the ECHR into UK law, over one hundred changes to UK laws, regulations and administrative practices could be attributed to actions brought against the Government under the Convention (Robertson, Ibid, p.500).

4.4 The Council of Europe and regulation of the Internet

In the mid 1990s the Council of Europe began to involve itself in policy formulation with regard to regulation of the Internet, at much the same time as the European Union was becoming active in this arena. The potential relevance of Article 10 in protecting freedom of expression on the Internet has been discussed by Sturges (1998) and Vitiello (1997), but as of April 2004 there remained a lack

[81] See for example VgT Verein Gegen Tierfabriken v Switzerland [Application 24699/94], judgement of 28 June 2001, para. 45. Available at <http://hudoc.echr.coe.int/hudoc/> [Last accessed 5/7/2004].

of established case law on its application to Internet content and access[82]. It is reasonable to presume that this will develop in future, as has happened in the United States with challenges brought under the First Amendment to legislation to control Internet access and content[83]. The period from 1996 onwards did, however, see considerable activity on the part of the Council in formulating a range of policies relating to control of Internet content and use, the most important of which are discussed in the following sections[84].

4.4.1 Media Recommendations

In October 1997 the Committee of Ministers adopted three recommendations, which focussed on the portrayal of violence in electronic media, the control of 'hate speech', and the promotion of a culture of tolerance, and which were directed towards the media[85] (Council of Europe, 1997a; 1997b; 1997c). With regard to the portrayal of violence in electronic media (Council of Europe, 1997a), the *Recommendation* laid down guidelines for member states to follow in acting to limit the gratuitous portrayal of violence whilst respecting the right to freedom of

[82] Judgements of the European Court of Human Rights can be searched and viewed at <http://www.echr.coe.int/Eng/Judgments.htm> [Last accessed 5/7/2004]

[83] For example, the successful challenge to provisions of the Communications Decency Act on the grounds that they were unconstitutional in outlawing speech protected by the First Amendment. For more about the case see <http://archive.aclu.org/issues/cyber/burning.html> [Last accessed 5/7/2004].

[84] *A note on terminology:* In order to clarify the following sections on Council of Europe policies towards regulation of the Internet, it would be helpful to provide a brief guide to the various regulatory instruments available to the Council, the most important of which are:
Conventions - These are legal instruments that are binding on member states that ratify them.
Declarations - Declarations announce policy directions, principles and intentions, and propose areas for future policy development. They are not legally binding instruments on member governments.
Recommendations - These are also not legally binding on member governments. The Committee of Ministers adopts Recommendations that are addressed to the governments of member states suggesting guidelines for national legislation or administrative practice.
Guidelines - These have the same legal status as recommendations for member governments, but do not require formal adoption by the Committee of Ministers, and may be directed at a wider audience, such as relevant professional organisations.

[85] Recommendations R (97) 19 - 21.

expression and information. It advocated a self-regulatory approach by the media, with the setting up of independent regulatory bodies in member states to which users can file complaints. It also highlighted the importance of education about electronic media, particularly in helping young people to develop a critical attitude to the portrayal of violence (Council of Europe, 1997d).

With regard to 'hate speech' the second *Recommendation* (Council of Europe, 1997b) contains guidelines for national governments' action against hate speech, including the need to develop an effective legal framework. In particular, this advocates stronger remedies in civil law for the victims of hate speech. Within the legal framework, however, member governments should 'make sure that any interference by public authorities with freedom of expression is extremely limited, that it is based on objective criteria and subject to judicial control' (Ibid).

The third *Recommendation* (Council of Europe, 1997c) stresses the positive role that the media can play in promoting awareness and appreciation of the diversity of the ethnic, social, cultural and religious groups that constitute society. Thus, the recommendation emphasises the importance of educating media personnel and adopting inclusive personnel recruitment policies to ensure balanced and diverse content.

Although these *Recommendations* were intended to provide a framework for the control of the portrayal of violence, the dissemination of 'hate speech' and the promotion of tolerance across all electronic media, including the 'new communications media', the wording of the *Recommendations* tends to focus on traditional media such as newspapers and television, although over time the increasing convergence of new and existing media may well render this distinction less important.

4.4.2 A Council of Europe Action Plan

Around the same time in June 1997 the Parliamentary Assembly of the Council of Europe adopted a *Recommendation on the scientific and technical aspects of the new information and communications technologies*[86] (Council of Europe, 1997e). This committed the Council to 'seeking common responses to the challenges and opportunities presented by the development of new information technologies'. Notably, the Assembly recommended that the Committee of Ministers support and reinforce the work regarding the impact of the new technologies on human rights and democratic values of the European Ministerial Conference on Mass Media Policy, who were due to meet in December 1997. At this meeting, which was held in Thessaloniki, Media Ministers passed Resolutions and approved an *Action Plan* 'to familiarise the public with the new Communications Technologies and to check misuse of their services' (Council of Europe, 1997f). The Conference resolutions expressed concern about the use of technology by those who promote violence and intolerance, and who lack respect for human dignity (Sturges, 2000b).

As with the EU *Action plan on safe use of the Internet* (European Commission, 1997a), the Council of Europe Plan emphasised the need for self-regulation, universal access to network services, public education and awareness, and the adaptation of national legislation to the demands of new technologies. In line with the Media *Recommendations* outlined above on the portrayal of violence and the control of 'hate speech', the Ministerial Conference pledged to combat the use of network services to disseminate hate speech and pornography. The balance of emphasis of the Council of Europe plan is however on freedom of expression in the networked environment rather than on safe use of the Internet, in contrast to the EU *Action Plan* (Sturges, 1998a). This supports the Council's claim that, for the Council, the highest importance is placed on the guarantee of freedom of expression in the new services and the need to avoid any interference by public

[86] Recommendation 1332 (1997), adopted 23rd June 1997. Available at <http://assembly.coe.int/documents/adoptedtext/ta97/erec1332.htm> [Last accessed 5/7/2004].

authorities beyond that which is permitted under the ECHR (Council of Europe, 1997f).

4.4.3 Freedom of expression and communications networks

As part of its commitment to the promotion of public access to information and freedom of expression, and the recognition of the importance of new information technologies as a means to enhance this access, the Council of Europe's Culture Committee appointed a consultant to prepare a report on *Freedom of expression and the communications networks*[87]. Drafted in December 1997 by Prof. Paul Sturges of the Department of Information Science at Loughborough University, the resulting report was accepted by the Culture Committee in October 1998. Endorsing the Council of Europe's commitment to the notion of 'universal community service' as a guiding principle, the report gives strong emphasis to the positive aspects and democratising potential of the Internet. This is set in the context of a discussion of the early years of the panic-induced Internet debate and the policy responses to this debate.

The report analyses potential approaches to address the issues and fears emanating from access to Internet content through legislative, technical and ethical means. The adoption of new legislation as a solution is rejected on the grounds both of the potential impact on freedom of expression and the difficulty of implementation, particularly when issues of jurisdiction are taken into account. Technical measures such as filtering and blocking are not regarded as a fully acceptable solution either, although recognition is given to their potential, if limited, value in specific circumstances: for example, if they are freely chosen by end users to control their own use or that of children in their care.

[87] Available at <http://www.coe.int/T/E/Cultural_Co-operation/culture/Completed_projects/NIT/Sturges98_18.asp#TopOfPage > [Last accessed 5/7/2004].

Instead the report favours the adoption of ethical approaches such as self-regulation based on codes of practice, and the promotion of user education. In particular, it is suggested that the Council of Europe develop a Charter or Recommendation on 'Self-regulation of the Networked Information Environment'. According to Sturges, this would set out the ways in which national governments could facilitate effective self-regulation, and would clarify the roles and responsibilities of different stakeholders, such as industry and user organisations, end users, legislative bodies and law enforcement agencies (Sturges, 1998a). The ideas expressed in the report were disseminated and debated in a variety of professional settings, including conferences sponsored by the Council of Europe throughout 1998 in Budapest, Oslo, Riga and Strasbourg. Comments made on those occasions were subsequently incorporated into the draft 'Helsinki Charter', discussed below.

4.4.4 Public access to and freedom of expression in networked information

The advice to prepare a 'Charter' was taken up by the Council and progressed through the 'Public access and freedom of expression' working strand of the Culture Committee's New Information Technologies programme. Prof. Sturges was requested to prepare a draft Charter for consultation. This initial draft was prepared in consultation with colleagues and relevant professional contacts, and the draft was circulated for informal review to a number of individuals (including the author of this thesis) in September 1998. The draft was then presented at the 17th meeting of the Council's Culture Committee in April 1999. The formal consultation procedure of the subsequent revised draft involved an electronic consultation process with relevant professional bodies and individuals; an international Conference, at which it was to be debated; and the formal Council of Europe committee ratification procedures. This consultation process is discussed in greater detail in the following sections.

4.4.4.1 The draft 'Helsinki Charter'

Focussing primarily on issues related to the provision of public access to the Internet, the draft Charter that was submitted for the electronic consultation exercise[88] had at this point the formal status of a draft *Recommendation*[89] to member states. It was referred to at this time by the Council as the '*Helsinki Charter*' after the location of the Conference at which it was to be debated. Its guiding principle was clear from the preliminary outline of scope, which included the statement that

> *The Charter's concern is that a widespread desire, both official and popular, to eradicate illegal content and avoid distasteful and possibly harmful content should not be allowed to damage full and free access by all users of public access points to any legal content they choose.*

The draft endorsed the principle of free (in the sense of being unrestricted) and universal access to networked information within the limits of the law, and that decisions on what content to access should rest firmly with the end user. In particular, young people should not be subject to any restrictions that are not applied to the community as a whole, although they should be warned in advance of the potential risks of online contacts made with other users. The staff of Public Access Points should not assume the responsibilities of an 'in loco parentis' role.

The draft does recognise that some specialised institutions, such as schools or HEIs, may need to impose some limits on access for practical reasons. Thus, for example, they may need to limit access to content and use that is not relevant to

---

[88] Included in the thesis as Appendix Six.

[89] Although the 'Charter' was originally envisaged as having the status of Recommendation, this was subsequently amended to the status of Guidelines. In addition, it was envisaged at one point that it would be entitled the Helsinki Charter, although this nomenclature did not endure. For the purposes of this thesis, the author has used whichever terminology was current at the point in the document's life cycle that is being written about.

the institution's aims and objectives, or which may hinder the institution's ability to serve users pursuing the primary purposes of the institution.

Attention is paid to the principles of providing a properly managed and staffed environment for public access to networked information in order to create a positive and supportive atmosphere. This includes the responsibilities of staff for identifying and facilitating access to quality networked information, particularly for young people, for example through the creation of gateway pages. Whilst staff of Public Access Points have a duty to request that users accessing illegal content should discontinue such access, whenever they are made aware of such use, they should not invade users' privacy by exercising general oversight of what content users are accessing. Wherever intervention in an individual's use has been deemed necessary, this should be carried out according to a predetermined procedure, and should be subject to immediate review so as to assess any further action that might be needed. The layout of Access Points should be designed to minimise the disturbance to other users of access to 'disturbing' (but legal) content, including image and sound files. This may, in some instances, require that users be prevented from making such access.

The use of filtering software to block access to content is described as 'an unwarranted interference with the individual's freedom of access to information' and should not be applied at Public Access Points, unless explicitly required by law. However, the use of 'recommender' software packages to filter for positively evaluated networked content is considered to be of value and to be encouraged at Public Access Points. Rating or labelling is seen as facilitating this 'recommendation' process with an appropriate metadata platform, such as PICS, being used to obtain ratings data about a site. Staff should alert users to the existence of warning pages that are attached to many sites containing disturbing content. In particular, the existence of these warning pages and of age verification schemes attached to some controversial content should be drawn to the attention of parents anxious about their children' access to such content.

Institutions responsible for providing Public Access Points should have a clearly articulated Internet Use Policy, which should be communicated to users by public display. In developing Internet Use Policies, Public Access Point managers should involve relevant bodies (such as professional associations, trade unions and library advisory boards). They should also seek guidance from existing Internet Use Policies, guidelines and 'netiquette' codes. According to the draft, Internet Use Policies should include clear statements on matters such as access to illegal content and the use of workstations for other illegal activities, and on the need to exercise consideration towards other users. Access policies should respect user rights, including the right of privacy.

4.4.4.2 The electronic consultation

The draft Charter as described above was made available on the Council of Europe website for consultation in May 1999. Although the electronic consultation period was originally scheduled to take place between 29th March 1999 and May 21st 1999, technical delays meant that the draft was not made available for consultation until mid-May. This had the effect of seriously curtailing the opportunity for interested bodies to respond to the draft. This restriction on the opportunity to participate in the consultation was exacerbated by the inability of the Council to rectify problems with the technical operation of the consultation website, further inhibiting the ability of interested parties to submit their responses.

Once the draft was available on the Council consultation site the researcher drew the attention of subscribers to relevant UK electronic mailing lists to its presence. On 14th May 1999 the following notice was posted on the Internet:

Subject: Freedom of Expression and Public Access to the Internet

Apologies for cross-posting.

Please forward this message to other relevant groups/individuals/lists.

The Council of Europe has commissioned a draft Charter on public access and freedom of expression in the networked environment. The Charter is intended to provide guidance for the managers of public access points, the governing bodies to which those managers report, and the Governments which lay down the policy frameworks within which public access is provided. Consultation on the draft Charter is currently taking place, and it is hoped that comments will be received from actual or potential public access point users, those with a professional, business or civil interest in the provision of public access, and by anyone else responsible for providing or managing public access points. Comments will be used to further develop the Charter, so that it can be accepted as Council of Europe policy.

The draft Charter and opportunities to comment can be found at: http://culture.coe.fr/postsummit/nti/en/project/helsinki/edraft_charter.htm

Please take the time to view the draft and provide feedback in order that the widest possible consultation may take place.

The lists to which the message was posted were chosen on the basis of the researcher's professional awareness, together with scanning of the description of UK academic mailing lists available on the mailbase web site[90]. They included:

[90]<http:// www.mailbase.ac.uk> [currently hosted at http://www.jiscmail.ac.uk, last accessed 5/7/2004]

List Name	*Description*[91]
lis-link	Library and Information Science news and discussion
pin [Policing the Internet]	For those interested in ethical, moral and political responsibilities related to the development of interactive information and communication technologies in UK Higher Education
lis-pub-libs	For discussion of topics of general interest (with a particular focus on networked services) to public librarians in the UK and elsewhere
itsupport	For staff involved in supporting IT in the UK academic community and beyond
dc-general	For discussion of all issues relevant to the development, deployment, and use of Dublin Core metadata.
lis-bailer	Discussion group for lecturers and research staff in Departments of Information and Library Studies in the UK
lis-fid[92]	To promote discussion of Information Management and Library and Information Science in an international context
lis-european-programmes	A forum for sharing information on all aspects of European programmes, projects and funding opportunities of interest to the UK LIS sector

Table 4.1: Consultation Mailing Lists

The draft Charter that was posted on the consultation website allowed respondents to comment in a hyper-linked textbox on each section of the Charter under the headings:

[91] from that provided at <http://www.jiscmail.ac.uk> [Last accessed 5/7/2004]

[92] International Federation for Information and Documentation

- General comments
- Principles of access
- Young people's access
- Access in specialised institutions
- Management of public access points
- Disruptive use
- Filtering
- Content rating
- Warning pages
- Internet Use Policies

Contributors were expected to abide by three basic rules of participation, namely: taking responsibility for the content and accuracy of any information posted; keeping responses relevant to the topic; and not straying beyond the limits of civil discourse.

It was intended that the views of participants responding to the consultation would be moderated and posted at 48-hour intervals in the forum section of the consultation site, and that these views would subsequently be part of the programme of the Helsinki Conference. In the event, the combination of late posting of the consultation draft and technical problems with the consultation site meant that very few attempts were made by organisations to respond, and when attempts were made respondents were unable to post successfully.

However, researchers at the Centre for Computing and Social Responsibility (CCSR) at De Montfort University, UK[93], having tried unsuccessfully to use the consultation site to post comments, made direct email contact with the researcher in order to input into the consultation. Their response made the following observations:

[93] <http://www.ccsr.cse.dmu.ac.uk> [Last accessed 5/7/2004]

Principles of access

"…one of the principles of access should be privacy. Users should be able to access whatever materials they choose without being monitored or records being kept of what they access unless there is prior evidence from another source that their activities violate the law or policies consistent with this Charter to protect the network or safeguard resources for the purpose for which they were allocated."

This comment was incorporated into the final version of the Charter, with paragraph 1.3 stating that 'Those providing Public Access Points should respect the privacy of users and treat knowledge of what they have accessed or wish to access as confidential'.

Young people's access

[Para. 2.3] "…mainstream schooling should integrally include education for all children on how to avoid being preyed upon, including in networked contexts."

Although this statement was not included in its precise meaning, it did lead to a revised paragraph 2.4. Although the role of *parents* in alerting their children to the potential risks of online contacts made with strangers is emphasised, the paragraph now contains the statement that 'Parental warnings about online contact with strangers should be reinforced as part of the education and training processes.'

Access in specialised institutions

[Para. 3.2] "We are pleased that there is recognition of the need of specialised institutions to restrict use that might 'hinder the institution's ability to serve users pursuing its primary purposes'. However, we are anxious that specialised institutions do not impose limits on access *beyond the extent needed* to ensure that resources are committed to their primary purpose…'

This suggestion was incorporated directly into the final draft, which now includes a new paragraph 3.3 that reads 'Specialised institutions should not, however, impose limitations beyond the extent needed to ensure resources are committed to their primary purpose'.

Management of Public Access Points

[4.3] "…it is not appropriate for great reliance to be placed on commercial gateway pages and sources of information when non-commercial sources are available, and thus that any gateway pages created should take this into account."

This comment was not explicitly stated in the revised draft, as the original wording of paragraph 4.3 already stated that 'The staff of Public Access Points should be pro-active in identifying and facilitating public access to quality networked information content, particularly for young people. It is appropriate for information professionals to create gateway pages for this purpose'. This statement, which subsequently became paragraph 4.4 in the revised draft, was felt to elucidate clearly the principle that it was not intended that gateway pages would be based on commercial sources.

Disruptive use

[Para. 5.1] "We are concerned that the current wording of this clause does not say anything about staff monitoring use for no reason beyond nosiness. Thus we would be anxious that the final sentence of 5.1 is re-worded to read 'However it would be an unwarranted invasion of users' privacy for staff to monitor the nature of the content accessed unless there is pre-existing good reason to suppose illegal content is being accessed (or access in a specialised institution is taking resources from the primary purpose of the institution)'.

In this instance, the final draft did not incorporate this comment, but retained the original less emphatic wording. Thus in the revised draft, paragraph 5.2 contained the statement that 'Staff *should not be required to* [researcher's italics] exercise general supervision of usage with the express intention of identifying the use of illegal or otherwise distasteful content'.

Filtering

[6.2] "We encourage the use of recommender systems, but only provided there is no commercial bias in such recommendations".

This statement did not lead to an alteration of the wording used in the revised Charter.

Warning pages

[8.1, 8.2] "We have read reports of disturbing content being accidentally accessed without warning pages: we consider it important that staff do not discount or unduly downplay this possibility".

This comment led to a revised statement (paragraph 6.5 in the final draft) that 'When assisting users, the staff of Public Access Points should be prepared to draw their attention to the warning pages attached to many sites that contain controversial content, but should make it clear that not all such sites carry warning pages'.

Internet Use Policies

[9.1-9.5] "We are anxious that all such policies should be consistent with this Charter".

This comment led to the insertion of the phrase 'consistent with the principles of this text' into paragraph 7.1 of the revised Charter, which now reads 'A Public Access Point should be operated within a clearly articulated and publicly available policy, *consistent with the principles of this text* [researcher's italics], and expressing the balance of responsibilities between staff and users.

Other issues

The CCSR response also voiced concerns about the potential for age verification systems 'exposing individual subscribers to the potential of fraud, if they are not operated by companies that have a high reputation in other spheres that they wish to maintain'.

This led to the insertion of paragraph 6.6 into the final draft, which read 'The age verification systems attached to some sites with controversial content also warn

users that they might wish to avoid such content, but users should be made aware of the risks associated with supplying personal data to such systems if they are not operated by reputable organisations'.

It can be seen that not all of the suggestions were incorporated into the final draft: this was on account of the need to balance these comments with the outcome of subsequent debate at the Helsinki Conference. However, the CCSR response clearly made a useful contribution to the process of drafting the final Charter. The emphasis that CCSR placed on privacy rights, for example, together with the weight given to protecting professional values and judgement over commercial interest, influenced the wording of the final draft. The value of this contribution illustrates the fact that it was very regrettable that the consultation process was so fraught with practical and bureaucratic difficulties, thus preventing other contributions.

The willingness of the draft's author to take account of suggestions for changes of wording, and the readiness of information professionals to offer their expertise to the formulation of the guidelines, are an indication of the strong potential of the use of electronic consultation mechanisms. However, this exercise also illustrated the crucial importance of ensuring effective management of the process, with the use of robust technical systems and an appropriate timeframe to allow for the resolution of difficulties encountered.

4.4.4.3 The Helsinki Conference

The next stage in the consultation process was the presentation and discussion of the Charter at a Conference entitled *Public access and freedom of expression in cultural institutions* that was held in Helsinki, 10th –11th June 1999. Although the problems experienced with the electronic consultation exercise limited its usefulness in practice, the Conference afforded the opportunity for a much wider range of individuals and organisations to contribute their ideas and opinions on the Charter (although given that these individuals and organisations were selected and

invited by the Council, there was the possibility of an element of bias being introduced into the exercise).

The Conference was co-organised by the Finnish Ministry of Education and Culture, the Council of Europe and the Nordic Council of Ministers. In its broadest aims, the Conference was intended 'to provide a forum for debate and exchange of experience on the implications of the digital era for public access to and freedom of expression in networked information in the cultural sector' (Council of Europe, 1999a).

In addition to submitting the Charter to the Conference for debate and validation, the Conference also aspired to explore questions such as:

- How can society capitalise on the opportunities offered by new information technologies to improve both access to and freedom of expression in networked information?
- How to develop policy that promotes access to and freedom of expression in networked information?
- How to avoid incurring payment for access to networked information such that a digital divide is engendered that will inhibit the participation of some citizens in the democratic process?

As well as members of the Council of Europe's Cultural Policy and Action Division, the Conference was attended by representatives of the governments of Council of Europe member states, representatives of cultural institutions, industry representatives, academics, and a wide range of invited experts. These included the Director of the IFLA Committee on Free Access to Information and Freedom of Expression (FAIFE)[94] and the Acting Chief Executive of the UK Internet Watch Foundation (IWF).

[94] <http://www.ifla.org/faife/index.htm> [Last accessed 5/7/2004]

The Charter was discussed in a range of sessions relating to different aspects of the provision of public access to the Internet and freedom of expression, in addition to special sessions held specifically to present and debate the content of the Charter. In presenting here the substance of the comments made during these discussions, the following typology has been used:

- Responses favouring less restrictive or more liberalising approaches to access to networked information;
- Responses favouring more restrictive approaches to access to networked information;
- Responses seeking to broaden the scope of the content of the Charter;
- Responses concerned with clarity of definition of terms or concepts;
- Responses seeking to amend the emphasis of the Charter with regard to specific domains.

These are potentially subjective categories, and in some instances there will be overlap between them (for instance, comments advocating the duty of governments to promote cultural diversity could be regarded as a liberalising approach *and* a call to broaden the scope of the Charter). In such instances judgement has been exercised and the comment placed in the most obviously appropriate category. Wherever possible, the comments have been attributed to the delegate putting forward the comment.

Responses promoting less restrictive or more liberal approaches to access to networked information

- FAIFE condemns *any* attempts by governments to censor the Internet (FAIFE representative); all censorship should be opposed on the grounds that it is wrong to impose our own views about content onto others (representative from Portugal);
- In accordance with the UN Convention on the Rights of the Child[95], Article 13, the Charter's approach advocating the same right to information on the

[95] Available at <http://www.unhchr.ch/html/menu3/b/k2crc.htm> [Last accessed 5/7/2004].

part of children as adults is welcome; it is considered better to discuss appropriate use with children rather than rely on published warnings (representative from the Public Libraries Association in the Netherlands);

- Emphasis on the role of education, information and guidance in the provision of Internet access for children is welcome (UK IWF representative);
- Self-rating by content providers and self-selection by users is an appropriate means of addressing the access of 'harmful' content (UK IWF representative);
- The importance of the role of privacy and confidentiality in promoting freedom of expression should be stressed (representative from Portugal);
- The Charter should build on existing ethical approaches to the Internet such as 'codes of netiquette' (UK IWF representative);
- Section 5.1 (on disruptive use) should be rephrased more positively with the emphasis on encouraging a 'decent' environment – it is questionable whether the staff of Public Access Points should take on the value-laden role of 'policing' use. Alternatively it should be removed altogether as differing legislative regimes make 'illegal' content very difficult to define (delegate from McLuhan Program in Culture and Technology, University of Toronto, Canada).

Responses promoting more restrictive approaches to access to networked information

- A regulatory approach rather than a self-regulatory approach is required where access to the Internet by children is concerned (representatives from Italy, Slovakia);
- It is not appropriate that cultural institutions should have a duty to provide access, and therefore the wording of 1.1 of the draft Charter should read 'should not hinder access' rather than 'should provide access' (representative from Slovakia);
- Unrestricted access is a noble aim, but a distinction needs to be drawn between different types of cultural institutions: in cultural institutions that

are funded by public money, there is a *duty* to make a human judgement about networked material, in the same way that librarians select books for their collections (representative from Romania);

- There is a need to make a distinction between Public Access Points in general areas and those in specifically child-oriented spaces, which should use positive filtering based on quality of content (UK IWF representative);
- Media convergence could make it more appropriate to adopt the same regulatory instruments for the Internet as for other media (UK IWF representative, representative from Italy).

Responses seeking to broaden the scope of the content of the Charter

- Governments should have a *duty* to make citizenship information available to all on the Internet; the Charter should define the range of compulsory information governments should make available on the Internet (several representatives made comments similar to these);
- Governments should have a duty to provide access to government information free of charge, and to provide access to networked information free of charge in schools (representative from Hungary);
- Cultural institutions should have a duty to maximise cultural content and to make cultural material available through digitisation (representative from Romania);
- In addition to Article 13 of the UN Convention on the Rights of the Child (the right to freedom of expression, including the freedom to seek, receive and impart information and ideas of all kinds), the Preamble should make reference to Article 17, the right of children to access to information and material from a diversity of national and international sources (FAIFE representative);
- The Charter should emphasise the right of children to education and competence, and the right to discover new information and ideas for themselves (representative from the Netherlands Public Libraries Association);

- The Charter should stress the rights of users to education and literacy (representative from Slovakia);
- Governments should have a duty to promote electronic literacy (representative from Hungary); staff of Public Access Points have a duty to promote electronic literacy, especially with regard to older users (delegate from McLuhan Program in Culture and Technology, University of Toronto, Canada);
- Public provision of access to the Internet should extend beyond cultural and educational institutions, and into areas such as pubs, factories, launderettes etc. (UK IWF representative, delegate from McLuhan Program in Culture and Technology, University of Toronto, Canada);
- The Charter needs a positive statement on the importance of making culturally specific material available, the encouragement of diversity and the widening of access through greater universal affordability, availability and usability (delegate from McLuhan Program in Culture and Technology, University of Toronto, Canada).

Responses concerned with clarity or appropriateness of definition of terms or concepts

- Recommendations to governments of member states (ii) should read 'to *encourage* that self-regulation of public access points is genuinely possible…' rather than 'to *ensure…*';
- The definition of Public Access Points should explicitly include local government specialised institutions;
- 'Principles of Access' (Section One) should be entitled 'Principles of Public Access';
- Principles of Access 1.1 should explicitly include educational institutions (representative from Hungary); the Title of the Charter does not reflect the inclusion of educational institutions (Council of Europe representative);
- Principles of Access 1.3 ('access to networks should not be denied, or content excluded from access, on any ground other than the law in force')

is problematic – what about unjust laws? Whose law should be taken into consideration? (Council of Europe representative);

- The Preamble should make reference to the UNESCO recommendation on the protection of artists' work, and therefore a statement on the responsibility to improve the conditions of artists' working lives should be included (representative from UNESCO);
- The recommendations to governments of member states (iii) (iv) (v), which all relate to the development of technical measures, should be amalgamated into a single recommendation (representative from the Netherlands' Public Libraries Association).

Responses seeking to amend the emphasis of the Charter with regard to specific domains

- The prominence of libraries as cultural institutions should be made more explicit (Slovakian representative);
- The emphasis should be on the responsibilities of the staff of Public Access Points to educate the public in order to encourage responsible use of networked information for the benefit of communities;
- The emphasis of the Charter needs to be on the positive aspects of public access to the Internet and its democratising potential (comment made by representatives from the Netherlands, Canada and Finland);
- The emphasis of the Charter should be on items related to the avoidance of censorship, in accordance with the principles of the UNESCO Public Libraries Manifesto[96] that states that public library collections and services should not be subject to any censorship. These principles are equally valid in relation to new information technologies (FAIFE representative);
- The Charter should be seen as a *political* document, that forces governments to take action to combat social exclusion by promoting equal access to networked information (representative from Hungary).

[96] Available at <http://www.ifla.org/documents/libraries/policies/unesco.htm> [Last accessed 5/7/2004]

During debate at the conference a majority of delegates focussed on emphasising the value of a commitment to human rights, freedom of expression and a 'values-driven' democratic model of the information society. At the same time, a significant minority of delegates expressed serious concern at the suggestion of unsupervised and unfiltered access by minors: the clauses on children's access were those that provoked the most heated debate. The guidelines sought to treat children as individuals with the same rights to information as adults, and stressed parental guidance supported by education, guidance and training for both parents and children, as paramount. However, there was a strong lobby for legislation and the implementation of filtering software to limit use of the Internet by minors. Strenuous calls were also made to broaden the scope of the Charter, for instance to encompass broader issues of social exclusion, educational policy, freedom of information and cultural diversity.

The comments made in the course of the Conference debates with regard to the Charter were collated by the researcher, together with those made by the CCSR in the course of the electronic consultation, and sent to Prof. Sturges (Appendix Seven). The Charter was subsequently redrafted and the revised draft submitted to the Culture Committee for approval in October 1999. Further suggestions as a result of this submission were incorporated into subsequent drafts. It was also agreed that the 'Charter' would have the status of "guidelines" rather than "recommendation": it was felt that the rapidly changing context of developments in information technologies made it most appropriate to offer guidance to policy makers, politicians and professionals in drafting legislation or governmental policies. Thus, the guidelines do not have a binding character or legal implications for member states. They were finally approved by the Culture Committee at their meeting in March 2000 and by the Council for Cultural Co-operation in May 2000.

The original draft Charter submitted for debate in the Conference and the final approved text of the Guidelines have been appended to this thesis (Appendices Six and Nine) so that readers may view for themselves the detail of differences in wording, emphasis and tone of the two documents. Although the researcher was unable to attend the October 1999 meeting of the Culture Committee at which the

revised draft was discussed, changes arising from that meeting are outlined in Appendix Eight, together with some rationale for the inclusion or omission of suggested changes.

A summary of the main substance of changes that occurred between the original consultation draft, and that finally approved in May 2000 is provided below, organised according to the section heading of the final document in which the changes have been incorporated.

Introduction

An explanatory introduction has been included in the final draft to further clarify the purpose and scope of the draft, as well as to outline the guiding principles of freedom of expression, universal access and self-regulation that underpin the initiative. In addition, the references have been expanded to include the incorporation of the Council of Europe *Declaration on a European Policy for New Information Technologies* (1999)[97]; the European Union *Action Plan on Promoting Safe Use of the Internet* (1999); and the United *Nations' Universal Declaration of Human Rights* (1945), Article 19. The reference to the *ECHR* was expanded to include Article 14 (the prohibition of discrimination) in addition to Article 10 (the right to freedom of expression), and the reference to the United Nations' *Convention on the Rights of the Child* (1989) was expanded to include reference to Article 17 (the right of the child to access to material and information from a diversity of national and cultural sources) in addition to Article 13 (the right to freedom of expression).

Definitions

The main changes made to the definitions provided to aid understanding and clarity of the guidelines are as follows:

[97] Available at < http://cm.coe.int/ta/decl/1999/99dec3.htm > [Last accessed 5/7/2004]

Cultural institutions This definition has been extended to clarify the inclusion of relevant institutions that are funded by central government, local government or Non-Governmental Organisations (NGOs). The definition has also been expanded to include, in particular circumstances, certain publicly- or privately-funded educational institutions (these were previously included under a separate definition).

Free access The definition of content to which the provisions of free access apply has changed from that which is 'subject to no restrictions other than those set out in the laws in force in the relevant jurisdictions' to that which is 'subject to no restrictions other than those recognised as acceptable by the international conventions cited in the introduction to these guidelines'.

Illegal content The revised definition of illegal content does not make reference to content prohibited by reference to laws governing official secrecy, but has added a reference to content protected by laws on confidentiality.

Public Access Points This has been expanded to explicitly include networked workstations made available for public access for educational purposes, in addition to those provided for cultural, leisure or professional purposes.

Telecentres A note has been added to this definition to highlight the fact that the primary purpose of such centres is economic rather than cultural.

Section One: Principles of public access

The heading for this section now includes the insertion of the term 'public' in order to offer greater clarification of its scope.

The wording of the first clause in this section (1.1 in both versions) has been amended to read 'Cultural institutions providing public access to networked information and communication should do so for all, without regard to…' instead

of ‘cultural institutions should provide public access to networked information and communication to all, without regard to…’. This removes the possibility of inferring from the text that all cultural institutions have an onus to provide public access to networked information and communication. In addition, ‘age’ has been removed from the list of unacceptable exclusion characteristics.

The wording of 1.2 in the final version (1.4 in the earlier draft) has been amended to read that it is ‘the *responsibility* [researcher’s italics] of individuals…to decide for themselves what they should, or should not, access’. The previous version read that it is ‘the *right* [researcher’s italics] of individuals… to decide for themselves what they should, or should not, access’.

The revised draft includes the insertion of three new clauses. The first one (1.3) puts an onus on Public Access Point providers to ‘respect the privacy of users and to treat knowledge of what they have accessed or wish to access as confidential’. The second new clause (1.4) adds an obligation onto Public Access Point providers to ‘provide assistance for everyone to acquire the skills required to use such services’. Finally, 1.5 places a responsibility onto Public Access Point providers to promote access to information content generated by local, regional and national public authorities ‘in the interests of an informed citizenry and a healthy democratic process’.

However, two clauses from the original version have been removed from the final draft. The first deleted clause (1.2 in the original) read ‘The principles of universal and free (in the sense of unrestricted) access to information which have been developed to apply to books and other documents in libraries and archives apply equally strongly to access to networked information’. Clause 1.3 in the original version, which has now also been deleted, stated that ‘Access to networks should not be denied, or content excluded from access on any grounds other than the law in force’.

Section Two: Children's access

The heading for this section has been changed from 'Young People's Access' to 'Children's Access' on the grounds that the latter refers more precisely to minors, whereas the former could include those of up to around 25 years of age.

The wording of the first clause of this section (2.1 in both versions) has been altered in such a way as to significantly dilute the original emphasis on the rights of children to full access to networked content. Thus, whereas the original clause read 'No restrictions should be applied to the use of Public Access Points by young people other than those applied to the community as a whole', it now reads 'Children choosing to use those Public Access Points that are provided for whole community use should, *as far as possible* [researcher's italics], be able to do so under the same conditions as other users. Nevertheless, in order to avoid access to harmful and/or illegal content, filtering systems requesting the use of personal age codes should be provided at Public Access Points'.

Clause 2.2 in the earlier draft has also been reworded to reflect a change in emphasis. The original clause read 'The staff of Public Access Points should not assume an 'in loco parentis' role which would require them to anticipate the advice parents might or might not give their children about particular information content'. This has been rephrased as clause 2.3 in the new version to read 'Although it is the responsibility of parents to advise their children about choices in the use of networked information and communication, the staff of Public Access Points should provide guidance for children'.

Similarly, clause 2.3 in the original draft has been reworded, this time placing a stronger onus on parents, rather than information professionals, for educating children about responsible use. The original clause 2.3 read '…because the Internet offers real time communication, as well as access to stored information, information professionals should be prepared to warn young people about the potential risks of online contacts made with other users'. In the revised version, clause 2.4 reads 'Because networks offer real time communication, as well as

access to stored information, parents should take particular trouble to advise their children about the potential risks of online contacts made with strangers. Parental warnings about online contact…should be reinforced as part of the education and training processes'.

Two new clauses have also been added to this section, both concerned with the obligations of Public Access Point providers as intermediaries and educators for children using their facilities. Thus 2.2 states that 'Children have a right to expect that Public Access Points will provide instruction and assistance in developing those skills which will enable them to become confident and capable users'. In a similar vein, 2.5 states that 'Access points provided specifically for children should provide them with levels of guidance and assistance in locating content appropriate to their needs'.

Section Three: Access in specialised institutions

This section now contains an additional clause (3.1) pertaining to the particular responsibility of specialised institutions to develop and digitise content in their fields, and to promote access to that content.

The original two clauses in this section have also been expanded, primarily to afford greater clarity and specification to the nature of restrictions to access that they may impose. Thus, for example, 3.2 now reads that it may be necessary for such institutions 'to develop a policy which confines the permitted range of access to that which is relevant to the institution's aims and objectives…'. This contrasts with the original wording that merely stated that it may be necessary for such institutions 'to impose some limits for practical reasons'. Moreover, the revised clause imposes a duty on such institutions to make users aware of any restrictions imposed 'by the public display of the relevant policy statements'.

Similarly, the revised clause 3.3 imposes a more clearly defined limit on restrictions to access in such institutions. Whereas the original clause merely

limited the *grounds* on which limitations may be imposed (that is, the need to commit their resources to the service of their primary purposes), the revised clause also limits the *extent* of limitations, which should not exceed 'beyond the extent needed to ensure resources are committed to their primary purposes'.

Section Four: Management of Public Access Points

With regard to the management of Public Access Points a new clause (4.2) has been inserted to highlight the responsibility of those responsible for the education and training of information professionals to 'ensure that the programmes they provide contain elements designed to produce well-prepared managers and staff for Public Access Points'. In addition the wording of the original clause 4.2 (now 4.3) has been amended slightly for greater clarity. In the original clause it was noted that the management and staff of Public Access Points have a responsibility 'to facilitate public access to networked information and communication so that individual users *are in a position* [researcher's italics] to make their choices freely and confidently'. This now reads '…so that individual users *have the necessary skills and a suitable environment in which* [researcher's italics] to make their choices freely and confidently'.

Section Five: Disruptive use

Significant revision has been made to the wording of the section outlining the responsibilities of Public Access Point providers to intervene in cases of disruptive use. The effects of this rewording are to put greater emphasis on the importance of providing a 'positive and encouraging atmosphere' (as stated in the new clause 5.1). It also places stronger emphasis on the importance of having a 'pre-established and transparent' process for handling any necessary intervention (covered by the new clause 5.3). The principles behind the original clauses however, have been maintained in the revised version. Thus, staff of Public Access Points are not required to exercise general supervision of usage with the deliberate aim of identifying illegal or offensive use, but, where such use is drawn

to their attention, 'they have an obligation to request the cessation of illegal use and to encourage more discrete use of disturbing content'.

Section Six: Filtering, rating and warning pages

In the revised version of the guidelines, the original sections six, seven and eight covering filtering, content rating and warning pages have been brought together under a single section six.

With regard to the use of filtering software, clause 6.1 has been amended. In part, this is to clarify that the imposition of filtering software *by the managers of Public Access Points* [researcher's italics, used to illustrate inserted wording] is an unwarranted interference with an individual's freedom of access to information. However, the precise meaning behind the clause has also altered. Thus, whereas the original clause specifies that filtering software should not be applied at Public Access Points *unless explicitly required by law*, reference to legal provisions have been removed from the revised clause. Instead the new clause aims to provide greater user empowerment and choice, through the insertion of the statement that 'If filtering and blocking systems are to be made available, it should only be as an option that individuals can choose and calibrate at their own preferred levels'.

The encouragement of the exploitation of systems for positive recommendation of relevant and high quality content, including the use of metadata for labelling and rating content, remains. Although the original clauses 7.2, 7.3 and 7.4 (all relating to the rating of content) have been amalgamated into a single clause, 6.4, the substantive meaning of the clauses has been retained.

However, the two clauses relating to the use of warning pages and age verification systems (6.5 and 6.6 in the revised version) have been reworded in such a way as to change the emphasis away from a potentially complacent reliance on warning pages. Thus, 6.5 now reads that the staff of Public Access Points 'should *be prepared* [researcher's italics] to draw [users'] attention to the warning pages attached to many sites that contain controversial content, *but should also make it*

clear that not all such sites contain warning pages [researcher's italics]'. In the original version, clause 8.1 read 'The staff of Public Access Points should draw the attention of those users who express anxiety that they might inadvertently access disturbing content to the warning pages which are attached to many sites that fall into this category'. Similarly, the clause relating to age verification systems has changed its tone from one of reassurance ('[The staff of Public Access Points] can also publicise, to parents anxious about the sites which their children might access, the existence of warning pages and age verification systems attached to some controversial content') to one of caution. The new clause 6.6 reads 'The age verification systems attached to some sites with controversial content also warn users that they might wish to avoid such content, but users should be made aware of the risks associated with supplying personal data to such systems if they are not operated by reputable organisations'.

Section seven: Internet Use Policies

The main changes to this section of the text involve the omission of two clauses (9.4 and 9.5) that in the original text suggested specific issues that should be included in an Internet use policy, namely: the use of workstations for illegal purposes or to access illegal content; user rights of confidentiality and privacy; and the need for users to exercise consideration towards other users. Instead, clause 7.1 in the revised version has been rephrased to read 'A Public Access Point should be operated within a clearly articulated and publicly available policy, *consistent with the principles of this text, and explaining the balance of responsibilities between staff and users* [researcher's italics, to indicate new content]'. The section no longer attempts to make any further definition as to the detailed content that should be included in such a policy.

4.4.4.4 Summary of changes to the *Guidelines* arising from the consultation

It can be seen that the text of the guidelines altered significantly as a result of the consultation process, and indeed the document's status altered from one of

Recommendations to one of *Guidelines*. Many of the textual changes were made to enhance the clarity of wording to prevent unintentional (or wilful) misinterpretation of the meaning or spirit of the guidelines. Changes have also been incorporated to achieve greater consistency and coherence with other international actions and conventions, whilst simultaneously removing some of the provisions that could potentially have provided the ability to hide behind the provisions of unjust or overly restrictive national legislation.

The final draft of the guidelines does represent an attempt at achieving the difficult balance between the right to freedom of expression and the responsibilities of Internet users towards the rights of others, particularly with regard to the right not to experience offence or discrimination. The guidelines are now broader in scope than had originally been envisaged. They now encompass the rights of users to access a range of diverse cultural content and the responsibilities of Public Access Point providers, together with local and national governments, to provide networked public information. There is a stronger emphasis on educational use, user empowerment and the role of the information professional as intermediary in providing guidance and training in the use of networked facilities. A greater level of importance is attached to policy development and the transparency of policy than was the case in the original draft, for example in the reworded section on specialised institutions. However, it has to be noted that as a result of the outcomes of the consultation process, in spite of the widening of scope of the guidelines (or indeed, because of this widening), there has been an overall dilution of the original emphasis on freedom of expression, especially with regard to access by minors to networked information.

The Council of Europe regarded the Conference as the first of a series to validate ideas and policy guidelines with regard to New Information Technologies, and considered the involvement of external experts in the consultation process as an example of freedom of expression and democracy in practice[98]. There is indeed a

[98] Comment made in opening presentation at the Conference by Ms Vera Boltho, Head of the Cultural Policy and Action Division, Council of Europe.

strong degree of correlation between comments made, both at the electronic consultation stage and at the Helsinki Conference, with subsequent revisions applied to the text of the draft. It would not seem unreasonable, therefore, to regard this case as a genuine example of democratic consultation in practice. However, although this approach is laudable, it should be noted that the entire process took from September 1998 to May 2000 to reach a version of the text that was acceptable to the Council of Europe and to relevant stakeholders. In a fast-moving area such as new information technologies this is hardly an ideal scenario. Similarly, the effective failure of the electronic consultation meant that the views of stakeholders were not heard, whilst government and institutional representatives had full opportunities to comment and seek modifications.

The intention was to make the guidelines available to all professionals, to be followed by further texts for professionals emanating from the New Information Technologies programme intended to help member states formulate policy and harmonise approaches. The programme has already resulted in a number of policy documents and expert reports in areas such as the promotion of cultural diversity[99] and the training of artists and cultural workers in the new technologies[100], as well as another set of guidelines, this time relating to cultural work within the information society[101]. However, with regard to the *Guidelines on Public Access to and Freedom of Expression in Networked Information*, the time, cost and effort that went into their drafting and the consultation process does not appear to have been reflected in the impact that they have made on practice in the cultural or information sectors. Having invested considerable resources in the drafting and consultation processes, the Council of Europe did not appear to make any parallel investment in the dissemination or promotion of the *Guidelines*. Although

[99] < http://cm.coe.int/ta/decl/2000/2000dec2.htm > [Last accessed 5/7/2004].

[100] <http://www.coe.int/T/E/Cultural_Co-operation/Culture/New_Technologies/N.I.T/Working_strands/NT_and_creativity/bongiovanni99_1.asp#TopOfPage> [Last accessed 26/8/2003].

[101] < http://www.coe.int/T/E/Cultural_Co-operation/Culture/Resources/Texts/CC-CULT(2000)49rev_EN.pdf?L=EN> [Last accessed 5/7/2004].

reference has been made to them in the professional literature in the UK (Stoker, 1999; Vitiello, 2000; Sturges, 2000a; Sturges, 2000b; Sturges, 2001; Sturges, 2002) most information professionals and policy makers appear to be largely unaware of their existence[102]. Indeed, even relevant professional associations such as CILIP do not acknowledge them in the professional practice area of their website[103].

4.4.5 Declaration on a European Policy for New Information Technologies

In May 1999, at the same point in time as the original draft 'Helsinki Charter' was being made available for consultation, the Committee of Ministers adopted the Culture Committee's *Declaration on a European Policy for New Information Technologies*[104] at its 104th session in Budapest (Council of Europe, 1999b). The Declaration was intended to act as a stimulus for the development of a policy framework for the application of new technologies in the field of culture and education. The same themes and emphases of the final text of the *Guidelines on Public Access to and Freedom of Expression in Networked Information* are echoed in the wording of the *Declaration.*

Thus, the *Declaration* opens on a positive note by welcoming the potential of the new information technologies to promote democracy, freedom of expression and cultural diversity. It also identifies the potential risks of widespread adoption of new technologies. In response to these risks it calls for the development of regulatory frameworks based on a combination of legislation, self-regulation, codes of conduct and the development of technical standards and systems. These are portrayed as essential to ensure the preservation of respect for human rights, especially freedom of expression, whilst also ensuring the protection of minors, the

[102] This impression was confirmed in an email from the author of the Guidelines, received 27/8/2003.

[103] <http://www.cilip.org.uk/practice/practice.html> [Last accessed 5/7/2004].

[104] Available at < http://cm.coe.int/ta/decl/1999/99dec3.htm e> [Last accessed 5/7/2004].

protection of individual privacy and protection against racial discrimination in the online environment. It calls for the commitment of governments of member states to the free flow of information and ideas through the development and promotion of access to educational content and to a diversity of cultural and linguistic content. As with the *Guidelines* recognition is paid to the importance of education and training to ensure that users develop the required skills and competence to make critical and discerning use of networked content.

4.4.6 Recommendation on self-regulation concerning cyber-content

Another outcome of the Action Plan agreed in Thessaloniki in December 1997 was *Recommendation (2001)8 of the Committee of Ministers to member states on self-regulation concerning cyber-content (self-regulation and user protection against illegal or harmful content on new communications and information services)*[105] which was adopted in September 2001 (Council of Europe, 2001a). This recommends the governments of member states to encourage the establishment of self-regulatory organisations that include representatives from Internet Service Providers, content providers and users. In particular, these organisations should be encouraged to develop codes of conduct for the industry, and to monitor compliance with the codes.

Although this *Recommendation* is not aimed specifically at issues related to the provision of *public* access to the Internet, many of the proposed mechanisms for content regulation are similar to those in the *Guidelines on public access* (Sturges, 2000a). They also accord well with the provisions of the EU *Action Plan* and UK measures such as the role of the Internet Watch Foundation. The development of measures to aid content identification and selection, such as content descriptors, search tools, filtering and conditional access tools is

[105] Available at <http://cm.coe.int/ta/rec/2001/2001r8.htm> [Last accessed 5/7/2004].

encouraged in the *Recommendation*, albeit with a clear statement that the use of filters should be the choice of the end user. A means to allow complaints about content to be made and acted upon, such as a system of hotlines, operated in co-operation with law enforcement agencies, is recommended. The *Recommendation* also encourages the creation of effective procedures for out-of-court mediation and dispute arbitration for content-related matters. Finally, member states are encouraged to undertake actions to encourage public awareness of self-regulatory mechanisms, content descriptors, filtering and access restriction tools, hotlines, and arbitration and mediation services (Council of Europe, 2001a).

A questionnaire survey[106] that was administered to members of the Steering Committee on the Mass Media of the Council in February 2001 by the Group of Specialists on Online Services and Democracy evaluated the extent to which member states had already implemented measures proposed in the *Recommendation*. Replies were received from twenty-two Council of Europe member states, plus one from Canada (a Council of Europe observer state). The analysis of responses suggests that the policy measures proposed in the *Recommendation* are in line with the actions being implemented in the respondent states. In particular, there is a strong compliance with the strategy of using self-regulatory mechanisms for addressing issues of Internet content regulation, such as Industry and user-based regulatory bodies, codes of conduct and hotlines. None of the respondent states implemented official prior control of content, and there was broad agreement with the principle of self-regulation and international co-operation in addressing the problems posed by illegal and harmful content (Council of Europe, 2002a).

[106] Available at <http://www.coe.int/T/e/human%5Frights/media/4%5FCyberfora/1%5FSelf%2Dregulation/3_Country_information/2_Summary_&_analyses/default.asp#TopOfPage> [Last accessed 27/8/2003].

4.4.7 Declaration on Freedom of Communication on the Internet

In May 2003, following a consultation period on a draft document, the Committee of Ministers adopted a *Declaration on freedom of communication on the Internet*[107] (Council of Europe, 2003b). Originally drafted by the Group of Specialists on Online Services and Democracy, the Declaration's main objective is very much in line with other Council of Europe initiatives in attempting to achieve a balance between freedom of expression and information on the Internet, and other rights guaranteed by the ECHR such as the protection of children. In particular, the *Declaration* condemns practices that are aimed at restricting or controlling Internet access for political reasons (Council of Europe, 2003c). The main guiding principles of the *Declaration* are:

- Member states should not subject Internet content to restrictions that exceed those applied to other content forms;
- Member states should encourage self-regulation or co-regulation for content disseminated on the Internet;
- Public authorities should not exercise prior control of Internet content, other than through the installation of filters for the protection of minors in places accessible to them, such as schools or libraries;
- Member states should foster and encourage access for all to Internet services on a non-discriminatory basis and at an affordable price;
- Freedom to provide services via the Internet should be encouraged – the provision of services via the Internet should not be subject to specific authorisation schemes on the sole grounds of the means of transmission, and service providers should be allowed to operate in a regulatory framework that guarantees them non-discriminatory access to national and international telecommunications networks;

[107] Available at <http://www.coe.int/T/E/Communication_and_Research/Press/News/2003/20030528_declaration.asp> [Last accessed 27/8/2003].

- Internet Service Providers should not be obliged to monitor Internet content to which they provide access or which they transmit or store, although they may be held liable for a failure to remove or disable access to information or services once they become aware of their illegal nature;
- To ensure protection against online surveillance, member states should respect the wish of Internet users to remain anonymous (however, this does not prevent member states from taking measures to trace those responsible for criminal acts in accordance with national law, the ECHR and other international agreements in the fields of justice and the police).

(Council of Europe, 2003b)

Thus, once again, the proposed measures reflect the spirit of other regulatory measures at EU, UK and Council of Europe levels, particularly with regard to the emphasis on self-regulation. The last bullet point above, however, is potentially problematic when considered together with another simultaneous but considerably more restrictive Council initiative, the *Convention on Cybercrime*.

4.4.8 The Convention on Cybercrime

At a conference of the G8 in Paris in May 2000 the need for nations to co-operate in the struggle against a range of different forms of 'cybercrime', such as computer viruses, computer-based fraud, hacking and the dissemination of child pornography or racist propaganda, was discussed. In his opening address the French interior minister, Jean-Pierre Chevènement, insisted that it was the duty of national governments to make it clear to their citizens that the Internet is not a lawless zone (Henley, 2000). It was noted that efforts to tackle cybercrime on the international front are hampered by the lack of international agreement on what constitutes a criminal act – thus, for example, the dissemination of Nazi propaganda is illegal in France, Germany and the Netherlands, but is protected in the US under the First Amendment (Ibid). Chevènement reported that, in order to address this situation, the Council of Europe was drafting a treaty that aimed to harmonise national laws against cybercrime, and urged the G8 members to adopt

the treaty. The Council's intention, according to Chevènement, was to produce '…a global text so there cannot be 'digital havens' where anyone planning shady business could find the facilities to do it' (cited in Henley, Ibid).

The origins of this treaty, the *Convention on Cybercrime*[108] (Council of Europe, 2001b) began with a decision by the European Committee on Crime Problems (CDPC) in November 1996 to set up a committee of experts to tackle cybercrime. It was agreed early on that the issues involved were of such a potentially serious nature, and were of such global reach, that they should be dealt with by the mechanism of a legally binding instrument such as a convention (Council of Europe, 2001c). Work on the draft treaty began in April 1997, and it was finally agreed in Budapest in November 2001.

The remit of the *Convention* extends well beyond the subject matter of this thesis and it would not therefore be appropriate here to provide a comprehensive analysis of all of its content[109]. However, the potential impact of some of the provisions of the *Convention* on freedom of expression on the Internet is sufficiently great to warrant some consideration of those aspects (it has, for example, been described by Castells (2001, p.178) as 'the most far-reaching, comprehensive attempt to control communication over the Internet to date').

The *Convention* identifies three primary aims in addressing the problem of cybercrime:

1. To harmonise the domestic, criminal, substantive law elements of offences and connected provisions in the area of cybercrime;

[108] Available at <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm> [Last accessed 5/7/2004]

[109] A useful analysis of the Convention can be found in Akdeniz (2003) *The Council of Europe's Cyber-Crime Convention 2001 and the additional protocol on the criminalisation of acts of a racist or xenophobic nature committed through computer systems.* Available at < http://www.cyber-rights.org/cybercrime/coe_handbook_crcl.pdf > [Last accessed 5/7/2004].

2. To provide for domestic, criminal, procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system, or for which evidence is in electronic form;
3. To set up a fast and effective regime of international co-operation in combating cybercrime.

(Council of Europe, 2001c).

Despite being called the *Convention on Cybercrime,* many of the provisions extend to crimes committed using a computer, or for which evidence is held in electronic form, irrespective of whether electronic communications networks are actually involved. The nature of offences that the *Convention* is intended to address include illegal access or interception of computer systems, data or systems interference, computer-related forgery and fraud, and offences related to copyright and neighbouring rights. In particular it establishes for relevant parties the rights, conditions, requirements and safeguards with regard to data storage, data disclosure and access to stored data, the collection of traffic data, and the interception of content data.

The Articles in the *Convention* that are of the greatest potential relevance to freedom of expression are those that concern Internet content, in the form of child pornography, and those related to the collection of evidence in electronic form. It should be noted that *all* the Articles are subject to the provisions laid out in the ECHR, and the powers provided through the *Convention on Cybercrime* can only be applied to specific criminal investigations. Unlike the blanket provisions for data retention of the UK *Anti-Terrorism, Crime and Security Act* (Parliament, 2001), the *Convention* only provides for data 'preservation'[110], and is not intended to lead to widespread surveillance of Internet content or use (Esposito, 2003).

[110] Data preservation is used to signify the retention of data relating to specific individuals identified to ISPs, as opposed to indiscriminate data retention (cf. Walker and Akdeniz, 2003, p.177).

In accordance with the ECHR, any restrictions imposed through the *Convention on Cybercrime* on the right to freedom of expression must be prescribed by law and be necessary in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary (Council of Europe, 1950, Article 10, para.2). Similarly, any restrictions imposed through the *Convention* on the right to privacy should conform to the conditions laid out in Article 8 of the ECHR. Thus, they must be necessary in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others (Council of Europe, 1950, Article 8, para.2).

Article Nine of the *Convention on Cybercrime* commits member states to criminalizing the production of child pornography for distribution through a computer system; the offering or making available of child pornography through a computer system; the distribution or transmission of child pornography through a computer system; the procurement of child pornography through a computer system for oneself or for another; or the possession on a computer system, or on a computer data storage medium, of child pornography. All of these actions have to have been committed intentionally and 'without right' for prosecution to be legitimate, and ISPs who have 'served as a conduit for', or hosted a website or newsroom containing such material, without the required intent, cannot be held liable (Council of Europe, 2001c). Member states also have some discretion with regard to the criminalisation of procurement and possession alone and the definition of what constitutes child pornography.

With regard to data preservation, Article Sixteen of the *Convention* requires member states to

> *…adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system…*
>
> (Council of Europe, 2001b, Article 16)

The maximum length of time that data should be required to be stored is 90 days, although enforcement agencies may be permitted to renew the data preservation order. Legislation should require that whoever is the recipient of a data preservation order should maintain confidentiality with regard to the order. In addition, Article Seventeen requires the implementation of legislation that imposes a duty of 'partial disclosure' of traffic data retained under Article Sixteen to the relevant authority.

Article Eighteen requires member states to implement measures that empower competent authorities to order the submission from individuals of specified computer data in their possession or control, whether it is stored on a computer or on a storage medium such as a floppy disk. Authorities should also be empowered to order ISPs to submit 'subscriber information': this information can include the subscriber's identity, postal address, telephone number and billing and payment information. Authorities should also be given the power to search, and if necessary seize, computer systems and computer storage media (Article Nineteen). The same Article gives authorities the power to order anyone with knowledge about the functioning of the relevant computer system, or measures taken to protect data held on the system, to provide the necessary information required to search and seize the system or data.

The provisions of Article Twenty oblige member states to implement measures that empower authorities to compel ISPs, as far as their technical capabilities allow, to collect or record real-time traffic data or to co-operate and assist authorities in the collection or recording of such data. Service Providers should be obliged not to disclose the fact that such an order has been made. Article Twenty-One, relating to the interception of content data, goes further still, although it is acknowledged that this Article should be applied only in relation to 'a range of

serious offences to be determined by domestic law' (Council of Europe, 2001b, Article 21). In such circumstances, authorities should be empowered to compel the same degree of co-operation from ISPs as for real-time traffic data in Article Twenty, but this time with disclosure of the content of such communications traffic. Again, ISPs should be compelled to maintain confidentiality of the investigation.

In addition to all the above provisions, Article Twenty-Three requires member states to co-operate with each other 'to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence' (Council of Europe, 2001b, Article Twenty-Three).

The original *Convention* did not include racism or xenophobia in its provisions for content regulation, because of concerns expressed about the potential impact on freedom of expression (Esposito, 2003). According to Akeniz (2003), this was largely in response to pressure from the United States, on account of the potential conflict with the provisions of the First Amendment. However, in November 2002 the Committee of Ministers adopted an additional protocol[111] to the *Convention*, requiring member states to criminalise the dissemination of racist and xenophobic material through computer systems, and the use of computer systems to disseminate threat or insult motivated by racism or xenophobia. This includes the denial, minimisation, approval or justification of genocide or crimes against humanity, especially those that occurred between 1940 and 1945 (Council of Europe, 2002b). Because of the requirements of 'intention' ISPs are accorded the same level of immunity from liability as prevails for the main *Convention*. The provisions of the protocol are also subject to the constraints imposed by the ECHR, in particular those of Article 10 pertaining to freedom of expression. The Council believes that, by establishing in the protocol the extent to which racist and xenophobic content violates the rights of others, its impact will be to help to

[111] Available at <http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm> [Last accessed 5/7/2004].

protect individual rights and freedoms on the Internet (Esposito, 2003). By April 2004 twenty-two countries had signed up to the protocol[112].

Clearly, computer-based crime is a major and growing issue for individuals, corporations and national governments, and the problem is compounded when such crime is committed and propagated on global communications networks. However, the *Convention on Cybercrime* is somewhat surprising in that it appears to extend well beyond the normal remit of the Council of Europe. Although, of course, the commission of any crime is likely to infringe on the rights of those affected by the crime, nevertheless the terms of the Convention do not appear to focus clearly on the Council's primary mission of the protection of human rights (and could be argued to detract from it). Indeed, it has been suggested that the *Convention on Cybercrime* is incompatible with the provisions of the ECHR and data protection legislation, and that the balance has been struck in favour of law enforcement rather than fundamental human rights (Akdeniz, 2003).

More surprising still is the lack of public consultation and awareness actions that accompanied the drafting and signature of a convention with such potentially important and far-reaching impact. According to Akdeniz (Ibid), submissions made by Non-Governmental Organisations were largely ignored by the Council of Europe during the brief consultation period (which in itself was not widely publicised). Moreover, arguably the most important provisions (that is, those relating to the interception of communications) were not made public until the end of the consultation period. He also criticises the *Convention* on the grounds of lack of legal clarity in the wording of some of the provisions; the over-extensive scope of some of the provisions; the lack of safeguards with regard to requirements for judicial warrants; the potential impact on e-commerce of government access to encryption keys; and the lack of provisions requiring 'dual criminality'[113] with regard to the provisions for mutual assistance.

---

[112] A regularly updated list of these countries can be found at <http://conventions.coe.int/treaty/en/searchsig.asp?NT=189&CM=&DF=> [Last accessed 27/4/2004].

[113] 'Dual criminality' requires that the actions under investigation should be illegal in both jurisdictions e.g. law enforcement agencies cannot request assistance from law enforcement

4.5 Council of Europe approaches: some conclusions

As with the European Union, the Council of Europe was relatively slow to act with regard to the 'problem' of the Internet: this reflects the relatively low priority accorded to the issue by national governments of member states in the early days of the Internet. However, from the mid-1990s onwards there has been greater weight accorded to the issue and, in particular, a greater recognition of the importance of international co-operation in decision-making with regard to the Internet. Thus, in addition to the EU and the Council of Europe, bodies such as the G8 group of states, the OECD and the United Nations (notably UNESCO and the WIPO) have all paid increasing levels of attention to regulatory issues concerning the Internet.

With regard to the Council of Europe, it is difficult not to conclude that fragmentation among different departments has reduced the impact and clarity of the considerable range of initiatives that are forthcoming from the various sections, each with their own (and in some cases, competing) priorities. For example, the Media section, the Culture section, the Legal Affairs Executive and the Committee on Crime Problems are all among those working on issues related to Internet content regulation. In addition, the case study of the development of the *Guidelines on Public Access* illustrates how high levels of bureaucracy and the need to resolve the competing interests of different stakeholders tend to result in very slow policy development, especially where sensitive issues such as access to Internet content by children and young people are concerned. The outcome of such policy development is also at risk of being very different from the original intentions of those who initiate the undertaking, as illustrated by this case.

However, with the possible exception of the *Convention on Cybercrime*, the various initiatives do, nevertheless, illustrate quite a high level of coherence, both across the various Council of Europe actions and with EU initiatives. In particular,

---

agencies in another country in investigating an action that is not a crime in the country from which they are requesting assistance.

the emphasis on self-regulation and actions to raise awareness and promote education is repeated, although a higher priority to freedom of expression can be seen in the Council of Europe actions than is evident in the EU actions. The Council of Europe tends also to be more positive in its statements concerning the benefits of networked information, particularly as concerns the promotion of democracy and cultural diversity.

The *Guidelines on Public Access* in particular can be commended in offering a clear statement of principles to assist those responsible for Public Access Points to provide free and non-censored access to information available on the Internet, whilst addressing issues of anxiety about the possible harmful effects of such access. However, the case study highlighted the need to devote time and expertise to the technical aspects of electronic consultation, if such an approach is to represent a genuine attempt at soliciting the viewpoints of the full range of stakeholders. It also demonstrated the importance of paying as much attention to policy implementation, dissemination and evaluation as to policy development. It was clear from the study that much of the potential value of the *Guidelines* had been lost as a result of the lack of importance given to the dissemination stage of the policy cycle.

CHAPTER FIVE: INSTITUTIONAL POLICY FORMULATION – THREE CASE STUDIES

5.1 Introduction

The previous two chapters have explored the development of Internet regulation policy at the national and European level. This chapter presents the findings from the institutional case studies, exploring the development, implementation and impact of measures to control and regulate the use of network facilities and access to Internet content, with particular regard to 'unacceptable' or illegal use, in three UK Higher Education Institutions. It was intended that investigation at this micro level would illuminate some of the operational difficulties in formulating and implementing policy in this area, and would provide an insight into the impact that such policy measures were having on individual Internet users.

Before presenting these findings the Chapter includes a brief outline of the background to national policy specifically applicable to higher education on this issue in the UK, and some of the challenges that higher education in the UK has faced with regard to Internet use. The findings of the case studies are presented on a within-case basis, in order to establish a holistic picture of the ethos and context in which each institution operates. However, the discussion of these findings offered in Chapter Seven will be made on a cross-case basis, with an emphasis on the theoretical relevance of the models of policy making that were found to prevail, and the impact on intellectual freedom that the chosen strategies appeared to be having.

The data collection within the three institutions, and its subsequent analysis, was directed by the research questions to be investigated. The specific issues explored were:

- What methods are currently in place to control or monitor Internet use, and what level of awareness is there within each institution of such measures?
- What problems (if any) have been experienced as a result of 'unacceptable' or illegal use by students or staff of Internet facilities, and, where relevant, what actions have been taken as a result of this use?
- How has policy in this area been developed, and who are the key players involved in the decision-making process and in the implementation of policy?
- What forces – both internal and external to the institution – impact to influence policy decisions?
- What impact do these decisions have on individual Internet users in the institutions, in particular with regard to their freedom of enquiry?

The case studies were carried out through interviews with a range of personnel and a representative from the student body at each institution, in addition to the analysis of a range of policy documents with potential implications for Internet use in the institutions (Appendix Two provides a table of respondents interviewed at each institution; Appendix Three provides a table illustrating the range of documents analysed for each institution). The analysis of this data was made using an inductive approach, identifying themes that arose from the documents and transcripts themselves. In particular, there was a concern to gain insights into the policy formulation process at the institutions, rather than to focus narrowly on the specific content of policy documents. The experiences and opinions of students were explored further via the questionnaire study. The findings of this study are presented in Chapter Six, and are complementary to the findings presented in this Chapter.

The three institutions are referred to as Institution A, B and C, in order to protect their anonymity, and the identity of participants in the case studies is not revealed, although their role within their own institution may be outlined. The chapter also introduces the discussion of policy models that will be further elaborated in Chapter Seven (Discussion of Findings).

5.2 The higher education context: some policy background

Academic institutions in the UK that receive their network services via the Joint Academic Network (JANET) are bound by the terms and conditions of the JANET Acceptable Use Policy (AUP). The current version of the AUP (version 7.0[114]) states that:

> *'It is the responsibility of User Organisations to ensure that members of their own user communities use JANET services in an acceptable manner and in accordance with current legislation'.*
>
> (Wood, 2003, para.4)

The Policy allows for use of the JANET network for any legal activity that is in furtherance of the aims and policies of the User Organisation, other than those activities defined by the Policy as constituting 'unacceptable use'. Such activities include:

- The creation or transmission (other than for properly supervised and lawful research purposes) of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
- The creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety;
- The creation or transmission of defamatory material;
- The transmission of material such that this infringes the copyright of another person;
- The transmission of unsolicited commercial or advertising material either to other User Organisations, or to organisations connected to other networks;
- Deliberate unauthorised access to facilities or services accessible via JANET;

[114] Available at <http://www.janet.ac.uk/documents/use_policy.pdf> [Last accessed 5/7/2004]

- Deliberate activities with any of the following characteristics: wasting staff effort or networked resources; corrupting or destroying other users' data; violating the privacy of other users; disrupting the work of other users; using JANET in a way that denies service to others; continuing to use an item of software or hardware after UKERNA has requested that use cease because it is causing disruption to the correct functioning of JANET; any other misuse of JANET or networked resources, such as the introduction of viruses.

(Wood, 2003)

Individual institutions are responsible for taking 'all reasonable steps' to ensure compliance with the policy, and for ensuring that 'unacceptable' use of JANET does not occur. Penalties that may be imposed on institutions for contravention of the JANET AUP range from suspension of network services through to referral for legal action.

In 2000 the Joint Information Services Committee (JISC) published a *Briefing Paper for Senior Managers in UK Further and Higher Education Institutions* (Charlesworth, 2000b) to draw attention to the implications of recent legislation and case law with regard to the Internet. Noting the rapid development of law related to the Internet of relevance to academic institutions, the paper also identifies the increasingly sophisticated technology available to end users and the potential that this offers for engaging in illegal activities such as hacking, copyright infringement and the dissemination of illegal content.

With regard to the liability of Higher Education Institutions and their staff for illegal content accessed or disseminated via their network services, the provisions of the *Obscene Publications Acts* of 1959 and 1964 (Parliament, 1959; Parliament, 1964), and the *Criminal Justice and Public Order Act* (Parliament, 1994a), among others, apply. Under these Statutory Instruments the transfer of obscene material electronically from one computer to another, via a network or the Internet, can be regarded as 'publication', even if an individual simply makes the material available for transfer or downloading electronically by others (Charlesworth,

2000b). The two main defences are 'innocent publication' (where the person who published the material did not know that it was obscene and had no reasonable cause to believe that its publication would result in liability) or publication in the public good. Thus, while providers of Internet services are unaware that illegal material is being made available via their system, they cannot be held liable. However, once they are told that this is occurring, they must take action to stop it, otherwise they leave themselves liable to prosecution (Ibid).

In consequence, the advice of JISC to academic institutions includes:

- State clear warnings as to the likely disciplinary consequences of viewing, storing or transmitting obscene material on University equipment, both in staff contracts and in Codes of Conduct for computer use;
- Do not abdicate responsibility for checking of content, as it may be viewed that a deliberate policy of not undertaking any scrutiny negates the defence of lack of reasonable grounds for suspicion;
- Make occasional searches of electronic records of the titles of files they host, and the domain names of sites from which information is cached, to check for suspicious file and domain names;
- Whenever such files are found, take action to ascertain their contents and, if necessary, remove them;
- Provide clear and effective mechanisms for individuals to report illegal material and ensure that, when such reports are made, fast and effective action is taken.

In addition, the advice stresses that institutions should pay particular attention to material that appears to amount to child pornography, as mere possession of such material is an offence. In addition to removing such material, the incident should be reported to the police (Ibid).

The first major UK law case to take place regarding the use of university computers to access or disseminate child pornography on the Internet took place in

1996. Alban Fellows and Stephen Arnold were charged with a total of 18 offences under the *Protection of Children Act 1978* (Parliament, 1978), the *Obscene Publications Act 1959* (Parliament, 1959), and the *Criminal Justice and Public Order Act 1994* (Parliament, 1994a). After being contacted by the US Customs, Vice Squad Officers raided the Department of Metallurgy at Birmingham University and discovered thousands of pictures of children engaged in obscene acts stored on the computer system. During the trial Fellows admitted four charges of possessing indecent photographs of children with a view to distributing them, and one of possessing obscene photographs of adults for publication. Arnold admitted distributing indecent photographs of children. Fellows was subsequently sentenced to three years imprisonment, and Arnold for six months[115]. The case was important in UK law, in that it established the precedent that computerised images could legally be regarded as photographs (Akdeniz, 1997b) and confirmed the principle that making the material available over the Internet amounted to its publication (Charlesworth, 2000b). It was also important for the role it played in initiating concern in the higher education sector about the use of University computer and network facilities for illegal purposes.

There have subsequently been a number of relatively high profile cases of individuals being prosecuted as a result of their accessing and storing child pornography on university computer facilities (for example, see *Guardian*, 1999; BBC, 2003c; *Sheffield Today,* 2003). In one of these cases, the accused was, at the time of committing the offence, a Pro-Vice Chancellor at one of the case study sites for this research project. In another of the cases, the defendant claimed that he had downloaded child pornography as part of an academic research project into hardcore pornography. However, he failed to prove to the court's satisfaction that the pictures were for research purposes (Quinn, 1999). To date, the criminal justice system has proceeded by charging the individuals directly responsible for the misuse, rather than holding the institution liable for illegal activities committed via their computer systems.

[115] Regina v Fellows and Arnold [1997] 2 *All England Law Reports* 548.

There have also been an increasing number of cases of university staff losing their jobs for accessing legal, but 'unacceptable' Internet content, or for accessing the Internet for personal use to the detriment of carrying out work duties. In one such case, six lecturers at one University were suspended over accusations that they had accessed pornography on University computers in breach of its code of practice that restricts staff use of computers to research, teaching, study and administration purposes only (*Times Higher Education Supplement,* 2001a).

There have, however, also been some examples of problematic instances where the restrictions of 'acceptable use' have been in direct conflict with the requirements of teaching programmes and academic enquiry. Dearnley (1999) describes the difficulties he encountered attempting to teach information science students about censorship and the ethical issues posed by the availability of pornographic and obscene materials on the Internet. As part of their academic programme, the students were encouraged to browse the web for pornographic and obscene material (but not to collect or store images or text that they came across). They were encouraged to try to locate actual pornography and sites containing academic debate relating to it. They were also asked to comment on the ease of finding 'free' sites containing pornography; the safeguards in place on commercial pornographic sites with regard to access restriction to adults; and the availability of obscene materials such as paedophilia and bestiality. However, this part of his teaching activities was declared 'unacceptable' by Senior Management at the institution, who felt that the risk to the institution posed by such activities was too great. In two separate memoranda Dearnley was informed that '…academic pursuits are not above the law', and that '…the way in which you have been using Internet pages in your units covering censorship is unacceptable to the University and cannot be followed in the future' (Ibid). This is in spite of the fact that the JANET AUP defines unacceptable use in paragraph 9.1 as:

> *The creation or transmission* ***(other than for properly supervised and lawful research purposes)*** *of any offensive, obscene or indecent images, data or other material…*
>
> (Wood, 2003, emphasis added by researcher)

In another example, a PhD student at Glasgow University was subject to an internal enquiry following media reports that he had emailed convicted paedophiles. The student, who was researching paedophilia, was cleared of accusations of misusing his position as a researcher and of breaching the University code of discipline or code of conduct in his use of their computers. He was, however, instructed to modify his research methods, and to obtain approval for 'sensitive aspects' of his research from the University's Research Ethics Committee (*Times Higher Education Supplement*, 2001b).

In a more recent case, Northumbria University removed content from an academic's web pages without his prior knowledge. The pages concerned included an essay on war myths and an article on war propaganda from the coalition involved in the 2003 war against Iraq. The academic concerned, who had strong anti-war opinions, claimed that these were used as teaching materials (Baty, 2003).

With regard to liability for defamatory content, the Godfrey v. Demon Internet Ltd case[116] appeared to establish the principle that, because Demon had chosen to receive and store the newsgroups containing the defamatory postings, and had the power to delete messages from them, it was in law a 'publisher' and thus liable for the content in question. The case was interpreted by JISC as indicating that academic institutions should take 'some minimum steps to monitor information content' to obtain liability protection, and that if they are informed of defamatory content on their servers, they must take all reasonable steps to remove or deny access to it (Charlesworth, 2000b).

Other means by which JISC recommends that academic institutions may limit their risk of liability for defamatory content include:

- Restricting the number and nature of UseNet newsgroups that they carry;

[116] See Chapter Three, p.92 -.

- Paying careful attention to the content of official institutional web pages;
- Restricting the use of personal web servers and personal web pages on institutional hosts;
- Publishing details of a contact to whom complaints may be made, and ensuring that appropriate action is taken immediately after receiving a complaint.

(Ibid)

These measures are also recommended in order to limit the risk of institutions being held liable for copyright infringements that take place through their network.

With regard to the monitoring and interception of Internet and email use, universities must ensure that such activities conform to the terms of the *Regulation of Investigatory Powers Act* (RIPA) (Parliament, 2000a) or the *Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000*[117] (Parliament, 2000b) (JISC, 2001). However, actions under these instruments must also take into account the provisions of the *Data Protection Act 1998*[118] (Parliament, 1998b) and the *Human Rights Act 1998*[119] (Parliament, 1998a).

Unlike its predecessor the *Interception of Communications Act 1985* (Parliament, 1985), *RIPA* is applicable to private and internal networks. Both *RIPA* and the *Lawful Business Practice* regulations allow for the monitoring and interception of network communications, but only if specific circumstances and conditions apply. In order to ensure that any monitoring or interception or telephone or network use is in accordance with the terms of *RIPA* and the *Lawful Business Practice* regulations, JISC's advice to higher education institutions includes:

[117] Available at <http://www.hmso.gov.uk/si/si2000/ 20002699.htm> [Last accessed 5/7/2004].

[118] Available at <http://www.hmso.gov.uk/acts/acts1998/19980029.htm> [Last accessed 5/7/2004].

[119] Available at <http://www.hmso.gov.uk/acts/acts1998/19980042.htm> [Last accessed 5/7/2004].

- Have a clear and readily available set of policies relating to email and Internet use, and draw the attention of users to these at regular intervals;
- Ensure that network users (including staff, students and visitors) are given effective and ongoing notification of the possibility of their communications being intercepted;
- Consider the necessity of altering the written statement of terms of employees to obtain their explicit consent to interception;
- Take reasonable steps to ensure that, where possible, persons external to the institution who are involved in communication with the institution are informed that communications may be monitored or intercepted;
- Appoint an individual as compliance officer to be responsible for the implementation of policies and procedures under the Act, and to whom interception warrants may be addressed.

(Charlesworth, 2000b)

It should be noted that, as the field work for the institutional case studies took place between March 2000 and September 2001, the institutions involved were in a relatively early phase with regard to the implementation of national policy, and case law in this area was not well developed.

5.3 Case study (1): Institution A[120]

5.3.1 Institutional Context

The first case study took place within a University College, referred to within the thesis as 'Institution A'. At the time of the study, the Institution had a student body of approximately 10,000 studying at both undergraduate and postgraduate level.

[120] Some of the findings presented in the course of this section have been previously published in the proceedings of the 9th International BOBCATSSS Symposium on Library and Information Science (see Cooke, 2001).

The mission statement of the University College claimed that:

> *[The] University College offers access to quality teaching and research within a committed regional and international environment which is caring, supportive of scholarship and provides students and staff with the opportunity for personal and professional development.*

The institution had traditionally emphasised its ethos as a 'caring' institution, both with regard to its approach to student welfare and academic progress, and with regard to the support offered to members of staff. Around 50% of the student population was comprised of home students living in the local area; additionally, approximately 50% was comprised of mature students.

Overall governance of the institution fell under the Council of Governors, with the executive function effected by the Director/Chief Executive. At the time that the fieldwork took place, there were a further five members of the Board of Directors each with specific areas of responsibility. One of these Board members was an Assistant Director with responsibility for library and media services, computer support services, student support, academic services and the Students' Union. It was this latter Assistant Director whose remit gave him the most immediate influence and control over the areas under investigation in the case study. At the time that the fieldwork for the case study was carried out (Spring 2000) a recent appointment had been made to a new position of Information Strategy Co-ordinator, with responsibility for policy development relating to the use of Information and Communication Technologies (ICT).

There were a number of different forums within the University College in which policy decisions were made or ratified, the most important of which was the Senate, in which major policy decisions relating to academic matters were taken. Other major committees included the Planning Board, which debated strategic, resource and estates issues and the Academic Audit Committee, concerned with quality assurance and monitoring. Individual Faculties held their own Boards of

Studies, and sub-committees were held for areas such as Teaching and Learning, Staff Development, Research and Equal Opportunities.

5.3.2 Information policy and strategy

At Institution A, the Information Strategy Steering Group (which reports directly to the Planning Board) was responsible for all areas related to information policy. This Steering Group had representation from the heads of relevant central service departments, but did not include representatives from academic staff or from the student body. It had established a number of sub-groups to develop strategy and policies for specific areas of information systems provision. The outcome of this Group had been the drafting of an Information Strategy that was accepted by the Planning Board in 1999. The Strategy is summarised in a 'vision statement' as follows:

> *Information will be readily available to staff, students and relevant external parties as appropriate, in an understandable format, accurate, complete, and delivered in a timely manner.*

The main focus of the Strategy was on increased co-ordination of information management and systems; increased use of learning and information technologies; enhanced user training and support, both for staff and for students; standardisation of software and hardware; improvements in access to IT facilities; and improved security of information systems. In addition, the Strategy committed the University College to updating its *Regulations for the Use of Computer Facilities* in order to 'avoid misuse of facilities and help improve security'.

The College was connected to JANET and the Strategic Plan included a commitment to provide 24-hour open access to computing facilities during College semesters. However, this goal had not been met, and the network infrastructure and hardware provision available to users at the time of the fieldwork was recognised to be insufficient to meet demand. This state of affairs was reflected in comments made by a number of interviewees, who saw inadequate technological provision as being a significant inhibitor to information access. Further barriers to

information access were outlined in a report by external consultants, who identified problems such as shortcomings in the planning and co-ordination of information systems, a lack of clear policies and standards for the provision and use of information systems, and a lack of user training and support. It was in direct response to this situation that the post of Information Strategy Co-ordinator had been created.

5.3.3 Conditions of Use for Computing Facilities

The University College had written *Conditions of Use for Computing Facilities*. At the time that the fieldwork took place these made no mention of possible monitoring of Internet use (although they did state that the institution 'reserves the right to examine computer files if it suspects they contain material which contravenes college regulations or infringes the law')[121]. The Information Strategy Co-ordinator, responsible for policy formulation in this area, did identify the importance that monitoring was going to have, as a result of the implications of the *Data Protection Act 1998* (Parliament, 1998b). The *Conditions of Use* made no reference to the extent to which personal use of facilities for recreational purposes was deemed acceptable or to any policy on blocking or filtering of Internet content. Users were informed that 'The creation, display, production and circulation of offensive material in any form or on any medium is forbidden', but no attempts were made to define the interpretation of 'offensive material'. The *Conditions of Use* did make reference to the *JANET AUP*, and required network users to observe the conditions of use that this imposed.

5.3.4 Policy awareness and implementation

Despite the existence of the *Conditions of Use for Computing Facilities,* the case-study interviews demonstrated a lack of awareness on the part of both staff and

[121] The document was revised in September 2001 to take into account the provisions of the RIPA, and now advises computer users that 'communications on the University College computer systems may be monitored and/or recorded…'

students of any University College policies relating to computer and Internet use. There was also evidence of decisions regarding issues such as blocking and monitoring of access being made on an ad hoc basis by individuals without a formal remit to make such decisions. Within the University College, approaches to the issue of website blocking, in particular, were characterised by a lack of formal policy backing. When asked whether she was aware of restrictions in place regarding access to Internet sites, even the Information Strategy Co-ordinator, with direct responsibility for the formulation of policy relating to Internet use, commented 'I know [the Internet Services Manager] does block odd things…I must admit I let her get on with it'.

The student representative interviewed was not aware of the existence of any regulations for the use of computer facilities, claiming never to have had these drawn to her attention in any way. However, an interview with the Faculty Librarian suggested that attempts *are* made to draw the attention of students to the existing rules by posting the rules on the College Website and displaying them in computer rooms and in the library. Both agreed, however, that induction training in the library and computer rooms did not address the appropriate use of computer facilities.

The academic staff representative, who was also Chair of the local branch of NATFHE, was emphatic in his denial of having seen any guidelines on the use of email facilities or the possible monitoring of email:

> *No. I have seen nothing that says email should only be used for College purposes. I have seen nothing that indicates formally that email is being monitored…*
>
> (Academic staff representative)

Moreover, the same interviewee claimed to have been told that it definitely *is* acceptable to use network facilities for purposes unrelated to employment:

> *Now it was always made clear actually when I was trained in email here originally that this was provided at no charge to the College, and therefore there was no problem in using it…*
>
> (Ibid)

Although he accepted that there might be instances when monitoring of email and Internet use could be justified, he was concerned about the lack of clarity as to what personal use may or may not be acceptable.

The majority of respondents were also unaware that an institutional code of practice on Freedom of Speech existed, although most respondents claimed confidence in their right of freedom to access information as required and to give voice to their own opinions.

5.3.5 Filtering and blocking of web-based information

Although no formal written policy existed authorising the blocking of access to Internet content for University College users, and filtering software was not installed, comments made by respondents indicated that a certain amount of blocking was taking place. This was done for a variety of reasons, usually related either to the cost of access, security issues or the potential offensiveness of the content. Access to chat protocols was blocked, as was access to free web-based email services such as hotmail.

The Information Strategy Co-ordinator responded to a question on content blocking by commenting:

> *When you talk to [the Internet Services Manager] you'll find that over the years that she's been responsible for the server, there are some areas, some sites, that she's restricted access to...she knows what people like and what people don't like.*

Later in the interview she added:

> *I think [the Internet Services Manager], from the pornographic side, for example, has agreed to restrict access. Of course, you're aware that in the Social Sciences and Humanities Faculty T. [a member of academic staff researching issues related to pornography] always needed access to pornographic sites…*
>
> (Information Strategy Co-ordinator)

These suggestions that ad hoc blocking was taking place were confirmed when interviewing the Internet Services Manager. When asked whether she was aware of any restrictions to specific sites, she responded that 'we use a configuration that we set up to enforce that'. On probing as to the basis for blocking specific sites, she acknowledged that pornographic sites drawn to her attention were blocked. There was also evidence of blocking measures to protect the sensitivities of individual members of staff within the Computer Support department, who were required to administer the student printing system:

> *…there are sites that disturb some people. The young man who used to work in the room there was African Caribbean. He sold the print-outs to students…And someone had printed off stuff on the Ku Klux Klan, and he found that very disturbing.*
>
> (Internet Services Manager)

And similarly:

> *We've got a young man who works in there, and he's RAF Reserve, and he was quite upset by some IRA stuff that was coming out. Which is actually quite valid research for students, particularly for Social Sciences and Humanities, and it's very difficult...I really would rather not censor in any way.*
>
> (Ibid)

Despite her reluctance to act as censor, and the recognition that access to such content could be a valid component of students' academic tasks, she had blocked access to the sites concerned. Moreover, when asked whether decisions to block access were taken in consultation with anyone else, she acknowledged that they were taken 'just off my own bat' and information on which sites had been blocked, or for what reasons, was not passed on to anyone else. This was despite her own

recognition that 'where it goes over the edge for one person is very different from another'.

The academic staff representative was concerned about the possible blocking of content:

> *[The blocking of pornographic sites] raises other questions…there may be colleagues, academics, who want to access these sites who have now been impeded in their work.*
>
> (Academic staff representative)

This tension between the demands of academic study and research, and decisions to block access to content on the grounds of potential offence, was evident in the experiences of the Faculty Librarian in her work with students. She described an incident that took place in the Library, with a student complaining about another student who was accessing pornography:

> *He was one example of a student accessing this material and it was upsetting other students. I said, you know other students are getting upset, it's not appropriate that you access this material in the library...He said it was for his studies and I was inclined to believe him because he was a social work student.*
>
> (Faculty Librarian)

In this instance, the student concerned was advised to speak to his tutor about gaining access to a computer in an area where other students would not be around to get upset. A similar approach was taken in the case of a design student, whose tutor had suggested that he discuss his information needs with the Faculty Librarian before accessing content in the Library. The student was researching 'fetishism...and rubber stuff', and was advised that 'the public access computers were not appropriate for what he wanted to do'.

The Students' Union representative also provided an example of a genuine instance of needing to access material that might be regarded as offensive by some users:

> *...[someone] who runs an Aids Clinic or something, did a survey about our students...a sex survey basically, sex and drugs, about how often students had sex and that kind of thing, and then how many drugs they'd taken and all this, and I wanted to write it up in a report but compare it with the national picture, so I was going [to the library] looking up sex and drugs.*
>
> (Students' Union representative)

Students using the Library had reported feeling intimidated and uncomfortable, as a result of other students accessing pornography. The Faculty Librarian commented:

> *There was an incident in the Library with a [male] social work student, a female student felt uncomfortable…I don't think there were many other students around, it was later in the day and she felt intimidated. This chap was looking at pornography and she felt intimidated by that…*
>
> (Faculty Librarian)

The Faculty Librarian reported problems encountered in the Library with students unable to access chat rooms and even some sites directly related to their studies. Such problems had been compounded by an apparent lack of communication within the University College concerning such decisions, library staff only becoming aware that sites were blocked when students attempted to access them:

> *We knew this blocking was going on in the library, but we didn't really realise what else it was blocking while they were blocking the chat lines…we didn't realise it would block access to other material that could be useful.*
>
> (Faculty Librarian)

There were no written documents available to either staff or students outlining the policies on the blocking of access to chat rooms or to web-based email. Lack of awareness of blocking decisions had led to users, including members of staff, being unable to differentiate between technical difficulties preventing access, and access that had been denied as a result of a deliberate policy decision. Confusion as to whether access was being denied, or whether they were experiencing technical difficulties, was described by the member of academic staff:

I find with the Internet use, whether it's to do with our technology, but when you try to contact places, the number of failed contacts you get. It does seem to be more from here than it does when I'm using it at home, so is that because of the usage of the technology, or the controls? I don't know.

(Academic staff representative)

5.3.6 Monitoring of Internet use

A similar lack of clarity and communication was apparent with regard to the University College policy on monitoring of Internet use. Employment contracts and computer use regulations that were in place at the time of the fieldwork made no reference to possible monitoring of Internet access, although the Internet Services Manager confirmed that such monitoring did take place. The Information Strategy Co-ordinator, whilst being unaware of current monitoring practice, did acknowledge that this issue was likely to be addressed in the near future, in part as a response to the *Data Protection Act 1998* (Parliament, 1998b). In the meantime, she noted 'what people often aren't aware of is that all the emails can be read by the Postmaster anyway'. Moreover, the interview with the Postmaster [the Internet Services Manager] revealed that she was 'occasionally' requested by members of Senior Management to monitor the email use of individual members of staff. She cited one instance:

…they asked me that time just to say who this person was in contact with and why. It was actually someone who was spending most of the day doing email rather than the job they should be doing.

(Internet Services Manager)

This suggests that concerns that had been drawn by other lecturers to the attention of the academic staff representative had some foundation, although suspicions of more widespread monitoring were hard to validate. He commented:

Other colleagues have told me...there are some in certain faculties who can monitor the Internet use. Though I suspected that was happening anyway on an institutional basis

because there is a real interest for employers in ensuring that the Internet is not being used in a certain way, for certain purposes...I think [the Internet Services Manager] is probably doing that.

(Academic staff representative)

Nevertheless, despite expressed concern at the possible uses of such monitoring, he was of the opinion that there was no institutional policy preventing personal use of institutional email facilities, commenting that 'certainly there has not been in the institution any statement that you may not use email for personal use, or any other use that [staff] may wish to make as well'.

The Faculty Librarian had not received any guidance or instructions as to acceptable use of the University College network facilities, or the possibility of having such use monitored, but was aware of the technical possibility of being monitored, and regulated her use accordingly:

I'm under the impression there isn't a systematic checking, but I'm quite aware about email and Internet, that the technology exists to check. So I wouldn't kind of send things by email that I wouldn't want to fall into the wrong hands.

(Faculty Librarian)

With regard to the specific monitoring of access to web content, as opposed to use of email, the Internet Services Manager stated that this had been happening, although it was a result more of technical problems than a concern with the nature of content accessed. Monitoring of web use on a regular basis was not regarded as feasible, as 'we don't really have the tools to do it'. On-the-spot monitoring by librarians of content accessed in the Library was also seen as impractical and ineffectual. The Faculty Librarian reported that '...we just don't have the time to wander round and police what's going on...And if they see a librarian wandering round they're just going to go 'click' and it'll disappear'.

A self-acknowledged lack of computer literacy on the part of the Head of Equal Opportunities – who acknowledged that he had his emails and relevant information

from the web printed out by his Assistant for his review – meant that he had not given any consideration to policy on unacceptable use of email, or to issues related to pornographic or extremist Web content.

5.3.7 Other factors impacting on Internet Use

Respondents identified a wide range of factors that impacted on access to Internet content within the University College, including both internal and external forces. Policy making with regard to network use had been influenced by the conditions laid out in the JANET conditions of service and AUP, and, according to the Information Strategy Co-ordinator, the approaches favoured by bodies such as UCISA and JISC had also influenced policy decisions. The role of governmental legislative initiatives was highlighted, in particular the importance that the *Data Protection Act 1998* (Parliament, 1998b) holds for information policy decisions within the higher education sector.

Other factors identified by respondents included security issues and the use of access control mechanisms such as passwords; cost factors; licensing and copyright restrictions; technical limitations; technical ability and the availability of end user support and training; the requirements of confidentiality; and a lack of co-ordination and communication between departments involved in policy decisions and implementation. These many and varied forces all played some part in determining the ease of access to online information experienced by students and academic staff at the University College.

5.3.8 Institution A – some conclusions

Although some of the factors limiting access to Internet content that are described above were beyond the control of the University College, it was clear that the impact of some of the decisions that had been taken to block access to specific sites risked constraining the freedom of enquiry of both academic staff and students. This applied to both politically sensitive and sexually explicit content.

Moreover, this impact had been significantly compounded by the lack of transparency and communication of blocking decisions.

Subsequent to the carrying out of the fieldwork, an illustrative example arose of the impact on academic freedom of measures to regulate access to Internet content at the University College. A member of the library staff who was embarking on a Masters research project, exploring 'alternative librarian websites and stereotyping of the profession' (personal email, 2003), contacted the author of this report to seek advice. In order to carry out his research work, he needed to browse a number of web sites, some of which he felt might contain sexual content, ranging from the mild to the fairly explicit. He had contacted the Computer Support department, in order to alert them to the fact that he might be accessing some sexual content and explained the context for this access. To his dismay he had been informed that he should 'desist immediately from using [the University College] facilities and equipment (including any used by you elsewhere that is the property of [the University College]) for such purposes and delete any information that you have accessed' (cited from personal email, 2003). His attention was then drawn to the University College *Regulations and Conditions for the Use of Computing Facilities*, in particular:

> 'The creation, display, production and circulation of offensive material in any form or on any medium is forbidden.'

No provision is made within the *Regulations and Conditions* for bona fide academic research on controversial topics. In addition to this advice, the enquirer was reminded of the disciplinary procedures cited in the *Regulations and Conditions* that could be invoked in the event of failure to observe the terms and conditions of the Regulations. This response had left him feeling 'despondent and isolated', and he was contemplating having to change his dissertation topic to one that would not pose such an obstacle.

The overall picture portrayed by respondents of policy making with regard to Internet access within the University College was one of disjointed and fragmented

approaches with a lack of a consistent or coherent approach to the resolution of issues raised by attempts to control or limit access. Decision-making appeared to be largely reactive to events and to the demands of individuals, rather than being indicative of a rational attempt at problem solving.

In this respect, the model of policy formulation evidenced characteristics of the 'garbage can' process (Cohen et al, 1972; March and Olsen, 1976; Kingdon, 1984; Burger, 1993; Parsons, 1995; Rowlands and Turner, 1997; Sabatier, 1999). As illustrated in fig. 1.2 on p.31, within this model, the place that an issue occupies on the policy agenda depends largely on the importance attached to the issue by various players in the policy process, and problems tend to be 'constructed' in order to justify solutions. In the context of this case study, the lack of importance attached to issues of control of access to Internet content by other actors in the Information Strategy formulation sphere meant that decisions relating to blocking of content were left to the Internet Services Manager, whose chief preoccupations were the security and integrity of the server, as well as protecting her own staff from potential offence. She did not welcome the role of 'gatekeeper' and recognised the need for better policy definition that 'creates some boundaries' [her words] and which would thereby protect her from comeback from users.

5.4 Case study (2): Institution B

5.4.1 Institutional context

The second case study site, referred to throughout the thesis as 'Institution B', was a large, campus-based University. Institution B was research intensive with a high international profile for both teaching and research. The University prided itself on its strong links with industry, commerce and professional bodies. At the time that the fieldwork was carried out at the institution (between September 2000 and March 2001) there were approximately 11,700 undergraduate and postgraduate students registered with the University, the vast majority of whom were studying full-time. The University attracted a high number of international students,

particularly at postgraduate level, and there was a strong gender bias with almost twice the number of male students to female students.

The University Mission, as stated in the *Strategic Plan 1999-2004*, was

> *To increase knowledge through research, provide the highest quality of educational experience and the widest opportunities for students, advance industry and the professions, and benefit society.*

The Strategic Plan maintained that the University's ethos is characterised by 'a physical and intellectual environment that allows academic freedom and scholarship to develop…' and stated that this ethos is embodied through the 'fostering [of] an open and responsive culture which enables individuals freely to exercise their intellectual curiosity…'

The principal Academic and Administrative Officer of the University was the Vice-Chancellor, who was also Chair of Senate. There was a Deputy Vice-Chancellor with a broad policy brief for planning and strategic resource issues: his areas of responsibility included that of Information Services and Systems. In addition, there were two Pro-Vice-Chancellors, one with responsibility for research and the other with responsibility for teaching.

5.4.2 Information policy and strategy

In carrying out the fieldwork at this institution, it was evident that the approach to policy formulation and implementation with regard to computer use differed considerably from that at Institution A. The case study interviews, and the documents scrutinised, at Institution B all indicated that a significant amount of time and attention had been devoted to defining, implementing and promoting policy decisions with regard to the use of Information and Communication Technologies (ICT). In addition to a demonstrable maturity of its information and computing policy-making procedures, Institution B also had the most developed

ICT infrastructure of all three case study sites, with network access in 98% of bedrooms in University-owned student residential halls.

The University had a clearly defined *Information Strategy* that emphasised its commitment 'to provide high quality IT services in support of research, teaching and administration'. IT services were the responsibility of the Division of Information Services and Systems. At the time of the fieldwork a new Director had been appointed to this Division and a major review of IT support was underway. The *Information Strategy* had also just been revised.

Policy decisions with regard to Information Services and Systems were proposed by the Information Services Committee (chaired by the Deputy Vice-Chancellor), and ratified by the University Council, the highest policy-making body of the institution. At the local level, Faculty IT Co-ordinators (who were part of Computing Services) were responsible for establishing strategy and policy within their particular Faculty. This was ratified at the Faculty IT Committee, which was chaired by the Dean of Faculty and attended by members of academic staff from the Faculty. There was no student representation on the Faculty IT Committee.

In addition to the *Information Strategy*, the University had a range of policies and codes of practice with implications for the management and regulation of Internet use. These included a *University Computing and IT Acceptable Use Policy* (AUP); a *Hall Network Service AUP*; *Policy and Guidelines for Dealing with Computer Pornography*; and a *Harassment and Bullying Policy*. It was clear that considerable attention was paid to promoting these policies, with very visible notices drawing attention to their existence displayed in almost every corridor of every campus building. Information on acceptable use of IT was also provided in the introductory leaflet on IT services provided to new students by the Computing Services Department ('*Launching in…to IT, information and learning at…*').

Institutional policies regulating computer and IT use were seen by ICT personnel and Senior Management as being essential in order to protect the University from potential legal liability, as well as to prevent the University being subject to

adverse publicity in the event of incidents of misuse. In addition to systems personnel, Senior Management, academic staff and Trade Unions representatives had all been involved in the negotiation of policies such as the *Harassment and Bullying Policy* and the *Computing and IT Acceptable Use Policy*, on account of the potential workplace implications. In the period prior to the fieldwork, there had been a lack of student representation in such policy formulation, but this gap had recently been recognised, and, according to the Student Union Network Administrator, there was now a commitment to include such representation in future negotiations.

Policy formulation had been directly influenced by recent legislation, as well as by institutional bodies such as JISC and UKERNA. The local Vice Squad had also been consulted in some instances. UKERNA had been closely involved in determining policy with regard to issues arising from the provision of network services in student residential halls. The Student Halls Service Manager remarked that '…UKERNA tell us what sort of things they think we should and should not be doing legally...and in particular, the issue of port scanning[122] came from them'. Despite a more proactive stance being evident at Institution B, policy decisions were nevertheless often the result of specific incidents arising in the University. According to the Head of Network Services:

> *…a lot of the policy that I know of arose because of individual cases. Especially the halls service, which was very new to us at the time. And things happen in the halls that make us think, well maybe we should have written that up.*
>
> (Head of Network Services)

[122] 'Port scanning' is the systematic scanning of computer ports (connection points) to identify open doors into a computer. Port scanning has legitimate use in network management, but can also be malicious in nature with the intention of identifying a weakened access point through which to break into a computer. [Definition from that in Webopedia at <http://www.webopedia.com>, last accessed 5/7/2004].

5.4.3 Policy and Guidelines for Dealing with Computer Pornography

In its *Policy and Guidelines for Dealing with Computer Pornography*[123] the University aimed to clarify its position in regard to this issue with the following policy statement:

> *The University seeks to maximise the opportunities afforded by new information and communications technologies for teaching and research. In affording these opportunities to its students and staff it also requires that they be used responsibly and legally. In particular, making material available via the computer which may be offensive, obscene or abusive is not acceptable and may well render the perpetrator liable under the law. The ability to undertake a particular action does not imply that it is acceptable.*

The *Policy and Guidelines* document made reference both to the University *Acceptable Use Policy* and the *JANET Acceptable Use Policy*, as well as to the University's *Code of Practice on Sexual Harassment* (subsequently the *Harassment and Bullying Policy*). The document stated clearly that the University 'will not condone the use of its computing resources to access, store or transmit material of a pornographic nature *for personal use*' [researcher's italics]. No definition was given of what the University would consider to be pornographic material for the purposes of implementation of the policy (although reference *was* made elsewhere in the document to the nature of obscene material as defined by the *Obscene Publications Acts 1959* and *1964*). The policy advocated the reporting of Internet content that is suspected to be illegal to the Vice Squad of the local Police Force (who were involved in the drafting of the *Policy and Guidelines*). In particular, this applied to pornographic material of a paedophile nature or pornographic material containing references to bestiality. As part of the policy, a commitment was made to providing training for relevant personnel to learn more about the policy and how to deal with incidents that may arise. The interview with the library representative suggested that this training did, indeed,

[123] This section describes the Policy and Guidelines in force at the time of the fieldwork. The document has subsequently been updated and is currently [July 2004] entitled Code of Practice on ICT Pornography.

take place at regular intervals, and had been very effective in raising awareness of the issues involved.

Noting the commitment to providing '…an environment in which academic freedom, scholarship and initiative can flourish…' made in the University Mission Statement, the *Policy and Guidelines* stated that legitimate study or research into pornography and its associated issues provide the only permissible reason for accessing such material. However, '…individuals must be able to show that the access is necessary to their work or studies…' and were expected to take care to ensure that such material was not displayed in a way that would offend others.

According to the Head of User Support, who was responsible for the initial drafting of the policy, much of the impetus for the policy arose from a CVCP report into equal opportunities, which resulted in the establishment of the University's Sexual Harassment Panel and the subsequent appointment of a full-time Harassment Adviser (who was interviewed in the course of the field work). This also happened to coincide with the point in time (around 1994) in which Internet use was beginning to expand across the University. There was a growing impression that '…a lot of harassment cases seemed to rest on people being sent porn, or porn being displayed…so the Computer Porn Policy was developed as an adjunct to the Sexual Harassment [Policy]' (Head of User Support).

Fears regarding the potential legal liability of the University had been a strong policy driver with regard to the drafting of the *Policy and Guidelines on dealing with Computer Pornography.* The Head of User Support acknowledged awareness that 'as a University, we were running quite severe risks by not having proper policies'. These fears, together with recognition on the part of the Head of User Support of the importance of University-wide 'ownership' of the policy, had resulted in the involvement of the Harassment Adviser, a member of security staff, representatives from the local police Vice Squad, and a member of Senior Management of the University in the policy formulation. This involvement had also been achieved as a result of awareness-raising by JISC, together with events that had taken place within and beyond the University itself:

> *Fortunately, at that time, JISC was doing some work to bring this to the attention of the great and the good, and so it wasn't just me saying 'if we don't do this, then the VC or the Registrar might end up in gaol'… one of the reasons for it was the fact that enough things had happened in the world to bring it up to, if not at the top, close to the top of the list of things that are important. To the Registrar in particular, but also the Senior Management generally…We had a number of incidents which illustrated the dangers…*
>
> (Head of User Support)

However, this sort of reactive stance was criticised by the representative of academic staff on the grounds that 'hard cases make bad law', and that it was 'highly inappropriate [to formulate policy] around your aversion to the worst possible recent cases'.

5.4.4 Computing and IT Acceptable Use Policy

In a similar vein to the *Policy and Guidelines for Dealing with Computer Pornography*, the University's *Computing and IT Acceptable Use Policy* (AUP) acknowledged the importance of respecting 'the traditions of academic freedom'. The AUP complied with the conditions of both the *JANET AUP* and the Combined Higher Education Software Team (CHEST) *Code of Conduct*, and applied to all staff and students of the University without distinction of user status. The policy did not prohibit personal use of computer network facilities but established that this should be regarded as a privilege subject to withdrawal rather than as a right, and that such use 'must not interfere with the user's duties or studies or any other person's use of computer systems and must not, in any way, bring the University into disrepute'. Priority was always to be given to users needing facilities for academic work. On joining the University all students and staff were required to sign acceptance of the conditions of the *AUP*.

The Policy was drafted initially by the Head of User Support in Computing Services, with input from other members of Computing Services personnel and a member of academic staff, and was then scrutinised by the Information Services Committee, prior to final ratification by the University Council. Acceptable and

unacceptable use of University computers and network resources were clearly defined in the policy, the definitions given coinciding generally with those of the *JANET AUP*. However, it is clear that much consideration had been given to the precise definitions, which were often afforded greater clarity or expansion than those provided in the JANET policy. Thus, for example, it was noted that the propagation of offensive, obscene or indecent material (except in the course of recognised research or teaching) would normally be considered to be a much more serious offence than the retention of such material. Similarly, whereas defamation was defined as unacceptable use, it was noted that 'genuine scholarly criticism is permitted'. The interview with the academic staff representative, who had been involved in the policy formulation, suggested that these refinements reflected his input. The definitions were also accompanied by specific examples of use that would be considered unacceptable.

In addition to the general provisions of acceptable use, the policy also deals with issues of

- Authorisation and authentication – a user must not 'masquerade' as another user, withhold his or her identity or interfere with audit trails;
- Privacy – establishing the right of access to all files by authorised systems personnel, and to access to staff files by other members of staff only after the granting of relevant authorisation and where a breach of the law or of the AUP is suspected. Student privacy was not regarded as a right and 'students should not expect to hold or pass information, which they would not wish to be seen by members of staff';
- Behaviour – users were expected to take adequate precautions against malicious software, such as virus programs. In line with the University's *Equal Opportunities Policy* and *Harassment and Bullying Policy*, they were expected to refrain from distributing material that was 'offensive, obscene, abusive or illegal'. In addition, users should not make unauthorised copies of information belonging to other users.

The Policy made clear reference to the provisions of a number of legislative instruments, and summarised the main provisions relevant to the *AUP*. These included the *Computer Misuse Act 1990* (Parliament, 1990); the *Criminal Justice and Public Order Act 1994* (Parliament, 1994a) (with regard to harassment); the *Copyright, Designs and Patents Act 1988* (Parliament, 1998b); the *Trade Marks Act 1994* (Parliament, 1994b); and the *Data Protection Acts 1984* and *1998* (Parliament, 1984; 1998b). The document also gave attention to the implementation of the *AUP*, with clearly delineated responsibilities for supervision and management of the policy's enforcement.

It was suggested by one respondent that the need for universities to formulate an *AUP* was, at least in part, a response to the moral panic promulgated through the media:

> *I have no doubt at all that universities, not this one in particular, have felt compelled to construct an AUP in part because of that moral panic, which I think is very damaging…They do, I think, inhibit use inappropriately.*
>
> (Academic Staff Representative)

The policy document was accompanied by another, entitled *IT Acceptable Use Policy Procedures,* which outlined in some detail the procedures to be followed in the event of a suspected breach of the *AUP* and the potential penalties that may be applied in the event of a confirmed breach. This document also outlined the role and responsibilities of departmental 'AUP Advisers', who are involved in much of the local implementation of the *AUP*. In each department, one member of academic staff was appointed to this role, which carried responsibility for:

- Ensuring that everyone in the department was aware of the role of the AUP Adviser;
- Raising awareness of the AUP and issues associated with it;
- In most cases, dealing with any incidents of unacceptable use that arose in the department;

- Ensuring that cases in the departments were all dealt with in a consistent way;
- Developing local guidelines for the treatment of cases;
- Ensuring that appropriate student cases were reported on the relevant form provided by Computing Services;
- Referring major cases to Computing Services or to the Head of Department;
- Ensuring that all records kept were maintained in accordance with the *Data Protection Act 1998*, and that all data subjects were made aware that records are kept.

As with the *Policy and Guidelines on Dealing with Computer Pornography*, protection against legal liability had been a strong driver in formulating the *Computing and IT AUP*, and the associated procedures:

> *…if we were going to be sued for defamation, or prosecuted for racial harassment or whatever, or the complicated things to do with copyright, then we can all be held liable…The things which we were told are most important, I think originally it was educating members of the University so they know what their responsibilities are, and to be able to demonstrate that you've told them what their responsibilities are. And secondly, having procedures to deal with things…*
>
> (Head of User Support)

5.4.5 Hall Network Service Acceptable Use Policy

Problems with 'unacceptable' computer use at Institution B had intensified as a result of the extensive networking of student residential halls, and this move towards network provision in halls had also resulted in a shift away from public access computers in laboratories and in the library as the primary locus of computer misuse. In particular, Computer Services personnel were concerned to prevent students from providing server-based services from their Hall Network connection:

> *…most of the day-to-day problems that we have are coming from students misbehaving in the Halls Service and one of the things that they are not supposed to do is to provide server-based services to each other, or to the outside world…we have taken action so that all such server-based traffic is blocked, essentially on a hall-by-hall basis.*
>
> (Head of User Support)

The Student Halls Service Manager considered that the move away from a public to a private space, and the fact that students are paying to use the Halls Service, had engendered an attitude change:

> *Because students in Halls, it's their own accommodation, they're in their own room and they're using their own equipment. And they pay to use the network. So it's an attitude thing, because they think they have a right to do what they want.*
>
> (Halls Service Manager)

As a result of such usage, a *Hall Network Service AUP* was added during 2000 relating to specific aspects of Computing and IT use connected with the Hall Service. In addition to complying with the conditions of the University *Computing and IT AUP*, students using the Halls Network Service are explicitly required to undertake not to use any 'applications that are provided with the specific purpose in mind of breaking copyright legislation, such as Napster'[124]. In addition, the policy states the right of the University to "port scan" any machine and browse services running on the machine. Students who connect a wireless access point to the network point in their room are reminded that they will be held responsible for **all** network activity coming from their network point. They should not allow anyone else (other than Computing Services personnel) access to their Hall Network connection, and must not configure their machine to provide any service

[124] Napster is software that facilitates distribution and downloading of music on the Internet. Developed by a student, the software was made freely available on the Internet. Following legal action taken by the recording industry in 2001, Napster was withdrawn. It was subsequently re-established as a legal, commercial service in alliance with the multinational media corporation, Bertelsmann. Meanwhile, a number of similar (free) music downloading sites, such as Kazaa, rapidly replaced Napster. The search engine Yahoo! reported that 'Kazaa' was the most popular search term on the web during 2003 (BBC, 2003d). For more detailed discussion of this issue, see Lam & Tan (2001). For discussion of the impact of music distribution and downloading on the Internet in a University environment, see Oppenheim and Robinson (2003).

to other users in their hall, on campus or on the wider Internet. Connection to external services that use a significant amount of bandwidth, and which cannot be demonstrated as relevant to academic work, is prohibited, as is use of the Halls Service to attempt to gain unauthorised access to computing systems, data or other resources.

5.4.6 Harassment and Bullying Policy

The University's *Harassment and Bullying Policy* commits the University to 'fostering an environment where staff and students and those associated with University activities can work, study and live free from intimidation, aggression, coercion and victimisation' and undertakes to eliminate all forms of harassment and bullying. The policy originated within the Personnel Services department, and was given final approval by the Equal Opportunities Council. Members of academic staff and of the Trade Unions had been involved in the formulation of the policy, on the grounds that 'You have to have people from academic departments involved…because unless you do that, and they buy into it, then you'll never get it through' (Harassment Adviser).

Sexual harassment is defined by the policy as 'unwanted behaviour of a sexual nature, or behaviour of a hostile or offensive nature based on gender'. According to the policy, the display of pornographic materials, including computer pornography, can constitute sexual harassment.

Racial harassment is defined by the policy as 'unwanted behaviour of a hostile or offensive nature based on race or ethnic origin by a person of one racial or ethnic origin against a person or people of another' and includes (among other actions) written threats or insults, racist jokes, the display of offensive graffiti or insignia and incitement of others to commit racist behaviour. Similar definitions are provided for religious harassment, disability harassment and harassment on the grounds of sexual orientation.

The policy defines stalking as a form of harassment that involves pestering an individual, either in person, in writing including in electronic formats or on the telephone: it notes that this form of harassment is being more commonly reported.

The policy is implemented through a Harassment Panel, composed of trained members of staff from all areas of the University. It is intended to be educational in impact:

> *…telling people what harassment looks and feels like, rather than 'thou shalt not do'…So it says 'this is what it looks like, this is what it feels like and this is how we deal with it', it doesn't say 'you are a new member of staff, you shall not therefore…' Also, it's training sessions, rather than saying I don't want you to do this, but if you see this happening then you have the responsibility to report it…*
>
> (Harassment Adviser)

5.4.7 Filtering and Blocking of web-based information

The University does not use any proprietary website filtering or blocking software, on the grounds that it would not be 'appropriate to a University environment', but they do block some network traffic 'on a case-by-case basis' (Head of User Support). A technical solution is regarded as being problematic, inappropriate and ineffective in a University context:

> *…with the students, it's where do we stop, if you start blocking? It's very difficult to draw a line. There aren't really any very good systems that block materials which don't block other things that you don't want blocked as well.*
>
> (Head of Network Services)

However, at the time of the fieldwork, Computing Services personnel *were* investigating the possibility of blocking student access to Napster[125], on the grounds that its usage of bandwidth downgrades the network, which 'reflects on

[125] This action was subsequently implemented, together with the blocking of other similar services.

the service' (Student Halls Service Manager). They were also concerned about the potential legal consequences of providing access to a service that was being used by students to download copyright-protected materials.

The reluctance to engage in wholesale filtering or blocking of web use meant that Computing Services personnel did not generally receive user complaints about content being blocked, although there were exceptions to this:

> *The nearest we've had to that is someone who sent us an email saying they'd been trying to get to a pornographic site and he couldn't get through, and was it us blocking it?…he made no suggestion that this was anything to do with his academic work, sort of 'I can't get to this site that I've subscribed to, is it you blocking me?' and it wasn't as it happened.*
>
> (Head of Network Services)

The SU representative who was interviewed confirmed that he was not aware of any problems encountered by students being unable to access sites relevant to their academic work, as did the member of library staff who was interviewed.

5.4.8 Monitoring of Internet Use

Respondents from technical services reported that there is no policy of systematic monitoring of email or web use at the University, but systems personnel will respond to reports or complaints and – in the words of the Head of User Support – 'a normal part of your job is to keep an eye open for anything strange'. The emphasis of such policing relates to detecting use of the network to provide server-based services, or to engage in port scanning or hacking activity. Computing Services personnel are relatively unconcerned with the content of email communication or recreational web browsing ('Someone could be full-time looking at sport or whatever, but that wouldn't concern us' – Student Halls Service Manager). The decision concerning to what extent they should 'police' the network was recognised as being one that was fraught with difficulty:

> *The extent to which we actually police the network is a very big issue…Because sometimes, if you do police it a lot, you become responsible for what's on there, because you say you're looking. So if you don't police it then you can't claim responsibility, even though you've told them what not to do. But also you do need to police it to a certain extent, because you don't want it to get completely out of hand.*
>
> (Student Halls Service Manager)

In contrast with earlier years, at the time of the field work they had recently made a decision to engage in less proactive monitoring activity, and to concentrate their efforts more on educating students (and staff) with regard to acceptable use. One way that they were trying to accomplish this was through the display of very prominent AUP acceptance pages as students register for the use of network services. According to the SU Network Administrator, the prevalence of Acceptable Use notices and the emphasis given to educating students had led to a more proactive approach on the part of a substantial proportion of students with regard to self-policing their own use, and to reporting unacceptable use on the part of other users. The academic staff representative also confirmed that there was a 'general culture' of awareness of the possibility of email and Internet use being monitored. He did, however, express some concern that this had caused some anxiety among personnel in his department, and was of the opinion that it did deter some legitimate access of controversial material.

In a parallel with the findings of the case study in Institution A, the member of library staff at this Institution did not consider it feasible to conduct much in the way of policing of Internet use within the library. With over 100 open access PCs scattered throughout a large building, it was logistically difficult to monitor use. However, as with Institution A, some incidents of inappropriate material being accessed had come to light as a result of the administration of printouts of material. On these occasions, the persons printing out the offensive material had been written to, and asked to 'explain their actions'. None of these incidents had led to students defending their use of the material on the grounds of academic need: in contrast, their approaches had been those of accepting it was a 'fair cop', and agreeing to refrain from such use in future.

Within the library, staff adopted a 'deliberately vague' approach with students concerning monitoring of use, in order to create an environment in which students are uncertain about the extent to which monitoring is taking place, leading them to 'self-censor'. According to the member of library staff interviewed this approach, together with the installation of the Halls Network Service, had led to a dramatic reduction in the frequency with which instances of misuse occurred with the public access workstations in the library.

The technical set-up of the University network requires all network traffic to use compulsory proxy connections, and this means that systems personnel are able to keep a log of all web use from the University network. This log is kept for ten days, and, according to the Head of Network Services, has been used retrospectively to provide evidence of misuse. The member of library staff interviewed confirmed that there had been a couple of occasions on which it had been necessary to consult the logs to investigate use of the network by library personnel, although on both occasions no evidence of misuse had actually been detected from the logs.

Email traffic does get logged as a matter of course, and, on occasion, Computing Services personnel will view the content of individual messages, for example to determine whether it is junk mail. At the time of the fieldwork, there was no statement on employment contracts to the effect that email might be monitored, although it was recognised that this would need to be changed in response to recent legislation. However, staff were required to sign an agreement stating that they had read and understood the *Computing and IT AUP*, and agreed to be bound by it. Induction training of new staff was also used to raise their awareness of the AUP. Staff email lists were neither moderated nor monitored by Computing Services personnel – this was seen as a matter for individual departments to handle.

5.4.9 Computer Misuse at Institution B

This institution has a high proportion of technically able students of computer science; at times this had caused problems. To quote the Head of User Support:

> *…what we had last year…are people who know enough to go and find bits of software which will go around, well port scanning's the main thing…most of them are 'innocents abroad' in the sense that they think they're just exploring this great world around them, and mostly if you speak to them appropriately, plainly enough, then they respond…*
>
> (Head of User Support)

This theme of 'innocents abroad' was echoed by the Student Halls Service Manager, who commented:

> *We have some very technically competent students in the University, and they're experimenting, seeing what they can do. And some of it is meant innocently, but they're offending people without realising that they are.*
>
> (Student Halls Service Manager)

One example of computer misuse had involved a group of students who were found to be hacking into the computer at their former school. In such instances, Computing Services work closely with academic departments in any disciplinary action that is taken, in particular through the departmental AUP Adviser system. As a result of the technical aptitude and enthusiasm of the institution's students, the Head of User Support generally considered technical threats to be of greater concern than issues related to the volume of network traffic and bandwidth limitations, or to the accessing of computer pornography.

He did, however, acknowledge the high profile that issues related to computer pornography occupy on the public agenda but, in general, he was confident that the 'problem' of computer pornography, if not resolved, was at least being contained effectively within the Institution:

> *…I think we have a situation where there is a LOT of circulation of, I would guess, middle-ranging material, the sort of stuff that isn't actually illegal, or the Vice Squad would never bother to prosecute even if it was technically illegal. There's a lot of stuff at that sort of level, which I think is circulating among undergraduates and occasionally things pop to the surface and we deal with them. And so I think a lid is being kept on that in the sense that we don't appear to be getting worse, and we don't have large numbers of complaints…*
>
> (Head of User Support)

There had been instances of library staff complaining about students displaying indecent images on library computers, particularly during evening opening hours. However, in an institution with a high male to female student ratio, much of this misuse was regarded by Computing Services personnel as being the result of what might be described as a 'laddish' culture:

> *The overwhelming majority of the things that I personally deal with are young boys, usually fresh from school, who just aren't thinking about what they're doing. Or not thinking about the consequences of what they're doing…just acting a bit daft…dodgy pictures, sending jokes that have gone beyond decent taste, or sent to inappropriate groups of people…lots of things of that sort.*
>
> (Head of User Support)

Nevertheless, the Head of User Support considered it important to adopt a 'zero tolerance' approach, and to 'set the cultural guidelines' by responding to all incidents. Usually this involved requiring the student(s) concerned to attend a meeting with him. This approach was generally considered to be effective, but there had also been incidents where stronger action had been called for. In at least two cases involving University staff, the co-operation of the police in the form of the local Vice Squad had been sought. These cases had resulted in the dismissal of University personnel, and in at least one of the individuals concerned being placed on the Sexual Offenders' Register.

The Halls Service Manager gave an example of how some students caused offence through the username that they used to connect their computers to the network:

> *…when they put your computer on the network, you have to give it a name. And we advise them what they should use for a name. Some of them name their computer the most amazing things. And that can offend people. Cos when you go to look on the network you see ****** so in that sense, they don't know they're offending people by doing that.*

Similar issues arose as a result of the use of 'inappropriate' images as background graphics on computer screens, causing offence to other students and to Computing Services personnel. The Student Halls Service Manager acknowledged that this could be a problem, even where the material concerned did not amount to pornography:

> *…if you talk about the wallpaper, it might just be a picture of a woman, she might actually have clothes on, so it's not pornography but it's still treating a woman as a sex object.*
>
> (Student Halls Service Manager)

None of the personnel or student representatives interviewed had encountered any problems with users accessing or disseminating racist or extremist political material. The University had, however, encountered difficulties as a result of detection by the Federation Against Software Theft (FAST) of a student distributing copyright-protected software. The benefits of having properly defined policies were illustrated in the course of this incident:

> *They [FAST] were extremely civilised in the way in which they behaved and the scale of what was going on was not sufficiently damaging to them or their clients that they felt they needed to take action, but it was clear that had we NOT adopted the appropriate attitude it would have been difficult for us, had we not already had a policy in place…we would have been on much less firm ground.*
>
> (Head of User Support)

Although FAST had recognized that the University did have appropriate policies in place, they had also commented on the lack of written procedures detailing the exact steps to be followed in specific circumstances and outlining the line of responsibility in particular situations. This comment had led directly to the

drafting of the *IT Acceptable Use Policy Procedures* document, as described on pp.190-191.

According to the Head of Network Services, there had been several incidences in the University of harassing or abusive emails being sent. Although this was generally student-to-student harassment, one case had involved a student harassing a member of library staff. In another case, a male postgraduate student had been dismissed from the University for sending 'unpleasant material' to a female student in the same department. Despite these incidences, technical staff did not look at the content of email messages as a matter of course, on the grounds that they 'didn't want to get into the area of censoring personal emails' (Head of Network Services).

5.4.10 Academic Freedom

When questioned about the existence of a policy on academic freedom, the Director of Information Services responded that this was 'taken as a given', and that, therefore, a documented policy was not appropriate. This was echoed by the Halls Service Manager, who commented that academic freedom was 'always in the back of our minds in anything that we do – I'm not aware of any statement, but obviously that is taken as read'. Despite the proactive approach to dealing with incidents of computer misuse, the Head of User Support was also confident that there was a real commitment not to jeopardise academic freedom in the University:

> *…what we're absolutely not about is curtailing academic freedom. What we're actually not about is curtailing legitimate academic activity of whatever sort. When the computer porn policy was being put together, one of the reasons it took so long to be firmed up was because of those academic freedom issues…*
>
> (Head of User Support)

They had involved a senior member of academic staff with strong views in favour of academic freedom in the formulation of the AUP. He commented:

> *…I think in a sense I was a token libertarian voice, there was a feeling that it would be sensible to hear someone who might not be as committed to a strong policing element…clearly there were concerns which I voiced about the extent to which people who, after all, in this department [Social Sciences], would be people who were doing research on some fairly murky topics, prostitution, paedophilia etc. could have their work confined inappropriately.*
>
> (Academic Staff Representative)

According to the Head of User Support, the AUP, in particular, was intended to reflect 'a culture which is permissive rather than restrictive'. This principle had been vigorously promoted by the representative of academic staff:

> *…there were probably more general concerns about the necessity, I think, to ensure that the AUP was driven first and foremost to encourage the use of the Internet for teaching, learning and research, rather than to contain it…at a fairly early stage, when drawing up the actual content of the AUP, I did point out that there wasn't a single positive statement in it anywhere saying that the University wished to promote the use of the Internet for teaching and research. It was entirely couched in terms of what you couldn't do, not what the University would like you to do.*
>
> (Ibid)

The original draft had been amended to reflect a more positive approach. The academic representative had also lobbied to ensure that the policy distinguished between the *accessing* of 'offensive' content and its *dissemination*:

> *Something I kept saying was why should we be overly concerned if people are accessing material we don't much like? It's the old problem with the obscenity law on offensiveness. What I find offensive, someone else might not. There are plenty of jokes about finding memos from [the Administration Office] offensive…offensiveness is indefinable.*
>
> (Ibid)

He goes on to note that 'offensive' content only becomes a problem when it is displayed or disseminated to others, for example through access in an open computer laboratory. Otherwise, simple access should not be problematised:

> *…we might frown on a lot of the uses, but why we should be either policing it or preventing it, seems to me unclear…in a university of all places, the leaning should be towards the encouragement of research rather than disabling it…a university above all else is an institution where freedom of speech and thought, and the opportunity to think the unpopular, ought to be cherished and protected…if people aren't free to access the dubious, the morally slightly 'iffy', then universities aren't doing what they ought to do.*
>
> (Ibid)

Although he recognised that some restraints were needed in order to maintain legality, he was concerned that 'the danger is to err on the side of constraints rather than on the side of being expansive'. With respect to his role as departmental AUP Adviser, he had adopted a hands-off approach, and, in fact, had taken no action against staff or students in his Department. He likened this approach to his behaviour in the offline environment:

> *I don't follow my staff to the bookshop to check that they're buying acceptable books, I don't follow them round the library to check that they're reading books that I don't find offensive, I cannot see why I should do so with the Internet.*
>
> (Ibid)

The Students' Union representative also spoke strongly in favour of a culture that maintained freedom of expression on the Internet:

> *I would hate to see the Internet being less of a free speech area. I think that's one of its beauties at the moment, that there are so many diverse opinions on there. And just like anything, you don't have to listen to those opinions if you find them objectionable, or they're not to your liking…I wouldn't like to see greater controls being put on the Net, to be honest.*

5.4.11 Other Factors Impacting on Internet Use

As in Institution A, regulatory decisions and mechanisms were not the only – or even the main – restrictions on Internet access. Despite having a well-developed network infrastructure at Institution B, at the time of the fieldwork problems with

the reliability of the network were inhibiting use. According to the academic staff representative

> *…I would say that's 99% of people's concern. I mean, it's the fact that the system is always down. Frankly, it's quicker to walk to the library than look something up on the Internet…I think most people would rather walk that ten minutes than spend it waiting for a machine to boot up and then get an error message. Basically, most people see the Internet as a generator of error messages. So I think they're so overwhelmed by the technical issues with the Internet that these other issues are very marginal.*
>
> (Academic Staff representative)

5.4.12 Institution B – some conclusions

Policy-making with regard to Internet access and use at Institution B appeared to be a product of much careful attention and widespread consultation, both internally and with external agencies. The issue was high on the policy agenda, and its importance was afforded clear recognition by members of the Senior Management team, not least on account of the potential legal implications involved. In addition to the attention paid to policy formulation and definition, it was evident that similar attention was paid to the implementation, dissemination and evaluation of policy initiatives. The effectiveness of the consultation process could be seen from evidence of the way in which comments made by participants had directly impacted on the wording of the policy provisions. This was particularly true with regard to the input by the member of academic staff concerning the promotion of the positive benefits of Internet use, the distinction drawn between access and dissemination of offensive materials and the protection of academic freedom.

Indeed, it was apparent that academic freedom was a genuine concern in the policy process, and due care appeared to have been taken to minimise the impact of proposed measures on intellectual inquiry and research. Overall, there appeared to be a widespread acceptance of the policy measures. In particular, the researcher was impressed with the consistency of the accounts given by individual interviewees. There was also a demonstrable coherence among the various policy measures, and a clear linkage between them and relevant legislative provisions.

However, despite the University's carefully considered and comprehensive policy formation, with widespread awareness-raising and dissemination, there was still evidence of incidences of abuse of network facilities, ranging from minor infractions to serious criminal activity. One of the more extreme examples came to light in 2003, when a Pro-Vice Chancellor of the University resigned his post and was jailed for nine months after a large number of child pornography images were found on his computer. The former Pro-Vice Chancellor, who was in post at the time that the case study fieldwork was carried out, admitted to surfing the Internet at work and at home in search of such images, as well as to disseminating indecent materials. The offences were ultimately detected by Police Officers working on Operation Ore[126], following an alert from authorities in the US, and not as a result of any University monitoring procedures. The findings from the questionnaire study, presented in Chapter Six, also indicated that, despite a high level of policy awareness among students, levels of misuse of computer facilities in the University remained high.

Although the decision-making process at Institution B demonstrated a move in the direction of a more considered and rational approach to policy formulation, with clear problem definition and democratic consultation, the ultimate failure of policy measures to successfully address the identified problem suggests that it would be inaccurate to present this case study as a perfect example of the 'rational actor' ideal of policy formulation (see fig. 1.2 on p.31). This model assumes policy-making is the outcome of rational processes based on perfect knowledge; policy implementation will be pursued consistently, unencumbered by external events and brought to a satisfactory conclusion (Rowlands and Turner, 1997; Burger, 1993; Turner, 1999). However, the limits imposed on the successful achievement of policy goals that resulted from the inability of policy actors to control all aspects of the policy environment at Institution B suggest that the notion of

[126] Operation Ore was a large-scale UK police operation aimed at intercepting an Internet paedophile ring. By November 2003 it had resulted in about 1,300 prosecutions from around 6,000 suspects. (See *Operation Ore: can the UK cope?* Available at <http://news.bbc.co.uk/1/hi/uk/2652465.stm> [Last accessed 5/7/2004]).

'bounded rationality' (Simon, 1957; March and Simon, 1958) is a more useful way of representing the actual policy process that was found to exist in the case study.

5.5 Case Study (3): Institution C

5.5.1 Institutional Context

'Institution C' was a large dispersed post-1992 University. A polytechnic prior to the removal of the 'binary divide', the Institution was originally a product of the amalgamation of a College of Technology and a College of Art. It had subsequently expanded through mergers with a number of specialist institutions and Further Education Colleges. At the time that the fieldwork took place (between April and September 2001 inclusive) the University had approximately 30,000 students (of whom over 30% were studying part-time) and around 4,000 members of staff.

The University aimed to build on its historical strengths in technical and trade education to become 'The leading University for professional, creative and vocational education underpinned by research excellence' (*ex* University website, January 2004). Considerable emphasis was placed on working in partnership with the local community; on knowledge transfer to industry and the local region; and on widening participation and being student-focussed (Ibid). The student intake of the University comprised a high proportion of students from ethnic minority backgrounds, in particular those from the Indian sub-continent[127].

The principal Academic and Administrative Officer of the University was the Vice-Chancellor; during the course of the fieldwork at this Institution, a new Vice-Chancellor took up post. The Core Executive included the Director of Finance, the Registrar and the Pro Vice-Chancellors. ICT services were the responsibility of the Department of Information Services and Systems (ISAS), headed by a Service

[127] This proportion was stated by one respondent to be around 25% of the total student population.

Director who reported directly to a Pro-Vice-Chancellor, Strategic Planning and Resources. IT and information policies were developed by ISAS and ratified through the University Information Services and Systems Committee.

5.5.2 Information policy and strategy

Institution C presented another very different picture of policy formulation with regard to the use of ICT. There was no single overarching Information Strategy document, although there was a plethora of advisory, policy and regulatory documents relating to ICT use. Many of these appeared to overlap in terms of content and remit, and indeed were on occasions directly contradictory in content. Academic staff in particular demonstrated a very low level of awareness of University policies relating to ICT.

At this Institution external agencies, such as the local Vice Squad, had not been involved in the drafting of ICT policies, but the policies of other universities had been used as a point of reference. According to the Director of ISAS 'what we did basically was to look at what other people were doing and interpret that within our own environments'. In this respect, he noted that consideration of the needs of the high proportion of Muslim students in the University had had a direct impact on policy decisions with regard to access to Internet content.

The organisational culture at the University was described by one respondent (Academic Representative B) as being 'bureaucratically hidebound, you need to find permission for everything'. The policy-making environment was described by the same respondent as being very centrally directed, unhelpful and rigid. These comments were mirrored by those of other academic respondents, who also spoke of policies being imposed by the centre and without consultation. One respondent [Academic Representative C] spoke of a 'big differentiation between the executive, the administrative and the academic branches' and a failure in policy making to recognise or use the expertise that exists within the academic staff in the University.

The Electronic Services Manager, responsible for implementing IT strategy in the University Libraries, offered a negative perspective on the policy formulation and dissemination process in the University:

> *I'm not awfully sure what the policy **is** here, that's the trouble. I mean the policy of the University is, as far as I can see, we don't have an IT Committee that oversees the work of ISAS in any sense. So really, they choose these things all by themselves and don't really refer out to the user body at all…they don't take user views…What does tend to happen in this place, and particularly with IT, is if you have a look on the Intranet you'll find a policy document and you'll think 'I wonder when that was?' And usually it'll have sat on the Intranet for a couple of months and somehow become policy by default, but then it becomes policy but doesn't really get referred to.*
>
> (Electronic Services Manager)

The account given by the Head of Human Resources (Policy and Development) describing the process of drafting and ratifying University personnel policies appeared to support this impression. Consultation during the process was limited to senior members of the Human Resources team, the University Core Executive, the Trade Unions and the Senior Staff Team ('All what you would call the managers in this organisation'). At this point a new policy would go for final approval to the executive body, consisting of the Vice Chancellor, the Pro-Vice Chancellors, the Deans and Senior Managers (according to the representative of Human Resources these would include 'Director of HR, Director of Finance, that kind of level, but not the level below'). It would also go to the Board of Governors for approval. The Head of Human Resources (Policy and Development) commented that the policy approval process 'can be a bit long-winded, but we're quite assertive in pushing it through the process'.

This lack of consultation or involvement of academics in policy formulation had resulted in a low level of 'buy-in' to policies, which, according to respondents, were generally perceived by academics as 'imposed'. However, a couple of respondents did make reference to the incoming Vice Chancellor, who had made a

public commitment to 'open and honest communication': they were optimistic that this might lead to a more open and consultative culture.

5.5.3 Guide to IT Legislation

During the period of the fieldwork at Institution C, ISAS produced a *Guide to IT Legislation,* which was made available to staff and students at the University via the University intranet. This included advice and guidance on a range of legislative instruments and issues, such as:

- The Computer Misuse Act 1990;
- Copyright;
- Data protection;
- Official Secrets Acts 1911-1989;
- Defamation – this included the statement:
  "In accordance with the Defamation Act 1996 the University acknowledges the convention of academic freedom but will take all reasonable care to avoid the dissemination of defamatory material and will act promptly to remove any such material that comes to its attention…You must…ensure those opinions and views expressed in personal home pages or via bulletin boards do not discredit their subjects in any way that could damage their reputation".
- Obscenity – here it was noted that:
  "The University is committed to the prevention of publication through any of the University's computing services of any material which it may consider pornographic, excessively violent or which comes with [sic] the provisions of the *Obscene Publications Act* 1959 or the *Protection of Children Act 1978*…Users of the computing services are reminded that these are principally for use in connection with academic purposes, therefore any use of the computing services to publish or gain access to obscene, pornographic or excessively violent material is inappropriate. You must not disseminate, access or encourage access to materials, which

the University deems to be obscene, pornographic or excessively violent through the University's computing services".

- Discrimination:

  "Inciting racial hatred by displaying any written material, which is threatening, abusive or insulting is an offence under the Public Order Act 1986…You must not use the University's computing services to place or disseminate materials, which discriminate or encourage discrimination on grounds of sex, gender, sexual orientation, race or ethnic origin".

- Criminal law – this section concentrated on the criminality of incitement to commit a crime, and advised users that they must not place links on Internet sites:
  - To sites which facilitate illegal or improper use;
  - To sites where copyright protected works, such as computer software, are unlawfully distributed;
  - To bulletin boards which are likely to publish defamatory materials;
  - To sites which display pornographic materials;
  - To bulletin boards which are likely to contain discriminatory statements.

5.5.4 Regulations for Using IT Facilities

The University *Regulations for Using IT Facilities* that were in place at the time of the fieldwork, and which applied to all users of the University IT facilities, concentrated principally on issues such as security and authorisation to use the facilities; licensing, copyright and Intellectual Property Rights; charging for the use of IT facilities; and use for commercial purposes. However, reference was made in clause 4.1 to personal use of University IT facilities with the statement that:

> *IT resources are provided to facilitate a persons [sic] work as an employee or student of the University. Use for other purposes such as personal electronic mail or recreational*

> *use of World Wide Web or Usenet News is not a right. Any such use must not interfere with the users [sic] duties or studies or any other persons [sic] use of IT facilities and must not in any way bring the University into disrepute.*
>
> (Regulations for Using IT Facilities, Clause 4.1)

Some reference was also made to offensive content, with the statement [6.3.14] that users must 'Not send or take any part in preparing any text, graphics or audio material which is offensive, abusive, obscene or defamatory or which may be unlawful'. Recognition was given to the fact that users may not be able to prevent the receipt of such material, but they were required to report its receipt or destroy it immediately. Similarly, clause 7.1.1, which concerned users' behaviour, required that users respect the rights of others and did not 'Create, display, produce, circulate or disseminate offensive material in any form or in any medium'. No definition of 'offensive' was provided, nor was any mention made of the requirements of academic research.

Users were reminded that they should comply with the requirements of other regulations and legislative instruments, such as the *University Student Regulations*; the *JANET AUP*; the University *Guide to IT Legislation*; the University *Internet Code of Practice*; and the University *Network Security Policy*. The *Regulations* were also accompanied by a document entitled *Notes on Procedures for Investigating Breaches of IT Regulations in the Case of University Employees.*

5.5.5 Student Regulations for the Use of ICT and Associated Software and Media

These regulations are disseminated to all students of the University via the handbook of *General Regulations and Procedures Affecting Students.* Again, the emphasis of the regulations was on security, licensing, copyright and virus protection, as well as reminding students of the need to comply with relevant legislation. However, with regard to personal use of University ICT facilities, students were in this document advised that they are 'only permitted to use

University computing or communication systems or software for the purposes specified in their programme of study or research'.

5.5.6 Internet Code of Practice

The University also had an *Internet Code of Practice*. Developed by ISAS over the period from 1997 (when ISAS first came into being as a department) to 1999, at the time of the fieldwork it had most recently been updated in February 2001[128]. The initial impetus for the policy had come from comments made by management consultants employed by ISAS who advocated the University developing its own AUP to supplement the *JANET AUP*. According to members of ISAS there had been some consultation with academic staff in the formulation of the policy, which was signed off at Vice-Chancellor level, but they had not involved external agencies, such as the Vice Squad, in drafting the policy. The Head of Security within the University had also been involved in the policy formulation. The academic personnel who were interviewed for the case study, however, were emphatic that there had *not* been any consultation with academic staff – even though one of the academic respondents had considerable expertise and was director of a research centre in the field of computing ethics [Academic Representative A]. Respondents demonstrated a very low level of awareness of the existence of this policy: even the Electronic Services Manager, responsible for IT services in the library which contains over 400 open access computer work stations, was not familiar with the contents of the policy.

Applicable to all students and staff at the University and to the use of all University online services, including email, the *Code of Practice* also referred computer users to the University *IT and General Student Regulations*, the *Guide to IT legislation* and the *JANET AUP*. A copy of the policy was given to all new students, and formed part of the Information Pack that is provided by the Human

[128] At the time of writing [January 2004] the wording of the Code of Practice appearing on the University website was unchanged from this version.

Resources department for new staff. It also appeared on the University intranet and was displayed on the walls of some of the computer laboratories. The Code noted that:

> *[The] University is committed to allowing its members the freedom to engage in academic investigation and scholarly debate and accepts that the use of the Internet makes a valuable contribution to the exercise of these. In addition, the University also aims to benefit from the Internet by presenting itself favourably to the rest of the world. The purpose of this Code of Practice is to ensure that the Internet is used in a way which is beneficial to all the members of the University, and which protects the good name of the institution and all its members.*
>
> (Internet Code of Practice, para.2.1)

In fact, the theme of protecting the University's reputation prevailed throughout the Code, together with that of the avoidance of potential legal liability. Considerable attention was paid to the issue of publication and dissemination of Internet content, whereas the issue of access of unacceptable content was given a much lower profile. This may be on account of the use of filtering software to deter such access from taking place[129]. With regard to such access, there was some recognition given to the needs of researchers, with the statement that 'Staff who by the nature of their research work need to have access to material which might compromise the position of the University or their own position must register their need to have access to such material with the Director of Information Services and Systems' (*Internet Code of Practice*, para.5.6). It was also noted that the Director of Information Services would keep a record of any such request (*Internet Code of Practice*, para.5.5). However, no mention was made of the action to be taken in the event of a student of the University requiring access to such material for academic purposes.

[129] As will be described later in the Chapter, there was institution-wide implementation of Websense filtering software.

5.5.7 Information Technology for Students: Guidelines for Use

This was a single A4 guidance sheet prepared specifically for students, which claimed to provide 'a summary of the most important points' of the various regulations and guidelines covering the use of University IT equipment, facilities and network services. In addition to the provisions outlined in the *Guide to IT Legislation*, the *Regulations for Using IT Facilities* and the *Internet Code of Practice*, these guidelines advised students that, unless it is to support their studies, 'surfing' across the Atlantic was outlawed on cost grounds. They were also advised to:

> *Ensure that what you do is legal, decent, honest and true.* ***Do not*** *[bold as in original document] receive, download, create, send or cause to be sent any material which may be offensive, abusive, obscene or libellous or which breaches University codes or which is illegal.*
>
> (Information Technology for Students: Guidelines for Use)

As with the *Internet Code of Practice*, no mention was made of what action a student should take in the event of a conflict between this clause and the requirements of their studies.

Additional advice provided in the guidelines warned students that 'The University retains the right to monitor all systems and networks used within or attached to the organisation or used on University premises'.

5.5.8 Draft Policy and Procedure for Dealing with Bullying and Harassment

This policy had been initiated by the Human Resources Development Team and a revised draft was being disseminated for consultation purposes in June 2001. It committed the University to 'providing a working and learning environment that promotes the dignity of every individual and is free from bullying and harassment on any grounds'. According to the Head of Human Resources (Policy and

Development), it had been reviewed specifically in order to make explicit that, as an organisation, the University accepted that email is a potential way of bullying somebody. In its scope it stated that it applied to all employees of the University, but it did not specifically mention application to students of the University[130]. The policy was available for staff to view on the University Intranet, and was communicated to new staff on their induction into the University.

Within the policy, the definition of sexual harassment included the 'electronic display or transmission of pornographic or indecent materials'. The definition of racial harassment included 'The display of racist graffiti or images' and 'The transmission of racially offensive materials or statements via electronic or other means'. Similarly, harassment related to sexuality was defined so as to explicitly include the 'Display of or electronic transmission of offensive materials'.

The Head of Human Resources (Policy and Development) noted the impact that European Union employment law was having on policy at the University, and the difficulty in balancing the duty of exercising a balance of care towards employees with that of protecting their individual rights. Thus, there was a duty of care to ensure that employees are not made to feel bullied or uncomfortable through another's use of email or the web. Further, the University aimed to promote 'a corporate culture where we do recognise diversity and that means creating an environment where people are comfortable and it's not macho' (Head of Human Resources, Policy and Development). At the same time, the implications of the *Human Rights Act* (Parliament, 1998a) meant that 'we have to be cautious in monitoring that we're not breaching anyone's rights, we have to balance the two together' (Ibid).

[130] However, clause 3.6 of the *Student Disciplinary Code* stated that 'harassment, including racial or sexual harassment of any student, member of staff or other employee of the University or any authorized visitor to the University' constitutes misconduct.

5.5.9 Code of Practice on Freedom of Speech

This appeared in the handbook of *General Regulations and Procedures Affecting Students* and all students, members of staff and visiting or guest lecturers at the University were required to comply with the Code's provisions. The initial paragraph stated a commitment on the part of the University to the principle of freedom of speech and expression within the law as being one of the 'cardinal principles upon which all institutions of learning should be founded' (*Code of Practice on Freedom of Speech*, 1.1). It also acknowledged recognition of the need to ensure that academic staff at the University 'have freedom within the law to question and test received wisdom, and to put forward new ideas and controversial or unpopular opinions' without risking losing their jobs or any privileges they may have at the University (Ibid). However, in common with the *Code of Practice on Freedom of Speech* at Institution A, the rest of this University's *Code of Practice* was concerned solely with issues relating to the organisation and conduct of meetings and lectures on controversial topics, or with controversial speakers.

There appeared to be minimal awareness on the part of staff at the institution of a policy relating to freedom of speech or academic freedom. For instance, when asked about the existence of such a policy, the Director of ISAS (who was ultimately responsible for policy decisions concerning access to Internet content) responded:

> *I can't remember whether we've got a policy, but there are, there is a generic policy, which says 'we treat our academics reasonably'…*
>
> (Director of ISAS)

5.5.10 Filtering and blocking of web-based information

The University used a commercial filtering software package, Websense[131], to limit access to 'inappropriate' websites. The Director of ISAS defined these sites as those containing 'material which is thought probably to be socially generally unacceptable, and that's generally in the area of pornography, but some violence also'. The software works by 'categorizing' sites according to their provenance and their content – so, for example, a university site would be categorized as 'educational institution'. Although the software was externally sourced, the University was able to amend the list of filtered sites in response to inappropriate blocking, as well as to add to the database of blocked sites by custom building its own categories.

This facility was actively used by the Network Management team, who acknowledged that the software sometimes 'gets it wrong', both in terms of blocking sites that shouldn't be blocked, and not blocking sites that should be blocked. The respondents from the team maintained that the software was not used to block political content, but was used primarily to block sexual content:

> *…we actually block on sex sites. It's quite amusing, it's an American site…Sex includes things like nudity as well. Now unfortunately, being America, bless them, we looked at nudity and found they'd blocked sites like, say, paintings, the Statue of David…So we went, mmm, OK, we're going to have to get realistic…What we get down to, we block explicit sex scenes, pornography…it's actual sites that contain graphic detail.*
>
> (Team Leader, Security and Network Management)

If users attempted to access blocked sites they would encounter a screen message that advised them 'You are not authorised to access this site – contact ISAS to request access'. If they wished to pursue access, they would then be required to complete a form stating the academic purpose for which they required access, together with the location and time at which they wished to access it. This form

[131] <http://www.websense.com> [Last accessed 5/7/2004]

had to be countersigned by their Dean of Faculty. At the time of the fieldwork, the Network Management team estimated that they received on average ten requests a month for access to blocked sites, of which at least 90% would be granted. According to the Team Leader, Security and Network Management, if access was granted, their policing role was still important:

> *What we actually specify then is, OK, we will do it, but the PC has to be in a) a secure area, obviously locked b) you are responsible for who actually has access to this machine, and the other thing we always say is, just because we're allowing you access doesn't mean we're not keeping an eye on you.*
>
> (Team Leader, Security and Network Management)

The implementation of the software appeared to have resulted in a significant shift of power in favour of the systems personnel, with the Team Leader commenting 'You can only get to where we want you to get to, the rest is denied'. However, information was not made available to other personnel about *what* categories of sites were blocked, and respondents demonstrated a considerable degree of uncertainty about this. The Electronic Services Manager, for example, commented with regard to Websense that 'I don't know what it is blocking…I don't know what they block now, but I know they don't block things like chatlines…'

According to the Director of ISAS, a major impetus in the decision to use filtering software had been concerns over the use of bandwidth. This appeared to have been of greater consideration than issues of legality:

> *It was done on the basis that anecdotal evidence tells us – not just here, but elsewhere – that maybe a proportion of bandwidth, a significant proportion, is being used, mainly for moving coloured pictures…and we're not funded to supply that, what we're funded to do is to supply educational services and it's an economic decision really…I don't think it's a legal issue because I think it's very difficult to actually decide whether something is unacceptable or legal or illegal.*
>
> (Director of ISAS)

This concern with cost and the use of limited IT resources as a major policy impetus was echoed by the Head of Security. However, the Security and Network Management Team Leader identified a rather different driver for implementing the software:

> *The biggest reason, I would say, why we drew it up to start off…if they [prospective students] bring parents, as they do, to have a look at the University, and they're walking round and see all these banks of PCs, if we can say, 'oh, by the way, we don't allow access to pornography at [Institution C], we will block it and we will actively pursue people who are trying to get to these sites', we thought it was a bit of PR as well.*
>
> (Team Leader, Security and Network Management)

This theme was echoed by the User Support Manager, who commented that the main policy driver had been 'Literally, embarrassment…we need to preserve our integrity and public face'. Academic staff also cited protecting the reputation of the university as having been a strong policy driver in the use of filtering software: according to one member of academic staff (Academic Representative B) the University 'was not a self-confident institution' and this tended to lead to an over-regulated and over-cautious approach. Another academic commented on how the University had been able to implement the software with relative ease:

> *There are tendencies for articulate technologists to 'bamboozle' academics. By which I mean that the non-technological academics are apprehensive towards the claims made by the technologists. They don't have the confidence or knowledge to argue against the need for controls.*
>
> (Academic Staff Representative A)

In addition to blocking sites with sexual content, the Security and Network Management Team Leader had been keen to prevent access to chat sites as well ('Nothing would give me greater pleasure'), but described how the new Vice Chancellor had not been in favour of this:

> *In fact, I actually mentioned it to [X] our Vice Chancellor, who said 'well does it cost us anything, is there any reason, does it hurt us?' I said,' well no, I don't suppose it does', so he said 'well, why should we? It's not breaking any laws, yes it's using our resources,*

but what's the specific motivator for this, are people actually complaining about this?' People were complaining about people accessing pornography, nobody was complaining about people accessing Web chat.

(Security and Network Management Team Leader)

Prior to the establishment of ISAS, the University had historically had 'very open' systems (this comment was made by a number of respondents). As a result, in the initial stages, the implementation of the software had met with considerable resistance from academic staff – 'a lot of Big Brother emails flying about' – but technical, security and human resources personnel all stated that they believed that the need to protect the University systems and ensure acceptable use of the Internet had gradually gained recognition and this had led to acceptance of the filtering policy.

However, academic staff interviewed for the study stated that they did not support the implementation of filtering and monitoring systems. Concern was expressed over the potential conflict between the needs of teaching and research and measures to limit access to controversial material. One member of academic staff (Academic Representative C), involved in teaching a module on 'Democracy in the Electronic Age', was concerned about the potential for blocking politically sensitive material. His students were on occasion required specifically to look at racist, homophobic or extremist material available on the Internet. He gave one example:

There would be an occasion for them to be going into BNP sites or whatever, particularly in the context of the election results, where the BNP has scored highly, the number of seats, where there is all this rioting going on…it's the sort of thing we would set our students in this department, going on to look at these things, to look at the types of information that's available on the Internet.

(Academic Representative C)

Another academic respondent commented:

> *As a researcher, I'm very Web-oriented, most of my information is sourced from the Web. The controls [i.e. Websense] impose a mechanistic constraint on where you can access data from. For example, within our Centre, there may be a researcher who wants to look at issues related to pornography. The sites they will need to access are likely to be blocked, and it is very difficult to unblock access.*
>
> (Academic Staff Representative A)

He gave a specific example of an occasion where he had had legitimate cause to access a blocked site, but had not been successful:

> *I tried to request access, but couldn't get a response. Those responsible for implementing the filtering software don't always understand the practical problems it causes.*
>
> (Ibid)

This conflicted with statements made by the technical team, the Electronic Services Manager and the respondent from the Human Resources department, all of whom maintained that it was very easy for researchers to gain access to blocked sites. The same member of academic staff (and others) also commented that access to 'legitimate' [non-controversial] sites is sometimes blocked in error.

One respondent in particular was unhappy with the lack of consultation that had taken place prior to the implementation of Websense:

> *…the question of filtering in the institution has never been articulated or debated. It was imposed. The rank and file academics like myself were not consulted. More and more information in academia is Web-based and there needs to be proper consultation on decisions like this.*
>
> (Academic Staff Representative A)

He did recognise legitimate concerns over the security and integrity of the University network, but felt that the use of filtering software was 'different from the necessary use of firewalls and other security devices, which I don't think anyone would argue with' (Ibid). While he recognised that there was an issue concerning the legitimate use of university resources, he noted that:

Constraints on access pose a big problem for us. They risk stopping us from delivering. The problems posed by inappropriate use cannot be resolved through a knee-jerk reaction such as has dominated.

(Ibid)

However, the representative from the Human Resources department was confident that adequate discussion *had* taken place prior to the implementation of the software. She commented:

We checked with the Deans at the start of the programme, and everyone was comfortable with this, there's been an academic discussion about the effect on students and the content of the material in the classroom and that's fine.

(Head of Human Resources, Policy and Development)

5.5.11 Monitoring of Internet Use

With regard to the monitoring of emails, the Director of ISAS declared that this did not take place in the University in a systematic way, but that they would respond to specific cases that required investigating. The Security and Network Management team also confirmed that, apart from virus checking, there was no systematic email monitoring.

However, although there was a lack of knowledge among academic staff about any University policy on monitoring of staff email, academic staff were concerned at the possibility that their email could be monitored:

The real issue with monitoring is why our emails should be monitored, and where do you start from? There is a tendency with software to monitor and collect data per se. This changes the relationship between those controlling the monitoring and those being monitored. Previously, before this technology was used, there would have had to be a good reason to investigate someone's correspondence. Now it is so easy to monitor, they don't need to have a reason.

(Academic Staff Representative A)

This respondent went on to discuss the dangers posed by the potential for data profiling (for example, to draw up the profile of someone who represents certain characteristics, run it against the profiles of university personnel, and monitor the emails of anyone who 'fits'). He accepted the desirability of filtering for specific beneficial purposes such as the detection and elimination of viruses, but was concerned that 'with all new technology, there is a tendency to use facilities for a purpose they weren't intended' (Ibid). Therefore, he felt it was important to know what guidelines had been laid down for members of the security team, and was concerned that there was no information provided about 'who is monitoring, or why' (Ibid). He said that colleagues had reported to him instances of having their email monitored.

Another member of academic staff had not encountered any direct evidence of email being monitored at the University, but he did comment that other colleagues had said that they did not want to continue particular email exchanges because 'they knew it would be monitored' (Academic Representative B).

When the Head of Human Resources (Policy and Development) was interviewed, she appeared to contradict the statements from the Director of ISAS and the members of the Security and Network Management team with regard to the monitoring of email, although she acknowledged that email monitoring in the institution was less systematic than were the controls on Web use:

> *We do monitor them, we flick through people's emails as well for certain words, and things like that, but I would suggest that on the email, as opposed to Internet access, we're probably still running more on a trust-based system.*

According to her, some personal use of email was deemed acceptable, although this policy was itself open to review:

> *I feel very strongly that if we're going to let people, we do actually let people send personal emails, to make it very clear that this is a privilege that can be taken away at any*

*moment, and we're very clear with the Trade Unions that it really is in the hands of their members as to whether **I** [researcher's emphasis] continue with this policy or not.*

(Head of Human Resources, Policy and Development)

This respondent was also of the opinion that the provisions of the *Human Rights Act* (Parliament, 1998a) might result in the withdrawal of this privilege: she felt that allowing personal use as well as business use might adversely affect the University's right to monitor email use.

5.5.12 Computer Misuse at Institution C

According to the Director of ISAS, the University had not experienced any instances of computer misuse that were sufficiently serious to require police involvement, although they had had incidents that had resulted in the dismissal and resignation of personnel. This had involved the inappropriate use of network services at the expense of work output, rather than issues concerning the access of socially, legally or morally 'unacceptable' content.

However, the Security and Network Management Team Leader described how, prior to the implementation of filtering software, they had detected that 'over 20% of websites accessed at [the University] were going to pornographic sites'. They had then looked at who was accessing these sites on a regular basis, and found that the seven heaviest users were all members of staff. None of this usage was claimed to form part of legitimate academic study. The Security and Network Management Team Leader described how they dealt with such users:

What we tend to do then in that situation is…we'll go and see D [the Head of Security] and say 'D, at these times of the day on this PC has been accessed pornographic material, what are you going to do?' And he'll say,' what time of day? I'll catch them'. And on one given day…the PCs were impounded. Nobody was actually sacked. There were some resignations.

(Team Leader, Security and Network Management)

He went on to describe a particular case:

> *One of the PCs, we could have sold for a fortune, it had the most impressive collection of porn I've ever seen…It was all categorised – it was an ex-librarian and it was all categorised and listed. It was impressive, wasn't it? [addressed to his colleague].*
>
> (Ibid)

The member of staff responsible for this 'collection' had subsequently resigned his position. During the interview with the Security and Network Management team, it was apparent that the team approached their 'policing' role with some enthusiasm. Although the Security and Network Management Team Leader did express some reservations about having to report individuals ('it's a hard thing to do because you could, in effect, be ruining someone's life'), he went on to justify his actions on account of the potential financial saving to the University:

> *It doesn't stop us enquiring though, does it?…Having a little dig…It's breaking lots of University policies and it's costing the University money. Pay in the time that the person's spending on it, which can be a lot of time, and also in actual bandwidth to America, where all these interesting sites are. It does cost money, so yes, we feel we have to pay our wages back to the University as well [laughs].*
>
> (Security and Network Management Team Leader)

In one instance, he had been involved in a disciplinary hearing against a member of staff who was spending a lot of her work time using Web chat ('expert witness, I think they called me', he noted). This member of staff had also subsequently resigned (an outcome described as 'Result!' by the Security and Network Management Team Leader, whose role had been primarily to compile the usage logs for her computer).

With regard to student misuse of network services, it was considered that the implementation of filtering software had been successful in terms of reducing their access to unacceptable content, especially pornographic material[132]. According to

[132] The results of the student questionnaire carried out at the institution appeared to support this claim, with none of the students acknowledging use of University network facilities to access

the Security and Network Management Team Leader, such access had previously caused problems, with female students complaining about male students accessing pornographic material in open access areas like the library and the computer laboratories. The Electronic Services Manager, based in the Library, confirmed that this had happened on occasion, but did not feel that it had been a frequent problem. However, there was now increased concern about students being engaged in the *production* of unacceptable Internet content, a fact that was reflected in the emphasis on content production in the University policies.

As was the case in Institution B, they had experienced problems with students using University computers to provide server services. They had resolved this by delegating the role of monitoring outgoing network traffic to technicians in the Faculties:

> *We sold it to all the technicians in all the Faculties, saying, this is a wonderful opportunity for you to control your area. And they were very keen, some of them. They said, yes, this is **my** area.*
>
> (Team Leader, Security and Network Management)

Respondents, such as the Head of Security and members of the Security and Network Management team, stated unequivocally that they would involve the police should there ever be any instances detected of access via the University network of pornographic material involving minors or animals, but to date this situation had not arisen.

However, in contrast to the statement by the Director of ISAS that the University had not had any cause to involve the police in cases of computer misuse, a member of the Security and Network Management team described a case of email harassment that *had* resulted in police involvement. In this instance, a student had used the University email facilities to send threatening emails to a celebrity. The

---

pornography, compared with 36% at Institution B. See Chapter Six for a more detailed outline of these findings.

police had been called in, but the Security and Network Management personnel had found themselves having to act as technical advisers to the police:

> *…that time the Police came in, they knew one hell of a lot less than us…I think they were finding out a lot from us…I don't think they'd been around for very long. I think it was a case of, we've got some Police Officers, you're now in charge of electronic security and protection, and arresting people who do this…we showed them how things worked.*
>
> (Team Leader, Security and Network Management)

The Head of Security also commented on this particular case, and expressed concern at the volume of 'inappropriate' email messages sent by students. He suggested that, where student email is concerned, some systematic monitoring *does* take place:

> *…about a year ago the University started monitoring some of the messages and they were surprised by the nature of what they were sending to each other. You've got to be very careful, it can come across as harassment and bullying.*
>
> (Head of Security)

The representative from the Human Resources department believed that instances of email 'bullying' were generally the result of ignorance rather than intent: for example, not understanding the impact of the use of capitals, being overly brief in composing email messages, or omitting to use please and thank you. She favoured an approach based on raising awareness of these issues rather than one based on punishment. As a result, a working group was currently finalising guidelines on the use of email, providing advice on netiquette, use of capitals and tone of language.

In fact, a number of respondents at the Institution noted the importance of the role of education in encouraging responsible use of network facilities, although this area did not appear to be without problems. The User Support Manager commented that 'The University has a chequered history on IT training', which came under a different department altogether from that responsible for the technical provision and security of the network (ISAS). The Electronic Services

Manager also commented that '[Student] IT training in this institution is a bit diverse, it's a bit scattergun. I don't think the students get any by default'.

5.5.13 Academic freedom

The focus on regulating the Internet use of University personnel at Institution C was perceived by academic staff as posing a threat to the relationship of trust between managers and academics at the Institution. One respondent, noting that the vast majority of academic staff made 'legitimate use' of university Internet access for their work, commented:

> *There is a real issue of trust, which was taken as a given in the past. The academic's role is based on outcomes, we're measured by what we achieve. With the advent of new technology, and the concern for what constitutes acceptable Internet use, the trust and outcomes basis has changed…this relationship of trust is potentially being changed to one of process and procedures, and risks modelling academia along industrialist lines whereby we have to justify what we do.*
>
> (Academic Representative A)

This undermining of the trust relationship was reflected in the comments of the respondent from the Human Resources department, who noted that originally the policy had been to have an entirely trust-based system, but that this had been abused by some members of staff. As a result, they had installed the Websense software, and:

> *We then moved on to making it very clear to people again what was expected, but also making it entirely clear that if they did anything outside of those expectations, if they tried to access sites which were deemed unacceptable, we would know, we have monitoring equipment.*
>
> (Head of Human Resources, Policy and Development)

The outcomes-basis of the academic role was also cited by another respondent with regard to use of the University network for personal use. Noting the fact that

his work pattern does not reflect a 9.00am – 5.00pm model, and that he makes considerable use of his home telephone and home computer for work-related activities, he did not consider that it should be regarded as a problem if he chose, for example, to look at the web at work to check the next football fixture:

> *I know that many employers are concerned with the amount of time that people spend on social or non-work-related Internet sites, and I think it is a potential problem in a job where you are paid to be there. But I think in an academic environment, where it is much more output oriented, my head of department isn't concerned with how many hours a day I spend working, he is simply concerned with how many publications I get out, how much research money I bring in, how much teaching I do. Those are the clear output criteria. So I could spend all day looking at millions of websites.*
>
> (Academic Representative C)

However, this viewpoint conflicted directly with that put forward by the Head of Human Resources (Policy and Development), who commented with regard to personal use of the web (even out of office hours) that:

> *Although there is monitoring equipment for email, we are very clear that staff may not use the Internet [sic] for anything that is not work related, we're very clear about that, with email you can, personal emails, but Internet absolute no no, you're not allowed to look at flight details, cricket scores…*
>
> (Head of Human Resources, Policy and Development)

With regard to controversial web content, while acknowledging the very difficult nature of having to respond to ideas and ideological perspectives that offend one's own beliefs, an academic respondent who taught politics noted that:

> *…very open access to ideas, to sources, what is then important in teaching is teaching people how to analyse those ideas and how to analyse the sources of those ideas.*
>
> (Academic Representative B)

This was echoed by another member of academic staff (Academic Representative C), who expressed his distaste for Holocaust denial, but also his disagreement with the German legislation criminalizing Holocaust denial[133]:

> *Simply because I think it stifles the debate and discussion…if the Holocaust denial debate was out in the open, it would be much easier to identify those people who are subversive against Jews, and to argue effectively against them.*

However, he was also clear that the concept of academic freedom does not imply unlimited licence:

> *I think academic freedom can only be defended when you are doing proper systematic research, and carefully constructed research. I think the idea of trawling round a pile of websites out of interest is not research, and I don't think it's defendable in that respect.*
>
> (Ibid)

5.5.14 Other Factors Impacting on Internet Use

Other restrictions on access to information on the Internet within the University cited by respondents included the increased tendency towards charging for information, including access to online newspapers and datasets. One respondent noted that this was a trend that was likely to grow. Similarly issues of copyright and Intellectual Property Rights were seen as exerting an inhibitory effect on access to information.

5.5.15 Institution C – some conclusions

It can be seen that policy-making at Institution C indicated a lack of consultation, particularly with regard to consultation with academic staff. Instead policy tended to be imposed from the centre, with a distinct differentiation between the administrative and the academic communities in the University. Academic staff

[133] Auschwitzluege Gesetz 1985.

tended to feel marginalized from the policy formulation process, and hence did not buy-in to policy measures. This situation was exacerbated by a lack of transparency in both the policy formulation and the policy implementation processes. Policy promotion, dissemination and evaluation also appeared to have received scant attention.

Furthermore, there was a wide range of policies whose remit overlapped, but whose provisions did not always demonstrate coherence, for example with regard to the acceptability (or otherwise) of limited personal use of network facilities, or policy with regard to the monitoring of email use. In some areas respondents showed a lack of consistency with each other in their answers, a situation that appeared to have more to do with a lack of awareness of what was actually happening within the institution than with a deliberate intention to distort the true situation.

The picture of an institution lacking in self-confidence, and therefore tending towards an overly cautious and regulated approach, was very clear. While policies did make reference to academic freedom, it was apparent that this was accorded a very low priority in comparison with the dual aims of protecting the University's reputation and avoiding offence, particularly with respect towards the sizeable Muslim community within the Institution. The exclusion of academic staff from the decision-making processes was risking the undermining of the trust-based relationship on which the University had previously operated, and was causing resentment towards what was perceived as an encroaching 'managerialism'.

The implementation of a technical 'fix' to regulate Internet use was accompanied by a lack of transparency as to the basis on which sites were filtered, or the extent of such filtering. Furthermore, the use of the Websense software had facilitated a significant power shift in the favour of technical personnel, who now had control over what information academic staff and students could access, and who appeared to derive considerable satisfaction from their role in policing Internet use. In

particular, the fact that the Security and Network Management Team Leader[134] had strong views against pornography had been allowed to exert a decisive influence over institutional policy formulation.

In an interesting turn of events, the technical solution had seemingly led to an example of the 'cockroach phenomenon' (Hosein et al, 2003). This refers to a situation whereby attempts to prevent a specific action lead to alternative (and equally undesirable) actions springing up to take their place. This could be seen in the changed emphasis on content creation once students found themselves unable to access existing 'unacceptable' content. It was noticeable that the technical solution had not generally been accompanied by a similar effort towards measures to promote education and awareness-raising of issues related to acceptable use.

At a similar point in time to the conduct of the fieldwork at Institution C, another study was carried out into a different area of policy-making at the University, namely that of the implementation of Closed Circuit Television (CCTV) within University premises (Prior, 2001). There is a high degree of similarity between the findings of Prior's study and the current one with regard to the policy-formulation process and environment at the University. Prior noted that the implementation of CCTV at the University had been initiated on the basis of assumptions and anecdotal evidence of an increase in security-related incidents, in the absence of any quantitative empirical evidence. There had been no consultation with academic, administrative or premises staff, or with students, all of who were subject to monitoring by the cameras. Furthermore, staff indicated a degree of uncertainty as to the extent and purpose of surveillance that was actually being undertaken. There were no plans for formal review or evaluation of the effectiveness of the implementation of CCTV: nevertheless, the University had submitted a bid to the Home Office for funding for a massive expansion in the use of CCTV. The author of the study suggested that staff had tolerated the implementation of the CCTV on the basis of an 'assumption of a benign

[134] This respondent made frequent reference to his aversion for pornography and his determination to prevent access to it.

organisational culture that was not out to spy on staff' (Prior, 2001). However, in parallel with statements made by respondents in the current study, Prior observes that increased employee surveillance tends towards a deleterious effect on trust and results in the deterioration of working relationships.

It was apparent that these examples of policy-making at Institution C could not be considered to fit the ideal of the 'rational actor'. They were based on imperfect knowledge; there was a lack of consideration given to all possible alternative modes of action; and there was an uncertain internal and external environment. When considering the case of this institution, the policy-making process appeared to align more closely with that of the 'bureaucratic imperative' (Burger, 1993; Rowlands and Turner, 1997; Turner, 1999), as outlined in fig.1.2 on p.31. This model has been described as decision-making that aims towards rationality, but that is impeded by the intervention of powerful organisational factors (Rowlands and Turner, 1997) and that is rules-governed (Burger, 1993). The policy confusion and lack of coherence or agreement between policies and policy actors, with a powerful impact on policy exerted by a small number of key actors, meanwhile was more characteristic of aspects of the 'garbage can' approach to policy-making.

5.6 Institutional policy formulation – conclusions

Although the picture of policy-making with regard to the regulation of Internet use demonstrated very different characteristics at each of the three case-study sites, it was apparent that all three institutions recognised a need to 'do something' about the use of network facilities. In part, this was a response to externally imposed constraints, such as the *JANET AUP* and relevant legislation, but it was also the result of concerns with the protection of institutional reputations, with the maintenance of a 'decent' and harassment-free working and learning environment, with the use of limited bandwidth capacity and with the potential for employees to 'waste' work time by engaging in personal use of the Internet.

It was apparent that measures taken to control Internet use were not without adverse consequences on the freedom of academic enquiry. This was true even in Institution B, where considerable efforts had been made to minimise this impact through a reliance on carefully drafted self-regulatory policy measures rather than through the imposition of technical constraints on access. Moreover, whatever measures were in place at each of the institutions, the occurrence of serious instances of misuse of online access had not been entirely prevented. At best, it could be argued that the evidence suggests that by having well-defined and disseminated policies in place, institutions are in a stronger position to protect themselves in the event of such instances occurring.

With regard to the different approaches taken by the three institutions, these appeared to be an accurate reflection of the maturity and self-confidence of each of the institutions. Thus, the least consistent and developed position was taken by the University College (Institution A), which was also the institution that had made the least provision for the protection of academic freedom. Although it had drafted some rules governing the use of computer networks, these were not actively promoted and decisions relating to Internet access were being made by the Network Administrator with no institutional back-up or transparency in the decision-making process. The picture was one of a relative 'policy vacuum', with a lack of consistent policy and a low priority having been given to the issue.

The post-1992 University (Institution C), which identified itself as being a 'not very self-confident' institution, evidenced a somewhat more developed and consistent approach, albeit one that was very top-down and that placed a high degree of reliance on the use of an externally sourced solution. Although some recognition was given to the importance of protecting academic freedom, there was evidence to suggest that the imposition of technical constraints were acting as an inhibitory force on academic enquiry. Policies had been developed without consultation with academic staff, and they were not well communicated. At the same time, network personnel were actively engaged in playing the role of 'policemen', and appeared to enjoy a high level of autonomy and power in this

role. The multiplicity of policy documents lacking in coherency or consistency could arguably best be described as 'policy confusion'.

The more mature and secure pre-1992 University (Institution B) afforded a much higher level of importance to issues of academic freedom, even though they also accorded a high place on the policy agenda to issues relating to the misuse of online services. They placed their reliance on well-developed and promoted policies, drafted in full consultation with academic personnel rather than on the imposition of technical restraints. There appeared to be a much higher level of awareness and acceptance of the policies and an overall policy coherence. Nevertheless, as will be illustrated in the next chapter relating to student use of online facilities, this reliance had not prevented misuse of these facilities.

At all three institutions, there was evidence of a significant shift in power relations away from academic staff and towards technical and managerial staff, who were seen to be able to exercise control over the sources of information to which the academic staff had access. This was most explicit in Institution C as a result of the use of technical constraints imposing a need to request the unblocking of sites from technical staff. However, in all three institutions, it was apparent that the ability of technical staff to monitor use of online resources was exerting a 'chilling' effect on individual use of such resources.

The next chapter will discuss student use of the Internet in the three institutions and their attitudes towards measures aimed at regulating this use. The findings of the questionnaire survey will be presented, and discussed briefly. Chapter Seven will be devoted to a full discussion of the combined implications of the findings of the case studies, the student questionnaires and the policy monitoring.

CHAPTER SIX: STUDENT USE – AND ABUSE – OF UNIVERSITY COMPUTER NETWORK FACILITIES

6.1 Introduction

The findings of the institutional case studies were supported by results from the questionnaire survey used to investigate students' use of computer networks, and their attitudes towards such use, at the three case study sites. The use of the questionnaire was intended to supplement the data collected from the case study research, which had thus far concentrated primarily on policy-making, implementation and impact from the perspective of staff at each of the institutions. Specifically, the questionnaire[135] was intended as an instrument to gather data on

- What use students in the three institutions were making of network facilities;
- What level of awareness they demonstrated towards institutional policies and regulations governing computer network use;
- Whether they were aware of any blocking, filtering or monitoring of their network use;
- Whether they had experienced offence as a result of other students' use of network facilities.

In addition, the questionnaire was used to explore students' attitudes towards

- Institutional filtering and monitoring of their Web and email use;
- Measures to protect their privacy in the online environment;
- Their expectations of the ability of students to bypass institutional controls on computer use;

[135] A copy of the questionnaire is included as Appendix Four.

- Their expectations of their own rights to impose controls on network use if they had responsibility for University network services;
- The rights of the Government to monitor email and web use in the interests of national defence and security.

These questions were intended to provide an insight into the effectiveness of the policy measures in place at the three institutions, and to determine what impact, if any, these measures were having on actual network use. They were also intended to explore students' experiences of, and reactions towards, measures intended to regulate their use of network facilities. The nature of the research question to be addressed, and constraints on the scale of the survey, meant that it was not intended that the data should provide a generalisable picture of students' experiences either across the sector or within the institutions concerned. The categorical and nominal characteristics of the data, and the variation in the size and composition of the sample groups, meant that it was not considered appropriate to make use of parametric statistical techniques to analyse the relationship between the different variables in the study. However, it was anticipated that the study would supplement the data obtained via the case studies by illustrating aspects of the impact of specific policy measures on a particular student group within each institution.

6.2 A note on methodology

The principles behind the design and administration of the survey questionnaire have been outlined in Chapter Two (Methods Adopted), and so will not be discussed in detail at this point. It would, however, be appropriate here to provide some context to the circumstances in which the survey data was collected. As it had been decided that the most effective means of administering the questionnaire was within a formal classroom setting, the number of respondents in each institution varied quite considerably, as did the composition of the student groups with regard to variables such as gender. The administration of the questionnaire within a classroom context did ensure that a high response rate was achieved, and

therefore the problems of bias associated with self-selected samples were avoided (Denscombe, 1998, pp.20-21; Moser and Kalton, 1971, pp.166-169; Harvey and MacDonald, p.126). The use of a purposive sample in a classroom setting enabled a response rate of 100% to be achieved (174 respondents in total), although a few students did elect to leave some questions unanswered. In order to collect the data during the course of a tuition session it was necessary to gain the co-operation of a member of academic staff in each of the institutions, and the researcher therefore made use of existing academic contacts within each of the institutions when selecting samples. Groups studying subjects with some relevance to the research topic were chosen, so that the member of academic staff was also able to use the exercise as an educational input for the students.

The student groups were as follows:

INSTITUTION A: Data was obtained from 27 final year undergraduate students taking a BSc in Computer Science. The questionnaire was administered in the course of a session on research methods.
INSTITUTION B: Data was obtained from a total of 129 second and final year undergraduate students. The group included students taking a BSc in Computer Science, a BSc in Computing and Management and a BSc in Information Management and Computing. The questionnaire was administered to students taking a module in Information Ethics.
INSTITUTION C: Data was obtained from 17 final year undergraduate students taking a BA in Public Administration and Managerial Studies. The questionnaire was administered to students taking a module in Democracy in the Electronic Age. In addition, one PhD student had also been invited to attend this particular session, and completed the questionnaire.

A more detailed breakdown of data on the composition of student respondent groups with regard to courses, cohorts, age and gender is provided in tables 6.1 – 6.4.

Table 6.1: Student course information

Institution		Frequency	Percent
Institution A	BSc Computing/Comp Science/Comp Eng	27	100.0
Institution B	BSc Computing/Comp Science/Comp Eng	50	38.8
	BSc Comp & Man	54	41.9
	BSc Comp & Info Man	8	6.2
	Not stated	17	13.2
	Total	129	100.0
Institution C	BA Public Admin & Managerial Studies	18	100.0

Table 6.2: Student cohort information

Institution		Frequency	Percent
Institution A	Final	27	100.0
Institution B	Second	55	42.6
	Final	65	50.4
	Not stated	9	7.0
	Total	129	100.0
Institution C	Final	17	94.4
	Post Graduate	1	5.6
	Total	18	100.0

Table 6.3: Age of student respondents

Institution		Frequency	Percent
Institution A	Under 25	20	74.1
	25 or over	5	18.5
	Not stated	2	7.4
	Total	27	100.0
Institution B	Under 25	115	89.1
	25 or over	4	3.1
	Not stated	10	7.8
	Total	129	100.0
Institution C	Under 25	14	77.8
	25 or over	2	11.1
	Not stated	2	11.1
	Total	18	100.0

Table 6.4: Gender of student respondents

Institution		Frequency	Percent
Institution A	Male	21	77.8
	Female	5	18.5
	Not stated	1	3.7
	Total	27	100.0
Institution B	Male	105	81.4
	Female	15	11.6
	Not stated	9	7.0
	Total	129	100.0
Institution C	Male	4	22.2
	Female	13	72.2
	Not stated	1	5.6
	Total	18	100.0
All institutions	Male	130	74.7
	Female	33	19.0
	Not stated	11	6.3
	Total	174	**100**

From these tables it can be seen that the majority of students were taking programmes with a strong computing element: the exception to this is in Institution C, but even here the students surveyed were those who had elected to take a module on electronic democracy. This was also the only institution where the sample group had a higher percentage of female to male respondents (72.2% of those stating gender): in Institutions A and B a significantly higher percentage of respondents were male (77.8% and 81.4% respectively of those stating gender). It can also be seen that all students were at undergraduate Level Two or above at the time of the field work: this was a deliberate sampling choice on the part of the researcher, to ensure that they had had spent sufficient time at the institution to have gained experience with institutional computing facilities and an awareness of any conditions of use of these facilities. The majority of students were under 25 years of age, although the sample group at Institution A did include a higher than average proportion of older students.

It is to be expected that the composition of the student groups will have exerted a considerable impact on their computer and network use. In particular it is possible that students undertaking programmes in computer science will be more able and inclined to engage in activities such as hacking and other misuse of facilities that requires sophisticated computing skills than students of other disciplines. It is also possible that in Institutions A and B the higher proportions of male student respondents may have impacted on the numbers of students reporting using University computing facilities to access pornography. Therefore, no attempts have been made to extrapolate from this data a picture of general student computer use across the institutions. However, the data obtained from the survey did enable the researcher to determine whether or not a proportion of the students at each institution are engaging in some form of 'unacceptable' use of network facilities.

The SPSS statistical analysis computer package was used to collate and analyse the data. Although this package is suited to the conduct of more sophisticated data analysis using parametric statistical tests, its use was chosen for this study on the grounds of its reliability for analysis purposes, and its ability to produce a range of useful and informative statistical tables. It also provides the researcher with a dataset that could be further manipulated in the future to extend the research beyond the current study. The findings are presented on a cross-case basis in order to facilitate a comparison between the institutions.

6.3 Findings

6.3.1 Student use of computing facilities

Students were asked whether they used University computing facilities to access email or the World Wide Web to assist with their academic work, for social or personal use, to assist with paid employment or business that is unrelated to their studies, or for any other purposes (Q.1). In addition to the pre-defined categories the 'other purposes' responses resulted in the creation of three further categories for analysis purposes: these were to host a website; to research career information

or to assist with job-hunting; and to assist with voluntary work. The results for the three institutions are shown in Table 6.5.

Table 6.5: Student's purposes for use of University network facilities

Use of computers	Institution A	Institution B	Institution C	Cumulative Total
Assist with academic work	26 (96.3%)	129 (100%)	18 (100%)	173 (99.4%)
Social/ personal use	25 (92.6%)	129 (100%)	18 (100%)	172 (98.9%)
Paid employment/ business	8 (29.6%)	63 (48.8%)	3 (16.7%)	74 (42.5%)
Career/ Job search information	0 (0%)	2 (1.6%)	1 (5.6%)	3 (5.6%)
Website hosting	0 (0%)	2 (1.6%)	0 (0%)	2 (1.1%)
Voluntary work	0 (0%)	2 (1.6%)	0 (0%)	2 (1.1%)
Other purposes	0 (0%)	1 (0.8%)	0 (0%)	1 (0.6%)

All of the students reported that they do use email and the Web; only one student (at Institution A) made no use of University computing facilities in order to do so. It is clear from table 6.5 that only a very small minority of students (two, both at Institution A) did not use the University network facilities for social and personal purposes, in addition to academic use: thus, overall 98.9% of respondents were engaging in non-academic or study-related use of University network facilities. Furthermore, almost half of the respondents from Institution B (48.8%) were making use of these for the purposes of paid employment or business that was not connected with their studies. This proportion was lower in the other two institutions, at 29.6% for Institution A and 16.7% for Institution C, but nevertheless was still significant.

In order to collect more detailed information on the specific nature of students' non-academic use of University computing facilities, they were asked whether **other than for purposes related to their studies** they had ever used University computing facilities for access to a range of specified content (Q.5). This content included sites related to their hobbies and interests; shopping sites; political material of an extreme nature; and pornography. One student at Institution B and one at Institution C responded that they had not used University computing facilities for access to any of these forms of content. In addition, two students (one at each of Institution A and Institution B) did not provide an answer to Q.5 at all. All of the remaining respondents had accessed at least one of these categories of content. The results are shown in Tables 6.6 – 6.10.

Table 6.6: Students reporting use of University computing facilities for access to sites related to hobbies and interests

Institution	Hobbies and Interests?	Frequency	Percent
Institution A	Yes	26	96.3
	No	1	3.7
	Total	27	100.0
Institution B	Yes	124	96.1
	No	5	3.9
	Total	129	100.0
Institution C	Yes	17	94.4
	No	1	5.6
	Total	18	100.0
Total Institutions	Yes	167	**96.0**
	No	7	4.0
	Total	174	100.0

Table 6.6 demonstrates that these students did make use of University computing facilities to gain access to Web content related to their hobbies and interests. A few even took the trouble to let the researcher know which sites they favoured (for example, Manchester City Football Club at www.mcfc.co.uk!). Although use in this context was marginally lower at Institution C, this difference was not found to be statistically significant.

Table 6.7: Students reporting use of University computing facilities for access to shopping sites

Institution	Shopping sites?	Frequency	Percent
Institution A	Yes	21	77.8
	No	6	22.2
	Total	27	100.0
Institution B	Yes	120	93.0
	No	9	7.0
	Total	129	100.0
Institution C	Yes	11	61.1
	No	7	38.9
	Total	18	100.0
Total Institutions	Yes	152	**87.4**
	No	22	12.6
	Total	174	100.0

The use of University computing facilities to access e-commerce sites was also very popular with students, particularly in Institution B where 93% of students had engaged in this practice. The proportion at Institution C (61.1%) appears to be significantly lower, but without further investigation it would not be possible to attribute a definitive causal factor for this. While it may be a result of the implementation of filtering software within the institution, it is also possible that students of computing have higher confidence levels with regard to e-commerce.

Table 6.8: Students reporting use of University computing facilities for access to games or gambling sites

Institution	Games or gambling sites?	Frequency	Percent
Institution A	Yes	15	55.6
	No	12	44.4
	Total	27	100.0
Institution B	Yes	88	68.2
	No	41	31.8
	Total	129	100.0
Institution C	Yes	2	11.1
	No	16	88.9
	Total	18	100.0
Total Institutions	Yes	105	**60.3**
	No	69	39.7
	Total	174	100.0

Again, use by students of University computing facilities for access to games or gambling sites was highest in Institution B at 68.2%. While the difference between this percentage and that reported at Institution C (11.1%) is particularly high, there is insufficient evidence to attribute causation to any single factor.

Table 6.9: Students reporting use of University computing facilities for access to pornography

Institution	Access to Pornography?	Frequency	Percent
Institution A	Yes	4	14.8
	No	23	85.2
	Total	27	100.0
Institution B	Yes	46	35.7
	No	83	64.3
	Total	129	100.0
Institution C	Yes	0	0.0
	No	18	100.0
	Total	18	100.0
Total Institutions	Yes	50	**28.7**
	No	124	71.3
	Total	174	100.0

Despite the policy emphasis placed by institutions on the prevention of access to pornography, the results of this study suggest that levels of this form of computer misuse is currently less prevalent among students than other forms of misuse. The results indicated that a much greater proportion of students engage in activities such as file sharing and music or software piracy (see Table 6.11 below). It is, of course, possible that this indicates the success of measures that have been adopted to curtail access to pornography, or that students were inhibited about acknowledging their use of such material but did not attach the same stigma to admitting engaging in activities such as copyright infringement. This may have led to a significant underreporting of access to pornography. However, the students were given strong assurances of anonymity and confidentiality and did not appear to be concerned about acknowledging their participation in other activities that they recognised as being in contravention of University policies or even in contravention of current legislation.

Gender may also have impacted on the responses to this question, with the highest levels of use of University computers to access pornography being reported in the respondent group with the highest male-female ratio (at Institution B). None of the female respondents in any of the institutions acknowledged accessing pornography via university computer facilities, in contrast to an overall statistic of 36.2% of male respondents. This zero-rating from female respondents contrasts with other studies, such as research carried out by Nielsen in September 2003 that reported that 29% of adult site visitors were female (Nielsen, 2003). It may be that females are more inhibited about acknowledging their use of university facilities for accessing pornography. The fact that residential halls' bedrooms are provided with network access may also have influenced the level of access to pornography at Institution B, with students more inclined to access such content in a private space. It is interesting to note that Institution C reported a zero level of access to pornography: this might suggest that the use of filtering software is very effective in this respect (either through preventing or through inhibiting access). However, it is also possible that the combined impact of a high female-male ratio in the sample group and a small sample size led to these findings.

Table 6.10: Students reporting use of University computing facilities for access to political material of an extreme nature

Institution	Extremist material?	Frequency	Percent
Institution A	Yes	5	18.5
	No	22	81.5
	Total	27	100.0
Institution B	Yes	23	17.8
	No	106	82.2
	Total	129	100.0
Institution C	Yes	3	16.7
	No	15	83.3
	Total	18	100.0
Total Institutions	Yes	31	**17.8**
	No	143	82.2
	Total	174	100.0

Positive responses to this aspect of content access were relatively even across the institutions, ranging from a low of 16.7% at Institution C through to a high of 18.5% at Institution A (with a mean of 17.8% across all three institutions). The respondents were not asked to provide further information about the specific nature of this content. Although levels of access to this form of content were considerably lower than for the other categories of content investigated in Q.5, the findings do suggest that a significant minority of students are using University facilities to explore politically extreme material on the Internet for purposes unrelated to their studies (see p.241).

The students were then further challenged with another question (Q.6) that asked them whether or not they had ever used University computing facilities for other specific purposes, such as to download or pass on software or music in contravention of copyright or licensing restrictions; to engage in hacking; to send hostile email messages; or to access material that they thought might be illegal. Despite the fact that they were being questioned about potentially illegal use of computing facilities, only two students (one at Institution A and another at

Institution B) provided no response to this question. The remaining responses are shown in tables 6.11 – 6.17.

Table 6.11: Students reporting use of University computing facilities to download or pass on software or music

Institution	Download software or music?	Frequency	Percent
Institution A	Yes	13	48.1
	No	14	51.9
	Total	27	100.0
Institution B	Yes	100	77.5
	No	29	22.5
	Total	129	100.0
Institution C	Yes	5	27.8
	No	13	72.2
	Total	18	100.0
Total Institutions	Yes	118	**67.8**
	No	56	32.2
	Total	174	100.0

The number of students admitting that they had used University computing facilities to download or pass on software or music, even if doing so breached copyright or licensing restrictions, was significant in all three institutions. The mean across all three institutions amounted to 67.8% of respondents (n = 118), with a high of 77.5% (n = 100) at Institution B. This mean of 67.8% corresponds closely to the findings of Oppenheim and Robinson (2003), who used a questionnaire to explore the use by Loughborough University students of online music file sharing services. In their study, 66% of student respondents acknowledged downloading music from the Internet.

These findings support concerns expressed by the British Phonographic Industry (BPI) about the scale of activity in UK Colleges and Universities with regard to downloading and sharing of music files, while reports carried out by universities themselves suggest that more than 50% of UK universities' Internet capability is used for illegal file sharing (Sherwin, 2003). Indeed, the BPI has announced that it

intends to prosecute universities that allow students to use their computer networks to copy music over the Internet, believing that universities are responsible for 'producing a generation of fans who believe that music is a commodity available free of charge' (Ibid). The International Federation of the Phonographic Industry (IFPI) has also threatened legal action in response to reports that 9.4 million Europeans visited the Kazaa site in October 2003 (Teather, 2003). However, the impact of file sharing on the music industry is not simple to determine: the research by Oppenheim and Robinson cited earlier suggested that students who downloaded the most music were also those who spent the most on purchasing music. Moreover, their interviews with the owners of record stores suggested that online file sharing was not having a detrimental effect on their sales.

There appears to be a strong gender bias with regard to file-sharing and music downloading activity, with 77.7% of male respondents across all three institutions acknowledging that they had engaged in this particular activity in comparison with only 24.2% of female respondents. Oppenheim and Robinson (op cit) also found a strong age bias, with none of their respondents over the age of 26 claiming to download music.

Table 6.12: Students reporting use of University computing facilities to access illegal content

Institution	Access illegal content?	Frequency	Percent
Institution A	Yes	5	18.5
	No	22	81.5
	Total	27	100.0
Institution B	Yes	54	41.9
	No	75	58.1
	Total	129	100.0
Institution C	Yes	2	11.1
	No	16	88.9
	Total	18	100.0
Total Institutions	Yes	61	**35.1**
	No	113	64.9
	Total	174	100.0

As part of Q.6 students were asked whether they had ever used university computing facilities to 'access material that you think might be illegal'. The figures in the table 6.12 indicating their responses to this question have to be interpreted with caution. Because students who had engaged in music downloading and file sharing were often aware of the illegal nature of this activity, some of them responded positively to the question on access to illegal content on account of these activities[136]. Therefore, it is to be anticipated that there was duplication between the two categories, and a positive response to the question on access to illegal content does not necessarily indicate access to other categories of illegal material such as child pornography or other obscene content. In fact, there were only three cases (one at each Institution) where the respondent had not engaged in file sharing or music downloading, but declared that they *had* accessed illegal content.

It would have been illuminating to have asked respondents about the nature of the illegal content accessed, but such a question was considered to be too threatening and intrusive to respondents to provoke an honest disclosure. At the very least, the statistics do show a relatively relaxed approach on the part of a substantial proportion of these students towards the access of illegal content, with 35.1% of respondents disclosing that they have accessed illegal content via University computing facilities.

[136] In some cases, they had written comments in response to the question 'Have you ever used University computing facilities for access to material that you think might be illegal?', such as 'yes, for music downloading'.

Table 6.13: Students reporting use of University computing facilities to send hostile email messages

Institution	Send hostile email messages?	Frequency	Percent
Institution A	Yes	3	11.1
	No	24	88.9
	Total	27	100.0
Institution B	Yes	18	14.0
	No	111	86.0
	Total	129	100.0
Institution C	Yes	5	27.8
	No	13	72.2
	Total	18	100.0
Total Institutions	Yes	26	**14.9**
	No	148	85.1
	Total	174	100.0

Again, the data on students sending hostile emails have to be interpreted with caution, as the findings are reliant on the students' own definition of what constitutes an 'email message that could be interpreted as hostile' (the wording of Q.6). This wording was a conscious decision on the part of the researcher, as it was considered that it was the intention on the part of the sender to cause offence or intimidation that was important. However, this does not permit a scientific measure of 'hostility' and does not provide an insight into the seriousness (or otherwise) of the level of intended or actual abuse.

It was considered possible that the gender profile of respondents might have impacted on the results to this question. Respondents at Institution C, where the sample had a strong female-male bias, were significantly more likely to report engaging in this activity. However, such an impact is not borne out by further analysis of the data: in fact, across the study male students were marginally more likely to report sending hostile emails than were females:

Table 6.14: Students reporting use of University computer facilities to send hostile emails, by gender

Gender	Send hostile email messages?	Frequency	Percent
Male	Yes	22	16.9
	No	108	83.1
	Total	130	100.0
Female	Yes	4	12.1
	No	29	87.9
	Total	33	100.0
Not Stated	No	11	100.0

As can be seen, across the three institutions 16.9% of male respondents acknowledged sending hostile emails, compared with 12.1% of female respondents. However, one should not read too much into these figures: as noted earlier, the statistics are based on self-reporting and it may be that males are more ready to admit to such activity. Alternatively, females may have a different perception of what constitutes a 'hostile email'. It is, nevertheless, clear, that a proportion of students have used University computing to knowingly send hostile emails, in breach of University policies, and that this was more widespread among respondents at Institution C than at the other two Institutions.

Table 6.15: Students reporting use of University computing facilities to engage in recreational hacking activities

Institution	Recreational hacking?	Frequency	Percent
Institution A	Yes	3	11.1
	No	24	88.9
	Total	27	100.0
Institution B	Yes	15	11.6
	No	114	88.4
	Total	129	100.0
Institution C	Yes	0	0.0
	No	18	100.0
	Total	18	100.0
Total Institutions	Yes	18	**10.3**
	No	156	89.7
	Total	174	100.0

With regard to hacking, the proportion of respondents at Institutions A and B acknowledging that they had used University computing facilities to engage in 'recreational' hacking was similar (between 11.1% and 11.6%), with no statistically significant difference between the two institutions. However, no respondents at Institution C acknowledged such use; it is possible that this can be explained by the fact that respondents at Institutions A and B were taking programmes in Computing, whereas the respondents at Institution C were studying Public Administration and Management. Another factor influencing this difference may also have been gender: whereas 12.3% of males across the study reported engaging in hacking, none of the female respondents claimed to have done so. The question was deliberately phrased using the term 'recreational hacking' in order to include, and encourage honesty among, those students who were engaging in hacking to 'test out' their knowledge and skills, but who had not done so in order to gain financial or other advantage.

Two male respondents, one each at Institutions A and B, had not answered Q.6 at all – all other respondents had either indicated a positive response to one or more of the suggested categories of use, or had declared that they had not made any such

use. Statistics for respondents claiming never to have used University computing facilities for *any* of the activities stated in Q.6[137] are presented in Tables 6.16 and 6.17.

Table 6.16: Students reporting no use of University computing facilities for any of these activities

Institution	Frequency	Percent
Institution A	12	44.4
Institution B	27	20.9
Institution C	11	61.1
Total across Institutions	50	**28.7**

These figures are also represented in Table 6.17, broken down by gender.

Table 6.17: Students reporting no use of University computing facilities for any of these activities, by gender

Gender	Frequency	Percent
Male	24	18.5
Female	24	72.7
N/S	2	18.2

Overall, it would appear that levels of the more serious misuse of University computing facilities did appear to be significantly higher among male respondents, and among respondents in Institution B in particular. It would be inappropriate to attribute a causal factor to this higher reported level of misuse at the Institution, but possible factors could include the networking of residential halls; the higher level of computing skills among the respondent group at this institution; the high

[137] To download or pass on software or music in breach of copyright or licensing restrictions; for recreational hacking; to send hostile email messages; or to access illegal material.

male-female ratio of the respondent group (81.4% of respondents were male); or the effect of institutional approaches to the regulation of network use. Determining whether this level of misuse is replicated among other student groups in the institution, and which factors have had the strongest influence on levels of misuse, could provide an interesting and informative area for further study.

6.3.2 Students' experience of offence as a result of other Internet users

Q.7 asked respondents whether or not they had ever been offended by, or felt uncomfortable as a result of, Web content that they had witnessed **other users** accessing on University computers. The question was carefully worded in order that they should respond according to their *own* experience of feeling offence; they were not asked simply to state whether or not they had witnessed other users accessing offensive content, as it was felt that the subjective nature of the definition of 'offensive' would result in a statistically meaningless response. Worded as it was, it was considered that this question was a reliable means of producing meaningful data in answer to the question of whether students had actually experienced offence or discomfort. The results are presented in Table 6.18.

Table 6.18: Students reporting having ever been offended by, or felt uncomfortable as a result of, Web content that they had witnessed other users accessing on University computers

Institution	Offence?	Frequency	Percent
Institution A	Yes	6	22.2
	No	21	77.8
	Total	27	100.0
Institution B	Yes	31	24.0
	No	94	72.9
	Not Stated	4	3.1
	Total	129	100.0
Institution C	Yes	3	16.7
	No	15	83.3
	Total	18	100.0
Total Institutions	Yes	40	**23.0**
	No	130	74.7
	Not stated	4	2.3
	Total	174	100.0

It can be seen that across the three institutions, almost one in four students (23%) *did* report having experienced some offence or discomfort as a result of Web content that they had witnessed other users accessing on University computing facilities. The proportion of students reporting this offence or discomfort at Institutions A and B was very similar, at 22.2% and 24% respectively, but was somewhat lower at 16.7% in Institution C. This may be a result of the implementation of the filtering software (although all three students at Institution C who had experienced offence or discomfort reported that this was on account of pornographic content, which the filtering software is intended to block).

Although the research questions did not focus on gender differences with regard to computer use, it is nevertheless interesting to note that common assumptions that measures to control access to computer-based pornography are needed primarily in order to protect females from experiencing offence did not appear to be supported by the results of this study. Table 6.19 shows that, of respondents from all three institutions, 24.6% of male respondents reported experiencing offence or

discomfort, in comparison with only 12.1% of female respondents. While the smaller number of female respondents may have led to a statistically unreliable figure, it is also possible that the 'laddish' culture in which the males find themselves means that they feel less able to shy away from content that they find objectionable. This, again, is another area in which a larger scale study could provide insights.

Table 6.19: Respondents reporting having ever been offended by, or felt uncomfortable as a result of, Web content that they had witnessed other users accessing on University computers, by gender

Gender	Offence?	Frequency	Percent
Male	Yes	32	24.6
	No	95	73.1
	Not Stated	3	2.3
	Total	130	100.0
Female	Yes	4	12.1
	No	29	87.9
	Total	33	100.0
N/S	Yes	4	36.4
	No	6	54.5
	Not Stated	1	9.1
	Total	11	100.0

With regard to the nature of the content causing offence, all those who had responded positively to Q.7 were then asked an open-ended question concerning the content that had caused them offence or discomfort. The responses provided were grouped into categories, as shown in Table 6.20. In view of the relatively small number of respondents (n = 40), and the similarity of responses across the institutions to this question, the results are shown collated for all three institutions.

Table 6.20: Nature of content causing offence or discomfort

Nature of content	Frequency	Percent
Pornography / hard core pornography	13	32.5
Violence / dead bodies	7	17.5
Bestiality	6	15.0
Racism / extremism / Nazi sites	2	5.0
Child pornography	1	2.5
Animal abuse / cruelty to animals	1	2.5
Abuse of email	1	2.5
Other	2	5.0
N/S	7	17.5
Total	40	100.0

If the responses for pornography, child pornography, and bestiality are taken together, they represent 50% of all positive responses, suggesting that pornographic content of one sort or another does indeed cause more offence than any other category of content. However, an unanticipated form of content that was cited by seven respondents was that of sites showing dead or mutilated bodies: a couple of these respondents even cited the address of the site that they had encountered[138]. One of the respondents who had declined to answer this question had written 'Too horrible to mention' on his questionnaire.

[138] <http://www.rotten.com>

6.3.3 Students' awareness of University Internet policies

In an open-ended question (Q.2) respondents were asked 'What University policies and/or regulations are you aware of relating to computer use?' The question was posed as an open-ended question in order not to lead respondents. However, whereas it had been anticipated that respondents would name specific policies (e.g. University Acceptable Use Policy), in reality most respondents answered by stating specific actions or forms of content that were prohibited (e.g. no spamming, no pornography). The breadth of these responses led to the creation of a large number of response categories. The results are presented overleaf in Table 6.21.

The table needs some explanation and should be interpreted with caution. Firstly, it should be noted that respondents could name as many different policies as they chose. Secondly, the open-ended nature of the question meant that respondents mentioned those policies or regulations that occurred to them spontaneously: the fact that an individual respondent did not mention a particular policy or regulation does not necessarily mean that on prompting they would not have acknowledged awareness of its existence. It also meant that respondents chose their own way of expressing any particular restriction: thus, whereas one respondent may have used the words 'no offensive use' or 'no illegal use' to refer to their awareness of the AUP, another may have given the name of the actual policy.

A final point concerns the last two categories, that is 'Not aware of any policies' and 'No answer to question'. The first of these categories relates to those respondents who specifically noted that they were not aware of any policies; the second relates to those who had left this question blank. It is possible that some of those who had left the section blank did so precisely because they were not aware of any policies or regulations. However, it was not considered that making this assumption constituted a reliable interpretation of the data, and therefore the use of two separate categories was preferred. It is therefore possible that the number of respondents who were not aware of any policies was higher than the figure for the penultimate category suggests.

Table 6.21: Students' awareness of University policies and/or regulations relating to computer use

	Institution A	Institution B	Institution C	All Institutions
No pornography/ Comp.Porn.Policy	2 (7.4%)	66 (51.2%)	5 (27.8%)	**73 (42%)**
(University) AUP	0 (0%)	39 (30.2%)	0 (0%)	**39 (22.4%)**
Copyright / no file sharing/ no music downloading	1 (3.7%)	27 (20.9%)	3 (16.7%)	**31 (17.8%)**
No hacking	0 (0%)	22 (17.1%)	0 (0%)	**22 (12.6%)**
No spamming	0 (0%)	15 (11.6%)	0 (0%)	**15 (8.6%)**
Netiquette / Email policy	1 (3.7%)	12 (9.3%)	1 (5.6%)	**14 (8.0%)**
No illegal use	3 (11.1%)	9 (7.0%)	2 (11.1%)	**14 (8.0%)**
No offensive use	5 (18.5%)	7 (5.4%)	0 (0%)	**12 (6.9%)**
No personal use	2 (7.4%)	8 (6.2%)	0 (0%)	**10 (5.7%)**
No chat / MSN messaging[139]	4 (14.8%)	0 (0%)	5 (27.8%)	**9 (5.2%)**
Legislation / DPA[140]/ CMA[141]	0 (0%)	5 (3.9%)	3 (16.7%)	**8 (4.6%)**
No games	0 (0%)	5 (3.9%)	2 (11.1%)	**7 (4.0%)**
No server provision / website hosting	0 (0%)	6 (4.7%)	0 (0%)	**6 (3.4%)**
Email / web use is monitored	1 (3.7%)	2 (1.6%)	0 (0%)	**3 (1.7%)**
Websites are filtered / blocked	0 (0%)	1 (0.8%)	2 (11.1%)	**3 (1.7%)**
Janet AUP	0 (0%)	2 (1.6%)	0 (0%)	**2 (1.1%)**
Hall Network Policy	N/A	2 (1.6%)	N/A	**2 (1.1%)**
University Security Policy	0 (0%)	0 (0%)	1 (5.6%)	**1 (0.6%)**
Other policies	4 (14.8%)	8 (6.2%)	4 (22.2%)	**16 (9.2%)**
Not aware of any policies	7 (25.9%)	4 (3.1%)	2 (11.1%)	**13 (7.5%)**
No answer to question	5 (18.5%)	7 (5.4%)	3 (16.7%)	**15 (8.6%)**

[139] MSN Messaging is an instant messaging service that alerts online users when other users in their contacts list are also online and allows for synchronous exchange of messages.

[140] *Data Protection Act 1998* (Parliament, 1998b).

[141] *Computer Misuse Act* (Parliament, 1990).

Despite the identified limitations of the data, the results presented here contribute significantly to an understanding of the general levels of policy awareness among the respondent groups at the three institutions, and are consistent with the findings of the three institutional case studies. At least 25.9% of respondents at Institution A (the University College) were not aware of *any* policies or regulations governing their use of University College computer facilities. Given the lack of attention that had been paid to policy development or dissemination at the Institution, this is perhaps not too surprising. Where respondents did declare an awareness of regulations, these were expressed in very general terms such as no offensive use, no illegal use, no personal use or no pornography. The most specific restriction that was mentioned was 'No chat / MSN messaging', noted by 14.8% of respondents, an awareness that is most probably prompted by the actual blocking of such facilities at the University College.

Respondents at Institution C (the post-1992 University) demonstrated a higher level of policy awareness: only 11.1% specifically claimed not to be aware of any policies or regulations. Awareness was highest with regard to the proscription of pornographic sites and chat or MSN messaging – as access to these sites is blocked, these results are not particularly surprising. Of all the respondent groups, students at Institution C were most likely to mention specific legislative provisions, such as the *Data Protection Act* (Parliament, 1998b) or the *Computer Misuse Act* (Parliament, 1990).

At Institution B, the pre-1992 University, respondents showed a very high level of policy awareness with only 3.1% of respondents at the institution declaring a lack of awareness of any relevant policies. A total of 51.2% of all respondents at this institution spontaneously stated that they should not access pornographic content, or mentioned the *Computer Pornography Policy* by name. In addition, 30.2% of respondents made reference to the University's AUP (whereas *no* respondents at either of the other two institutions made reference by name to the relevant institutional policy). In addition, a fairly high proportion of respondents at Institution B (20.9%) indicated that they were aware of the fact that they should

abide by copyright restrictions, and should not engage in file-sharing activities. Respondents here also made reference to other categories of computer misuse that are proscribed when using University computer services: these included hacking, spamming, website hosting and provision of server services. None of these categories of misuse were mentioned by respondents at either of the other two institutions. These results are entirely consistent with the picture of an institution that devotes considerable time and attention to policy development and dissemination, and which accords a high place on the policy agenda to issues related to computer misuse.

6.3.4 Students' awareness of filtering and monitoring

Respondents were asked whether they were aware of any blocking or filtering of access to websites from University computers (Q.3). Their responses are shown in Table 6.22.

Table 6.22: Students' awareness of blocking or filtering of access to websites from University computers

Institution	Aware of blocking/ filtering?	Frequency	Percent
Institution A	Yes	13	48.1
	No	13	48.1
	Not stated	1	3.7
	Total	27	100.0
Institution B	Yes	77	59.7
	No	52	40.3
	Total	129	100.0
Institution C	Yes	10	55.6
	No	8	44.4
	Total	18	100.0
All Institutions	Yes	100	**57.5**
	No	73	42.0
	Not stated	1	0.6
	Total	174	100.0

Table 6.22 shows how divided the responses to this question were in all three institutions. In Institution A, opinions were shared equally between those who believed that access to websites was filtered or blocked: the positive responses appeared to be related primarily to the blocking of chat and instant messaging sites[142]. Institution B had the highest level of positive responses to this question: in this case, these responses appeared to relate particularly to a recent initiative blocking the use of Napster and other related file-sharing sites[143]. Interestingly, at Institution C, which had implemented institution-wide content-filtering software, respondents did not demonstrate a significantly higher level of awareness of the filtering of websites than at the other institutions, with just over half of respondents answering in the affirmative to this question – and 44.4% unaware of any filtering or blocking of access.

Respondents were also asked whether or not they believed their University monitored email content (Q.4a) and Web use (Q.4b). Responses indicated a high level of uncertainty with regard to whether or not monitoring was taking place, particularly with regard to the possible monitoring of email content, as shown in tables 6.23 and 6.24.

[142] A number of respondents had noted the blocking of these sites in their response to this question.

[143] Again, a number of respondents had noted the blocking of such sites.

Table 6.23: Does the University monitor email content?

Institution	Monitor email?	Frequency	Percent
Institution A	Yes	4	14.8
	No	1	3.7
	Don't know	21	77.8
	Not stated	1	3.7
	Total	27	100.0
Institution B	Yes	84	65.1
	No	14	10.9
	Don't know	31	24.0
	Total	129	100.0
Institution C	Yes	2	11.1
	No	1	5.6
	Don't know	15	83.3
	Total	18	100.0
All Institutions	Yes	90	**51.7**
	No	16	9.2
	Don't know	67	38.5
	Not stated	1	0.6
	Total	174	100.0

Table 6.24: Does the University monitor web use?

Institution	Monitor web use?	Frequency	Percent
Institution A	Yes	8	29.6
	No	0	0.0
	Don't know	18	66.7
	Not stated	1	3.7
	Total	27	100.0
Institution B	Yes	83	64.3
	No	6	4.7
	Don't know	40	31.0
	Total	129	100.0
Institution C	Yes	9	50.0
	No	0	0.0
	Don't know	9	50.0
	Total	18	100.0
All Institutions	Yes	100	**57.5**
	No	6	3.4
	Don't know	67	38.5
	Not stated	1	0.6
	Total	174	100.0

In Institution A, the majority of respondents (77.8%) stated that they did not know whether email content was monitored, only 14.8% were of the opinion that it was monitored and only one respondent was confident that it was *not* monitored. Twice as many respondents (29.6%) at the institution thought that web use was monitored, although the majority (66.7%) were still uncertain about this. No respondents declared that they were confident that web use was *not* monitored.

There was an even higher level of uncertainty with regard to the monitoring of email content at Institution C, with 83.3% of respondents declaring that they did not know whether this was happening, and again only one respondent stating that it was *not* monitored. However, opinion was divided with regard to the monitoring of web use between those who thought that it was monitored, and those who declared that they did not know. Again, no respondents stated that they were confident it was *not* monitored.

Respondents at Institution B were more likely to believe that their email was being monitored, with 65.1% claiming that they thought it was, against 10.9% who thought that it was not monitored and 24% who were not sure. A similar proportion of respondents to those who thought their email was being monitored also thought that their web use was being monitored (64.3%), although in this case there was also a higher level of uncertainty, with 31% declaring that they did not know whether this use was being monitored and only 4.7% confident that it was not.

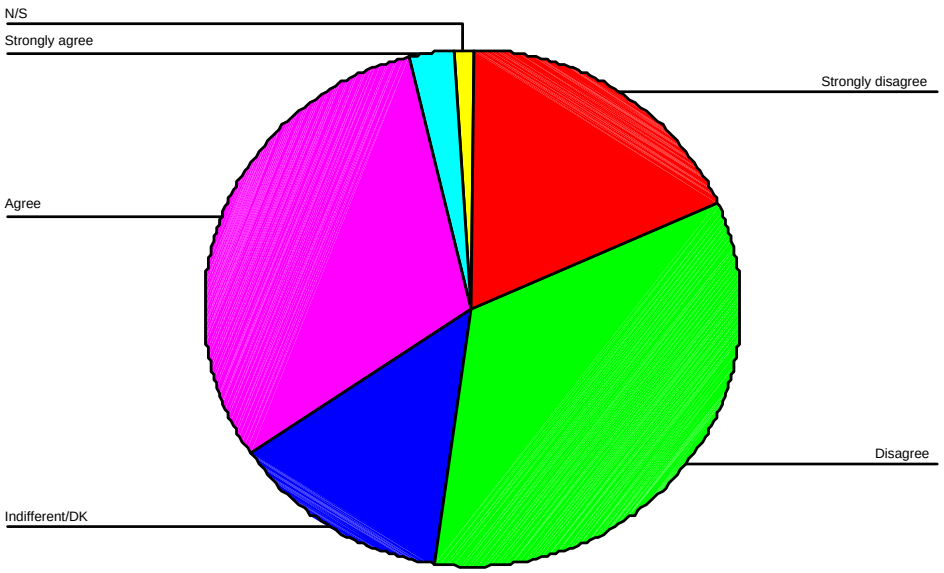
Overall, the picture across the institutions is one of considerable uncertainty – something that institutions may consider to be to their advantage – and may, indeed be encouraging deliberately, as was the case in the library at Institution B (see p.195) – this uncertainty having the potential to contribute to lower levels of misuse.

6.3.5 Students' attitudes to the control of Internet access and use

In Q.8 to Q.17 a Likert scale was used for respondents to rate their attitude towards a range of issues relating to the control of Internet access and use. As the statistical differences in responses between the institutions to the majority of these questions were not significant, and causal explanations for any minor differences could not amount to anything more than guesswork, the results are presented on a cross-case basis. The exception to this is Q.17, which asked respondents about their attitude towards the right of the Government to monitor email or web use in the interests of national defence and security. Although it is still not possible to attribute causal factors to any differences found, it was felt that the scale of the differences in response to this question did provide an insight into some significant differences in thinking among the three respondent groups and warranted illustration. In addition to providing the table of results, the findings are shown as pie charts, as it was considered that this kind of data is easier to interpret and understand when represented in this graphic format. Tables of figures are included to give further clarification of the statistical breakdown.

Graph 6.1

Q.8 The University should monitor Web access

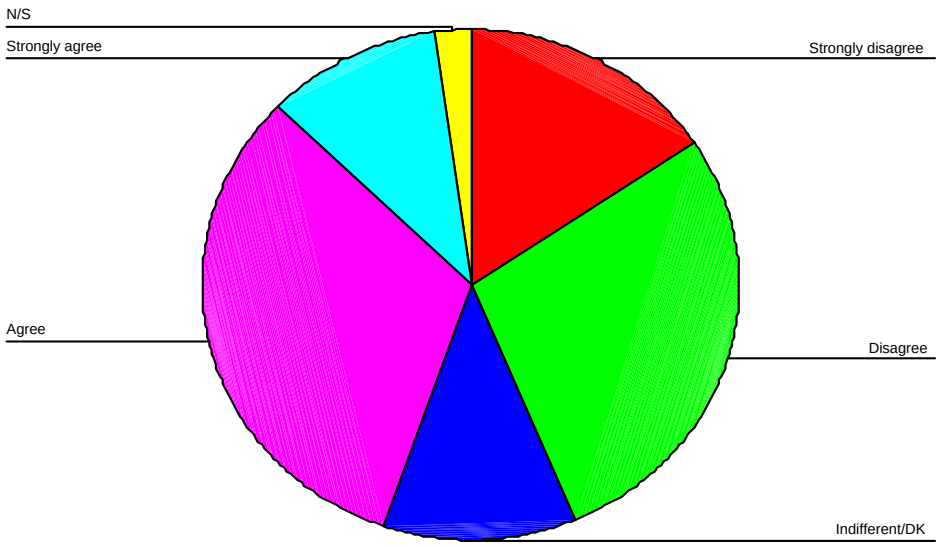


	Frequency	Percent
Strongly disagree	32	18.4
Disagree	59	33.9
Indifferent/Don't know	23	13.2
Agree	53	30.5
Strongly agree	5	2.9
Not stated	2	1.1
Total	174	100.0

It can be seen that a majority of the respondents did *not* agree with the statement that 'The University should monitor Web access', with 52.3% disagreeing or strongly disagreeing with this statement. This compares with 33.4% who agreed or strongly agreed with the statement. A considerable proportion of respondents (18.4%) were in strong disagreement with the proposition. Nevertheless, the figures suggest that one in three students in the respondent groups considered that it *is* appropriate for the University to monitor their Web use. This is a lower rate of acceptance than has been found in studies of public library users (see, for example, Sturges et al, 2003), but this difference could be expected in an academic environment with raised expectations of privacy and academic freedom.

Graph 6.2

Q.9 The University should block access to offensive sites

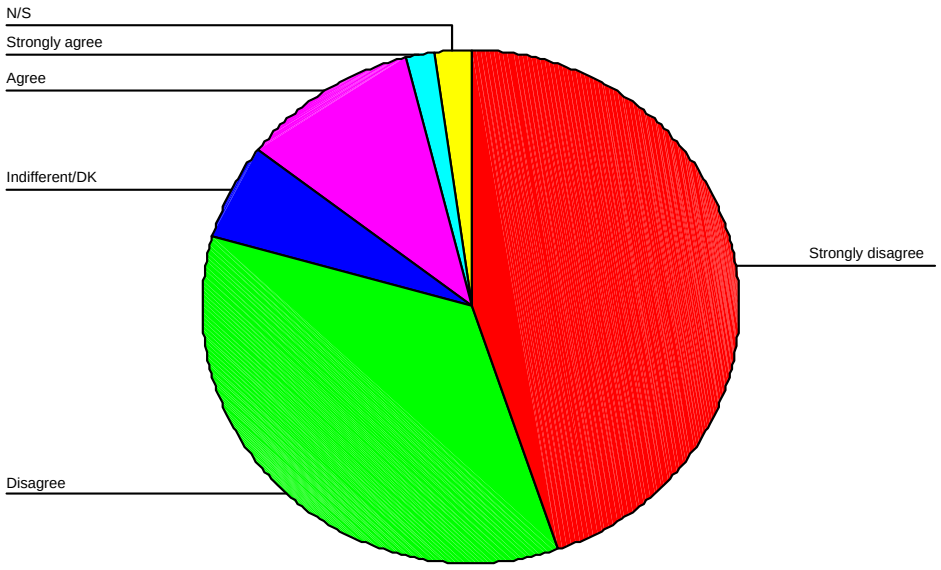


	Frequency	Percent
Strongly disagree	27	15.5
Disagree	49	28.2
Indifferent/Don't know	20	11.5
Agree	56	32.2
Strongly agree	18	10.3
Not stated	4	2.3
Total	174	100.0

When respondents were asked their opinion on whether the University should block access to offensive websites, opinions were almost evenly divided between those who agreed or agreed strongly that it should (42.5%) and those who disagreed or disagreed strongly that it should do so (43.7%). Of all respondents, 10.3% agreed strongly with the statement that 'The University should block access to offensive sites'. It cannot therefore be assumed that students will invariably resent attempts to restrict their access to Internet content: these figures would suggest that a substantial proportion may consider that it is in their own interest, or is at least entirely reasonable, for the University to impose such restrictions.

Graph 6.3

Q.10 The University should monitor email content

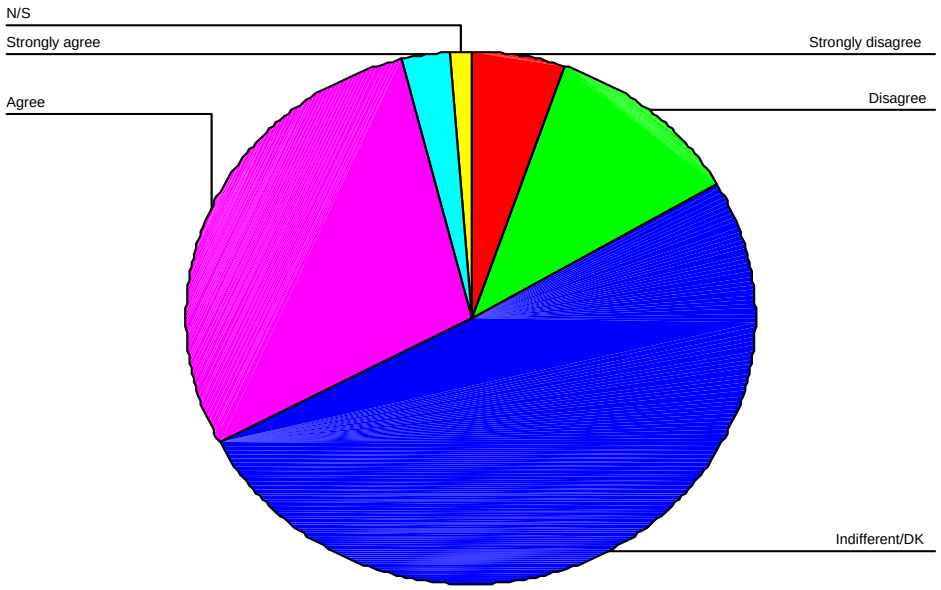


	Frequency	Percent
Strongly disagree	78	44.8
Disagree	60	34.5
Indifferent/Don't know	11	6.3
Agree	18	10.3
Strongly agree	3	1.7
Not stated	4	2.3
Total	174	100.0

However, when respondents were asked to respond to the statement that 'The University should monitor email content' the majority were strongly against accepting the statement. Altogether 79.3% of respondents disagreed or disagreed strongly with the statement, compared with only 12% who supported it. Of those who disagreed a substantial proportion felt strongly about the issue, with 44.8% of all respondents disagreeing strongly. Respondents were also less likely to 'sit on the fence' in response to this statement, with only 6.3% claiming to be indifferent or not to know what they thought. A number of students had added written comments to the effect that email correspondence deserves the same level of privacy protection as would be afforded paper-based correspondence.

Graph 6.4

Q.11 There are sufficient controls in place in the University to protect my privacy online



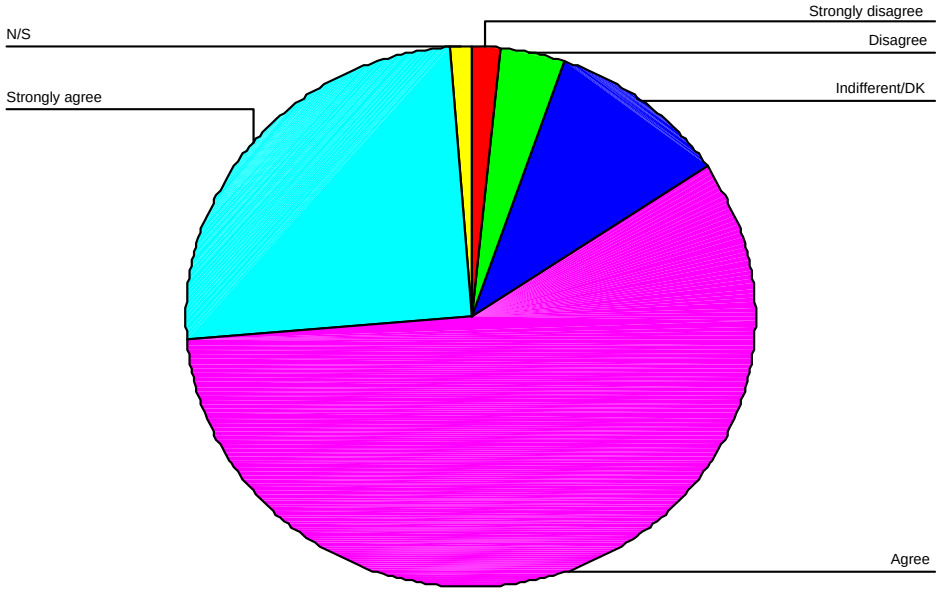
	Frequency	Percent
Strongly disagree	9	5.2
Disagree	20	11.5
Indifferent/Don't know	88	50.6
Agree	50	28.7
Strongly agree	5	2.9
Not stated	2	1.1
Total	174	100.0

With regard to their confidence in the level of privacy protection afforded by the University to their online transactions, respondents evidenced a high level of uncertainty. Half of all respondents (50.6%) stated that they were indifferent, or did not know, to the statement 'There are sufficient controls in place in the University to protect my privacy online'. It would seem highly unlikely that such a high proportion of students would really be indifferent to their own privacy protection (especially in the light of their responses to Q.10), so this would suggest that they are not sure of the effectiveness of measures to protect their privacy

online[144]. Of the remaining respondents, quite a high proportion (31.6% of all respondents) believed that their privacy online *is* protected at the University. Only 16.7% of respondents disagreed, or strongly disagreed, with the statement.

Graph 6.5

Q.12 Whatever measures the University takes to control online access, some students will always be able to get round them



	Frequency	Percent
Strongly disagree	3	1.7
Disagree	6	3.4
Indifferent/Don't know	18	10.3
Agree	101	58.0
Strongly agree	44	25.3
Not stated	2	1.1
Total	174	100.0

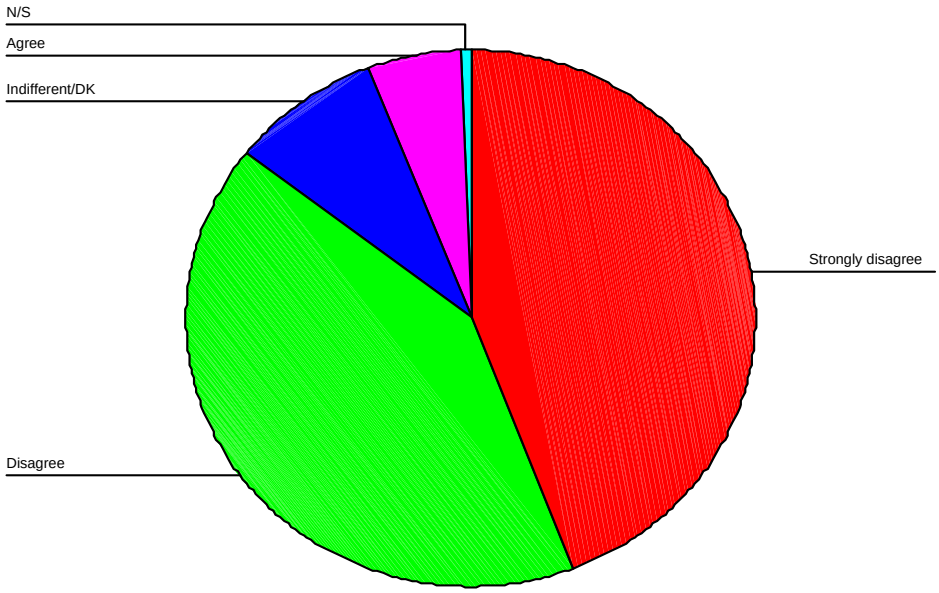
Whatever uncertainty respondents might have felt about the effectiveness of online privacy protection within their Universities, they were very sure that University measures to control online access would always be vulnerable to students' abilities to bypass them. When asked to rate their agreement or disagreement with the

[144] In future work, the researcher would not use the same category for 'Indifferent' and 'Don't know' as the implications of each of these responses may be quite different.

statement ‘Whatever measures the University takes to control online access, some students will always be able to get round them’ 83.3% of all respondents agreed, or strongly agreed, with the statement. Only 5.1% actively disagreed with the statement. Although this does not, of course, necessarily reflect the *actual* ability of students to bypass such controls, it certainly does suggest a culture that anticipates being able to circumvent measures of control.

Graph 6.6

Q.13 It is none of my business what measures the University takes to control/monitor my Internet use



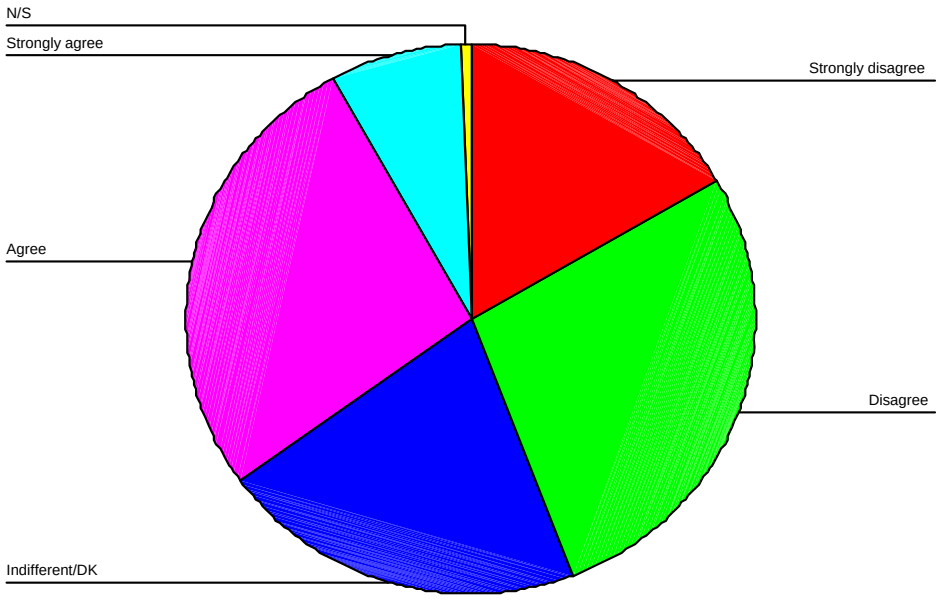
	Frequency	Percent
Strongly disagree	77	44.3
Disagree	72	41.4
Indifferent/Don’t know	15	8.6
Agree	9	5.2
Agree strongly	0	0.0
Not stated	1	.6
Total	174	100.0

There was an even higher uniformity of response to the statement that ‘It is none of my business what measures the University takes to control or monitor my

Internet use'. Whether they supported monitoring of use or not, 85.7% disagreed, or strongly disagreed, with this statement, indicating that they did consider it to be their business what measures the University took. Only 5.2% of respondents agreed with the statement and none of them agreed strongly with it.

Graph 6.7

Q.14 If I were in charge of University computing facilities I would expect to have the right to block access to offensive (but legal) content



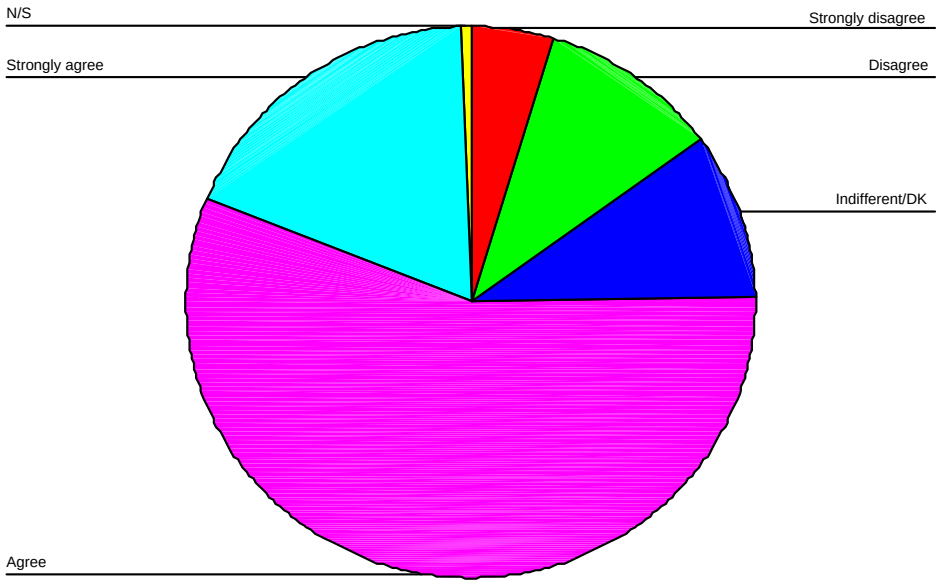
	Frequency	Percent
Strongly disagree	29	16.7
Disagree	48	27.6
Indifferent/Don't know	36	20.7
Agree	47	27.0
Strongly agree	13	7.5
Not stated	1	.6
Total	174	100.0

When the tables were turned and students were asked about their expectations if they were in charge of University computing facilities, 34% agreed, or strongly agreed, that they would expect to have the right to block access to offensive – but legal – web content. However, a considerable proportion of respondents (20.7%)

were not sure (or possibly were indifferent) about what they thought about this, and the greatest proportion (44.3%) of students disagreed, or disagreed strongly, with this statement.

Graph 6.8

Q.15 If I were in charge of University computing facilities I would expect to have the right to block access to illegal content



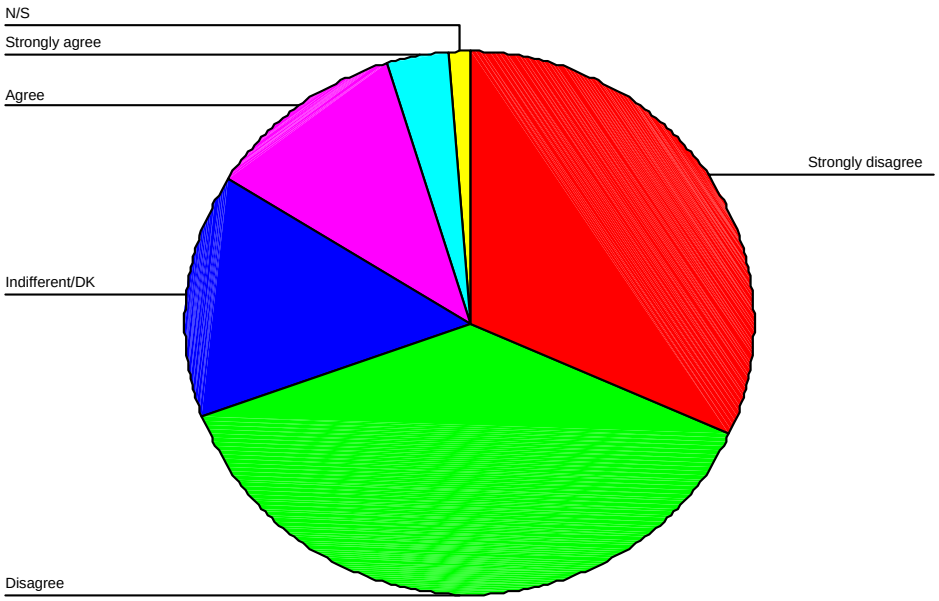
	Frequency	Percent
Strongly disagree	8	4.6
Disagree	18	10.3
Indifferent/Don't know	17	9.8
Agree	98	56.3
Strongly agree	32	18.4
Not stated	1	.6
Total	174	100.0

If respondents were uncertain about whether they would expect to have the right to block offensive – but legal – content, there was much less uncertainty when it came to illegal content. In this case, 74.7% of respondents agreed, or strongly agreed with the statement 'If I were in charge of University computing facilities I would expect to have the right to block access to illegal content'. Only 9.8% did

not know or were indifferent, and a total of 14.9% disagreed, or disagreed strongly, with the statement.

Graph 6.9

Q.16 If I were in charge of University computing facilities I would expect to have the right to monitor email content



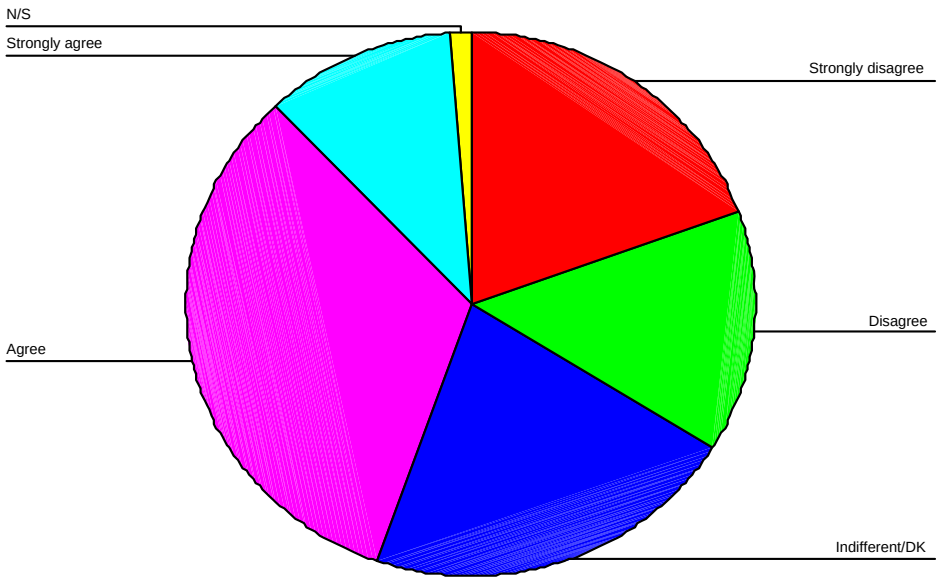
	Frequency	Percent
Strongly disagree	55	31.6
Disagree	66	37.9
Indifferent/Don't know	25	14.4
Agree	20	11.5
Strongly agree	6	3.4
Not stated	2	1.1
Total	174	100.0

The reluctance to accept University monitoring of email content that respondents had expressed in Q.10 remained largely unchanged in the hypothetical scenario of their being responsible for University computing facilities. 69.5% of respondents disagreed, or disagreed strongly, with the statement 'If I were in charge of University computing facilities I would expect to have the right to monitor email content'. Only 14.9% agreed, or agreed strongly, with this statement. It is clear

that the majority of respondents attached considerable importance to the privacy of their email correspondence, and did not accept a right on the part of the University to monitor this correspondence.

Graph 6.10

Q.17 The Government should have the right to monitor email / Web use in the interests of national defence and security



	Institution A	Institution B	Institution C	All Institutions
Strongly disagree	4 (14.8%)	25 (19.4%)	5 (27.8%)	34 (19.5%)
Disagree	10 (37.0%)	11 (8.5%)	4 (22.2%)	25 (14.4%)
Indifferent/ Don't know	8 (29.6%)	26 (20.2%)	3 (16.7%)	37 (21.3%)
Agree	3 (11.1%)	49 (38.0%)	5 (27.8%)	57 (32.8%)
Strongly agree	2 (7.4%)	16 (12.4%)	1 (5.6%)	19 (10.9%)
Not stated	0 (0.0%)	2 (1.6%)	0 (0.0%)	2 (1.1%)

It should be noted that the fieldwork for this survey was carried out in the period from December 2001 to February 2002, only months after the terrorist attack in September 2001 on the World Trade Centre and the Pentagon in the United States.

It also followed the implementation of legislation in the UK regulating the surveillance of electronic communications (RIPA[145]), the hurried enactment in December 2001 of the Anti-Terrorism, Crime and Security Act[146] and attempts by the Home Office to impose greater retention and surveillance measures on communications data (see Chapter Three, pp.96-103). The issue of government surveillance and interception of electronic communications was therefore receiving considerable media attention during this period.

It can be seen from Graph 6.10 that a significant proportion of these students did agree, or agreed strongly, with the statement that 'The Government should have the right to monitor email or Web use in the interests of national defence and security'. Altogether 43.7% declared support for this statement, against 33.9% who disagreed or disagreed strongly. However, there was also a considerable proportion (21.3%) that was undecided (or indifferent), and opinions did vary between the respondent groups. Thus, for example, students in Institution B were more likely to agree or agree strongly with the statement (50.4%) than those at the other two institutions. Those at Institution A were *least* likely to agree or strongly agree (18.5%). Gender differences in response to this question were analysed but not found to be statistically significant.

6.3.6 Other student comments

Respondents were also given an opportunity to answer an open-ended question (Q.18) inviting them to make other comments about Internet use and access. Although most students did not take up this opportunity, the comments that were made tended to follow similar themes and can be categorised as follows:

[145] The Regulation of Investigatory Powers Act 2000. Available at <http://www.hmso.gov.uk/acts/acts2000/20000023.htm> [Last accessed 5/7/2004].

[146] <http://www.hmso.gov.uk/acts/acts2001/20010024.htm> [Last accessed 5/7/2004].

- Students commented on the subjective nature of offensiveness and the difficulty of defining what is offensive;
- A couple of respondents commented on the benefit to society of allowing freedom of thought and expression, and one noted that "It is for the greater good that the Internet be kept largely ungoverned and access should be full";
- Email should be afforded a high level of privacy / the same level of privacy as other forms of correspondence – comments of this nature were made by a number of respondents;
- At Institution B, where students pay for network access in residential halls, a number of respondents commented on the cost of access, and complained about recent increases in this cost;
- At the same Institution they commented that, if they are paying for access, there should not be any restrictions – one student felt this should also apply if they are using their own computer ("If your own PC is logging onto the University network, it is your own business");
- One respondent suggested that it was unrealistic to expect students to use the Internet only for specified purposes, as 'people will always break the rules'.

6.4 Conclusion

Although the limitations in size of the sample groups do not allow for the extrapolation of generalisable truths about UK students' use and misuse of University computing facilities, this questionnaire study has contributed to the information and insights obtained in the institutional case studies. It is clear that these students did make extensive use of University computer networks, and that this use was not generally confined to academic purposes. Nor was it always restricted to legal purposes or those that respected the terms of use imposed by the individual Universities. In particular, the results suggested that file-sharing activities, especially music piracy, was taking place on a large scale, leading to the potential for legal action to be taken against individuals or institutions.

The considerable efforts made at Institution B to develop and disseminate policy on Internet access and use appeared to have been successful in achieving a high level of policy awareness among these students. However, it should be noted that this awareness did not appear to have impacted on levels of misuse of facilities: in fact, of the three respondent groups, students at this institution appeared to engage in higher levels of misuse than at the other institutions. While this group may not have been representative of the institution as a whole, it can be deduced from these results that simple awareness of conditions of use and Acceptable Use Policies does *not* guarantee that students will respect these conditions. At best, such policies provide the institution with a defence in the event of a legal challenge, whilst exerting a less damaging impact on academic freedom than measures such as the imposition of filtering software.

With regard to students' attitudes to filtering and monitoring, it was interesting to note the consistency with which all three groups of students differentiated between the monitoring of Web use and that of email use. Although there was a fairly high level of tolerance of monitoring of Web use, and even of blocking of access to some Web content, it was clear that students expected to be afforded a high level of privacy in their email communications. Even in the hypothetical situation of their being in charge of University computing facilities, they still generally did not expect to monitor email content. There was a rather higher level of acceptance of the right of the Government to monitor email communication in the interests of national defence and security, but this might have been influenced by the emphasis on measures to combat terrorism imposed in the wake of the September 11 attacks in the US.

The findings from the questionnaire study led to the identification of further research that could be carried out to extend and explore the work – this will be discussed in Chapter Eight of the thesis. Prior to that, the appropriateness and any limitations that were identified in the methodology of this part of the work will be discussed in the next Chapter, as will the overall implications of the findings of the policy monitoring, case studies and questionnaire study.

CHAPTER SEVEN: DISCUSSION

7.1 Introduction

This Chapter discusses the findings from the different components of the study, and their implications when considered as a whole in the context of the original research question. Following an initial restatement of the research question, the findings are discussed and subsequently considered with reference to the policy process models introduced in Chapter One. In the course of the discussion, the contribution made to the theoretical and practical knowledge of the subject area is identified and the appropriateness of the methods adopted is considered. Where deficiencies in the research design have been identified, these will also be discussed. Consideration of the final conclusions from the study is reserved for the final chapter, Chapter Eight, as are suggestions for further areas of related research.

7.2 Reconsidering the problem

It has been recognised that policy formulation with regard to the Internet is a bi-directional process, with regulation of the Internet being both affected by, and affecting, the context in which policy is implemented. Appropriate policy measures to promote access to the Internet can bring about a more democratic and 'open' space, just as restrictive approaches can constrain the choices available to citizens and limit their freedom of speech and access to information on the Internet. The overall aim of this study was to explore a range of such policy measures intended to regulate access to Internet content, including those implemented at both the macro and the micro level, and to consider the potential impact they may exert on freedom of expression and freedom of access to information. The erosion of the 'public sphere' as a forum for rational debate and decision-making identified by Habermas (1962; 1989), and a concern for the conditions that afford the promotion of 'ideal speech' were used to provide a theoretical rationale for the study of such an impact. The use of a typology of

policy process models was adopted in order to explore and illuminate the factors and forces that are shaping policy formulation in this area. A new policy process model was developed to further advance the theoretical and methodological tools available for the analysis of a range of areas of information policy.

7.3 Discussion of policy approaches at macro and micro level

Despite the inherently democratic architecture of the Internet and its resistance to conventional forms of governance, the findings of the policy monitoring and analysis at both macro and micro levels confirmed the viewpoint of those who have suggested that the Internet is, in fact, a closely regulated sphere, subject to a multi-tiered governance structure (as, for example, previously posited by Wall, 1997; Wall, 1998; Akdeniz, 1997a; Walker, Wall and Akdeniz, 2000; Valauskas, 1996). A wide range of relevant measures were identified in the course of the policy monitoring and the case study research; moreover the breadth of scope and application of such measures appeared to be extending, a phenomenon that can be described as 'policy creep'. Despite rhetoric to the contrary, the findings suggested that in, their impact on information access, the restrictive perspective dominated over the distributive perspective in measures taken at both macro and micro levels.

Over the period during which the study took place, the monitoring of EU and Council of Europe policy indicated that the issue of Internet content control occupied a high position on the European policy agenda. This was particularly true with regard to the regulation of sexual content, and its access by minors[147]; however, there was also evidence of measures intended to extend the sphere of European regulation into the control of racist and extremist political content and the oversight of personal communications over the Internet (particularly in the wake of the events of 11th September 2001).

[147] As Heins (2001) has noted, the European Parliament definition of "harmful content" relates directly to the protection of the morals of minors.

At the same time, EU and UK measures to control content were accompanied by those aiming to promote the growth of e-commerce. This combination of content control and promotion of the Internet as a virtual marketplace, with the accompanying 'skewing' of discourse to favour an advertising and sales environment, provides a good example of the distortion of the 'ideal speech' situation. This distortion contrasts sharply with the vision portrayed by the European Commission Legal Advisory Board (1997) in its response to the *Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services* (European Commission 1996c), cited on page 71 of the thesis, which championed 'the potential empowerment of users through increased transparency of government and availability of public sector information'.

In a similar vein, the Council of Europe claims to be an organisation that has the protection and furtherance of human rights and fundamental freedoms at the very heart of its mission. Articles Eight and Ten of the ECHR afford protection of the privacy of the individual and of the right to freedom of expression to citizens of member states. Moreover, European Court of Human Rights' rulings have highlighted the particularly high protection afforded to information and ideas expressed in the context of political debate, on the grounds that public debate 'is at the very core of the concept of a democratic society'[148], and the fact that this applies equally to 'ideas that offend, shock or disturb'[149]. Again, this is strongly supportive of the notion of the undistorted Habermasian public sphere.

It was indeed evident from the case study analysing the development of the *Guidelines on Public Access to and Freedom of Expression in Networked Information* that concerns for the preservation of freedom of expression did exert an influence throughout this particular policy formulation process, as did a genuine

[148] Lingens v. Austria, judgement of 8 July 1986, Series A, No.103, 8 EHHR 103 (1986), para.42, cited in Gomiens (1996).

[149] Handyside v. United Kingdom, judgement of 7 December 1976, Series A, No. 24, 1 EHHR 737 (1979-1980), para.49.

commitment to the promotion of the positive benefits and democratising potential of the Internet. The commitment to freedom of expression was most apparent in the initial draft of the document, especially in the declaration that *no* end users of public access points should be prevented from accessing any legal content they choose on account of official or popular pressure to remove illegal, distasteful or harmful content. However, although a commitment to freedom of expression was still apparent in the final document, in particular through the emphasis on end user control, it has to be noted that the original statement was considerably diluted by the time that the final draft was agreed, and that the vision of full and unrestricted public access to the Internet for all citizens, irrespective of age, no longer prevailed as a policy goal. The difficulties inherent in reconciling a wide range of conflicting viewpoints and policy priorities on the part of the different actors involved ultimately inhibited the achievement of the original policy goals.

Policy approaches at European level with regard to the regulation of Internet content were found to be closely mirrored by those adopted at national level in the UK. Although measures had been taken in the UK to promote increased public access to the Internet in the interests of economic competitiveness and social inclusion, intensive media reporting of child pornography on the Internet, and of use of the Internet to commit criminal actions, had encouraged an increasingly restrictive and regulatory approach on the part of the government and a range of law enforcement agencies. The claim made by Hill (1994, p.8) that in the UK 'Freedom of speech is a long-established and cherished freedom…and must be deemed to lie at the heart of our national information policy' does not sit easily alongside the statement by the then Home Secretary, Jack Straw, in 2000 that 'the Internet cannot exist in an anarchistic free speech environment' (cited on p.90 of the thesis). Such a statement indicates that priorities seen as contributing towards the preservation of law and order were being afforded a higher place on the policy agenda than was accorded to 'soft' concerns such as freedom of expression.

These divergent viewpoints are more than an issue of rhetoric or semantics: they are of crucial importance. As Rowlands (1997) has pointed out, the manner in

which a problem is framed and defined by policy makers is crucial to the policy response that will be used to address it:

> *If we see people sleeping on the streets as a problem of vagrancy, then the policy response may be framed in terms of law enforcement and policing. We might also view the same issue as an indicator of social deprivation or a sign of failure in other policy areas such as community care; in which case, the policy response will obviously be very different (we might provide low cost housing, for example, or appropriate mental health care).*
>
> (Ibid p.86)

Thus, if the 'problem' of the Internet is perceived and defined as one of providing equality of access to the new informational environment, the response will be very different to a situation where the problem is seen as being one of the potential harm of 'unacceptable' content. In the former case, the distributive perspective is likely to prevail; in the latter, the restrictive.

As with the EU and the Council of Europe, the policy measure of choice to address this 'problem' at UK national level was that of voluntary self-regulation and the development of technical measures such as rating systems, albeit with an undercurrent of the threat of more repressive measures should this approach fail. However, from an initial emphasis on the control of child pornography, the sphere of regulation here had also extended to encompass defamatory content, copyright infringement and racist content. Much attention had also been paid, both at European and at UK level, to provisions to facilitate the surveillance and interception of electronic communications, ostensibly in response to the events of September 2001, although evidence indicated that these measures were already being planned in advance of these events. Moreover, such measures had been implemented with an apparent disregard for the normal judicial safeguards that have historically accompanied such measures in the offline environment.

The case studies at the institutional level indicated that the issue of the regulation of Internet access, use and content was also high on the agenda of the three academic institutions that were studied, albeit in one case (Institution A) concerns

were addressed through the means of informal and ad-hoc measures. This attention was driven by a multiplicity of forces, such as anxieties about potential legal action; institutional reputation; the provisions of the *Janet AUP*; bandwidth and network traffic costs; controlling the use of employee work time; the avoidance of employee and student harassment; and a general concern with the maintenance of a 'decent', moral environment. However, although a token recognition of the importance of academic freedom was made in all three institutions, in only one (Institution B) did this concern appear to have been accorded a significant importance in the policy formulation process towards Internet regulation.

As a basis for further discussion of the findings of the case studies, a Venn diagram can be used to illustrate those aspects of the findings related to policy formulation and implementation that were similar, and those that differed, in the different institutions (figure 7.1 overleaf).

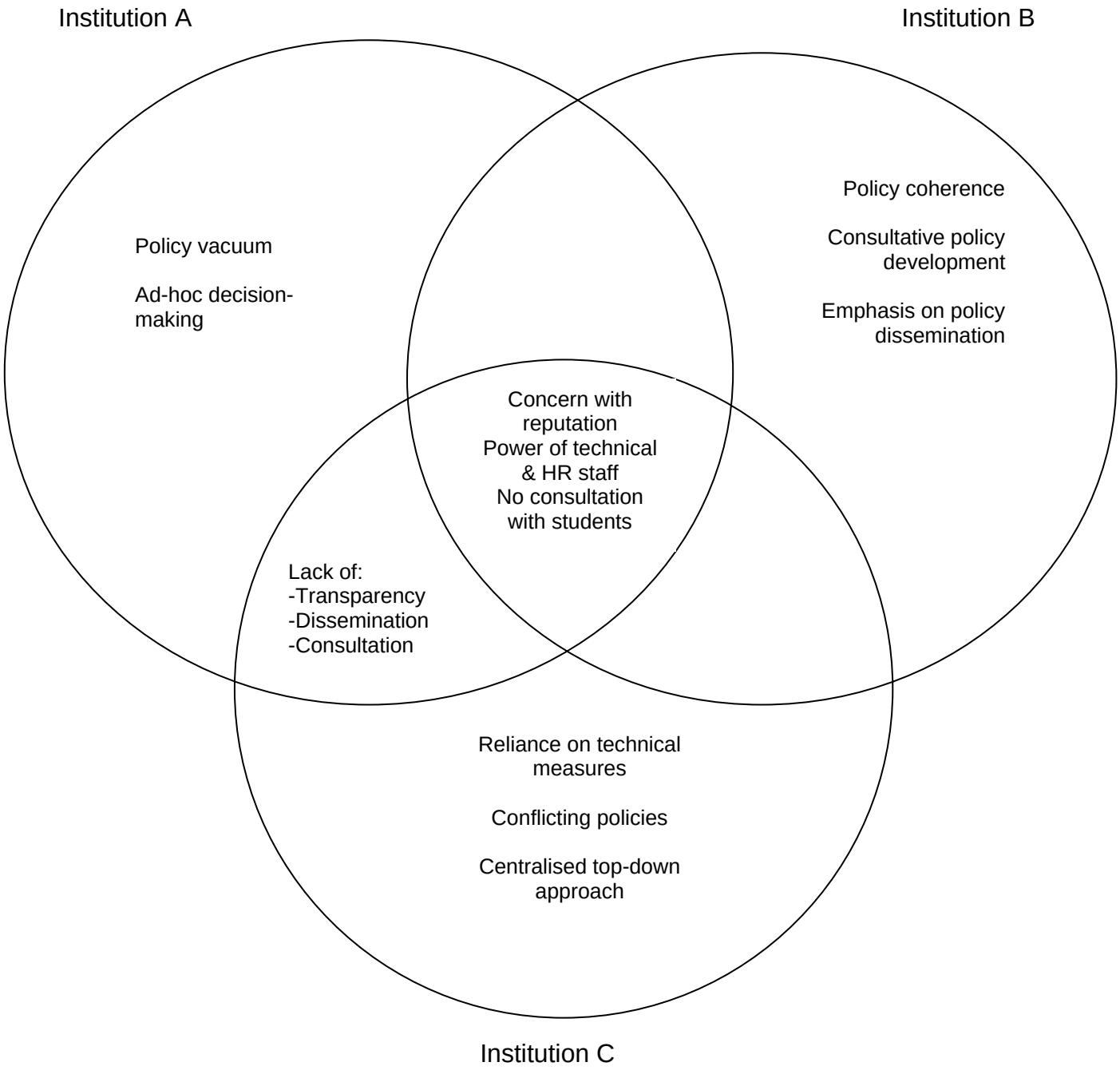


Fig.7.1: Features of the policy process at the case study sites

It can be seen from Fig. 7.1 that one of the features of policy-making that was common to all three institutions was a concern with the institution's reputation, which acted as a powerful policy driver at all three sites. The fact that UK Higher Education Institutions are subject to the provisions of conflicting and as yet often untested legal provisions at national level, that all have implications for the regulation of Internet use (such as the *Data Protection Act 1998*; the *Regulation of Investigatory Powers Act 2000*; and the *Human Rights Act 1998*), had contributed to an atmosphere of uncertainty and potentially over-cautious regulatory approaches. In particular, the case studies illustrated the potential for legislation to result in unintended outcomes that conflict with the original aims of the measure: as, for example, the citing at Institution C of the *Human Rights Act 1998* (Parliament, 1998a) as a justification to prohibit personal use of University email systems on the grounds that continuing to allow this use would remove the right of the Institution to monitor email use.

It was also notable that none of the institutions had involved students in their policy formulation, although one had latterly recognised the need to address this in future policy development. This failure to involve students in the policy process may well have contributed to the lack of policy compliance on their part that was revealed in the course of the questionnaire research. A significant feature in all three institutions was the very strong role that technical staff were able to play both in the policy development and implementation stages: their command of the technical aspects of the 'problem', and of any potential solutions, gave them considerable power in determining which approaches were favoured, and in the subsequent 'policing' of policy adherence. The ultimate result appeared to be a considerable shift in the power balance that operated between academic and technical support staff. This aligns with Habermas' view of the potentially distorting effect on rational debate incurred as a result of the words of 'experts' or 'technocrats' who are able to manipulate discourse through their superior command of technical knowledge (Outhwaite, 1994, p.9).

The satisfaction derived from being able to adopt the role of 'policeman' and 'gatekeeper' on the part of technical staff[150] that was evidenced by some participants in the institutional case studies, has potentially worrying implications for the future defence of academic freedom in an electronic environment. In particular, the implementation of filtering software at Institution C was shown to have exerted a major impact on the power balance operating between academic and technical staff. Whereas at one time University librarians were all too often seen as the 'gatekeepers' to knowledge, with the power to impose access restrictions on books and journals, this perceived role appeared to be shifting in the direction of technical personnel. This is a matter of concern with regard to the potential impact on academic freedom: although the power held by librarians was no doubt on occasion subject to abuse, it was at least held in the hands of a profession openly committed to freedom of expression and freedom of access to information (as described in Chapter One of this thesis), and professionally accountable to this ethic. It seems clear from the case study findings that the overriding concern for technical staff was the integrity and security of the systems for which they have responsibility, and issues such as the preservation of academic freedom were accorded lesser importance by them.

Furthermore, the findings of the case studies indicated that moves to engage in increasing amounts of electronic surveillance were perceived by academic staff as undermining the trust-based model of academic autonomy on which universities have operated in the past. The increase in the potential to undertake electronic surveillance was identified by academic personnel as representing an undesirable encroachment of a culture of managerialism. Uncertainty of the extent of employer monitoring was found to be exerting a panoptic effect (Foucault, 1977) that led academics to 'self-censor' their communication and information-seeking activities. Such an internalisation of discipline within the individual ('governmentality': Dean, 1999) in the electronic environment has been discussed

[150] As illustrated, for example, by the comment made by the Network Team Leader at Institution C, that 'just because we're allowing you access doesn't mean we're not keeping an eye on you' (cited on p.216)

by Mehta and Darier (1998) who describe the pressure that Internet users experience

> *…to conform to the normalizing influences inherent in this deployment of electronic power. Although considerable resistance is evident, the fear of reprisals from "legitimate" authority and self-appointed Internet "police" shape the behavior of many.*
>
> (Ibid, p.110)

However, the findings with regard to student use of university computer network facilities also provided evidence of other changes to the definition of norms, values and morality in the electronic environment. In the questionnaire study conducted as part of this project, 67.8% of all student respondents (including 77.5% of those at Institution B) reported engaging in software or music piracy. Such results appear to be supported by the findings of Oppenheim and Robinson (2003), who cite a figure of 66% of students surveyed acknowledging participation in music file-sharing activities. It is very unlikely that the same percentage would have been prepared to steal CDs or software packages from offline shopping outlets.

There is potential here for further research into the change in attitude engendered by the electronic environment, in particular whether this altered ethical response to the issue of theft is a result of a perception of a decreased likelihood of being caught when stealing online; the fact that the theft does not involved tangible property in the form of a manufactured 'artefact'; a belief that it is in the interests of the artists concerned to have the widest possible audience for their music; a retaliation against a perceived exploitation of consumers on the part of record companies or software houses; the ease with which theft can be carried out in the electronic environment; or, a combination of some or all of these[151].

The importance of the impact of organisational culture on policy decisions was very apparent in the findings of the case studies. The top-down confidence-lacking organisational cultures of Institutions A and C had led to a reliance on a cautious regulatory approach, whereas Institution B, with its stronger market

[151] Further discussion on these issues can be found in Oppenheim and Robinson (2003).

position and more established, mature, and consultative academic culture, was more confident in adopting a self-regulatory approach underpinned by carefully developed ethical policies. However, it should also be noted that ultimately none of the institutions had succeeded in preventing misuse of their computer facilities as evidenced by the student questionnaire findings. Indeed, the evidence from the questionnaire study indicated that it was in Institution B that the *highest* levels of misuse, including for illegal purposes, was taking place. This was in spite of the fact that this was the Institution in which awareness of policies on computer misuse was also at the highest level.

The results of the questionnaire study further suggest that it is wholly unrealistic – and probably counter-productive – for universities to adopt policies that disallow *all* personal use of university network facilities. With a mean of 98.9% of students across the three institutions engaging in some form of personal use, policies stating that no such use is allowed will inevitably be seen as lacking in credibility. Rather, the results indicate that efforts to constrain non-academic use should be concentrated on those areas that represent the greatest potential legal liability for the institution. This is particularly evident with regard to the widespread file-sharing activity that was seen to be taking place.

7.4 The use of policy models to explore the findings

7.4.1 Lessig's models of direct and indirect regulation

The various forces that can bring about a regulatory impact on information flow have been illustrated by Lessig (1999) in his models of direct and indirect regulation, as shown on p.34 and p.35 of the thesis. These forces comprise those of legislation, the market, social norms and architecture. Of these modalities of constraint, Lessig (Ibid) argued that it is the modification of architecture (through code) that has the most crucial role to play in exerting democratic regulation of the Internet without prejudicing freedom of expression. Other critics have disagreed with this perspective. For example, Hosein et al (2003) maintain that, whereas

code can be an effective regulatory mechanism, it also represents the interests of its developers and therefore is socially shaped. More seriously, Internet regulation through architectural modification, such as age verification schemes or filtering software, has been open to charges of being subject to inaccuracy, lack of objectivity and ambiguous standards, while the 'invisibility' of solutions such as filters and their potential use for censorship renders them antithetical to free speech values (Harvard Law Review, 1999).

This viewpoint is supported by the findings of the investigation into institutional measures to regulate Internet use: while the implementation of filtering software in Institution C did appear to have been more successful than ethical approaches in reducing levels of computer misuse, the interviews with academic staff in particular indicated that the negative impact of this measure on academic enquiry at the University had been significant. The lack of transparency that accompanied this implementation, with a low level of awareness demonstrated by either staff or students of the fact that their Internet access was being filtered and a lack of information being made available about the basis for filtering decisions, also exerted a detrimental impact on academic freedom in the institution. Academic staff were powerless to challenge regulatory decisions on account of this lack of transparency, and also in some cases because they lacked the technical language that could have enabled them to engage in the debate about these decisions.

With regard to the specific issue of the regulation of Internet content and access at the macro level, the combination of legal initiatives intended to bring about the adoption of an increased range of self-regulatory measures, the fostering of conditions favourable to the development of e-commerce, and the promotion of technical measures and educational initiatives designed to control Internet content and use espoused by the various bodies of the EU, the Council of Europe and the UK government, can more usefully be interpreted through the modified model of 'indirect' regulation proposed by Lessig (1999, p.93; illustrated on 35 of the thesis). However, such indirect regulation had also led to a lack of transparency and accountability. Such a lack of accountability in the approach towards Internet

regulation of the EU was commented on in the *Library Association Record* (1998d):

> *Because the approach to Internet regulation has been legislation-driven in the United States, and of course because the US has a constitution, the debate can at least happen in an ordered and accountable manner. The danger with the European approach, according to civil liberties groups, is that it tends to be more covert.*

Certainly, this study has shown that the EU, the Council of Europe and the UK authorities have tended to favour a pragmatic approach based on an encouragement of self-regulatory approaches. However, this approach has also been shown to have led to a lack of clarity in the legal position exerting a 'chilling effect' on ISPs, who are deterred from hosting controversial material, or material that could attract legal action (as is illustrated, for example, by the case of www.thinkofthechildren.co.uk described on page 92, or that of Godfrey v Demon, described on p.91).

Collins and Murroni (1996, p.172) have also criticised a reliance on self-regulation through bodies such as the Internet Watch Foundation, on the grounds that 'Self-regulatory bodies are accountable not to citizens or consumers – even through the imperfect channel of Parliament – but only to the industry which has established them.' This leads ultimately to the risk of a situation where only 'acceptable' voices are heard: and because of the lack of transparency and judicial process to review decisions to withhold access to content, citizens are not even aware of the restrictions imposed. At the micro level the findings of the questionnaire study demonstrated clearly that even well-disseminated and communicated self-regulatory measures are ineffective unless they have full 'stakeholder' acceptance and support through their participation in the formulation process.

The development of the Council of Europe guidelines was a good example of a genuine attempt to devote attention to the policy consultation process, and had the potential of being an illustration of genuinely democratic policy formulation in practice. It is unfortunate that a combination of delays, technical difficulties and

bureaucracy significantly reduced the value of the electronic consultation (which, ironically, in the process *could* have demonstrated the potential of the Internet to act as a forum for the public sphere envisaged by Habermas). The process highlighted the huge difficulties involved in reconciling a wide range of viewpoints and divergent agendas in the democratic process, and the subsequent compromises that were reached to accommodate a plethora of different groups representing different interests. The end result was a document that evidenced a dilution of the strength of commitment to the principle of freedom of expression from earlier drafts, in particular with regard to the emotive issue of principles of freedom of access for minors.

Another serious issue that was revealed by this particular case study was the importance of paying sufficient attention to the dissemination and evaluation stages of the policy process. Thus, despite the considerable amount of time and energy devoted to the consultation stage and to the subsequent careful reformulation and redrafting, the impact of the guidelines had been undermined, with the majority of public access providers unaware of their existence. It would certainly not be realistic to suggest that the guidelines have had any significant impact on the practice of most information professionals, and there is little evidence of their having exerted any influence on policy-making by national governments. A similar lack of attention to policy dissemination was seen at the organisational level in Institution C, where one respondent described how a new policy document 'sat on the Intranet for a couple of months and somehow become policy by default…but doesn't really get referred to' (Chapter Five, p.206).

7.4.2 The Re-Interpreted Policy Process: The Rational Actor, the Bureaucratic Imperative and the Garbage Can

The inability to achieve a successful solution to the 'problem' of Internet regulation would suggest that claims that the Rational Actor model of policy making represents an unattainable ideal (Rowlands and Turner, 1997) are supported in this policy area. The case study at Institution B indicated that the

policy-making process at this University *was* based on careful attempts to achieve rational and successful decision-making, with attention paid to consultation and evidence-gathering. However, even so the inability of policy formulators to achieve perfect control over the policy context (the fast-changing technical environment and the non-compliance of students, in particular) inhibited the achievement of policy goals. Evidence of a genuinely rational approach to policy formulation in this area was much less apparent at the other two case study sites. At the macro level, the multiplicity of competing agendas and priorities involved in formulating policy within the EU, the Council of Europe and the UK had also led to a subversion of the original policy goals.

This distortion of policy goals due to the impact of different policy actors and stakeholders is more suggestive of the Bureaucratic Imperative model, and indeed many of the characteristics of this approach could be seen at both macro and micro level. The diluted emphasis on the protection of freedom of expression in the final draft of the Council of Europe *Guidelines* as a result of the need to accommodate a wide range of divergent views is one such example. The powerful impact of organisational culture and departmentalism was particularly apparent at the micro level, especially in the rules-governed approaches taken to policy development at Institution C. This approach had, arguably, led to a relatively successful attempt in Institution C to limit misuse by students of network facilities, as indicated by the findings of the questionnaire study: however, it also appeared to have seriously undermined the trust and goodwill between academic and managerial staff, as well as having exerted a negative effect on the freedom of academic enquiry.

As could be anticipated, it was at the problem definition and agenda-setting stage of the policy process that features of the Garbage Can model could be seen most clearly. The role of a wide range of policy drivers, including a media-generated moral panic, in putting the 'problem' of the Internet onto both the public policy agenda and the institutional agenda, was very apparent. Similarly, the 'attachment' to this problem of measures that arguably were the result of the policy priorities of individual policy actors can be described as a characteristic of Garbage Can

policymaking. Fisher's interpretation of the implementation process of the Anti-Terrorism, Crime and Security Act is a good example:

> *[ATCSA] has become a legislative portmanteau into which have been dumped many measures that have nothing to do with terrorism or with any emergency…The Bill appears to have been prompted by a government that wants to be seen to be 'doing something' about terrorism.*
>
> (Fisher, 2002, p.16)

This would seem to be a classic example of a 'solution seeking a problem' and certainly reflects the findings of the monitoring of the policy process at national level: a 'solution' that the UK government had already determined that they wished to implement, was – post-September 11 – 'attached' to the 'war against terrorism'.

Characteristic also of the garbage can model was the legislative confusion that surrounds the conflicting provisions of much of the recent UK legislation in this area, in particular between the data interception and retention provisions of RIPA 2000 and ATCSA 2001, and the privacy provisions of the Data Protection Act 1998 and the *Human Rights Act* (Parliament, 1998a). The fragmentation of initiatives at both EU and Council of Europe levels, all emanating from different departments with a diversity of priorities, and the 'skewing' of outcomes to accommodate the agendas of the more powerful and/or vocal stakeholders, also provide a good illustration of the garbage can model in practice.

At the organisational level, the findings from the case study in Institution A indicated a tendency for measures to be implemented on an ad-hoc basis in response to pressures for regulation from individual stakeholders (as shown, for example in the case of the sensitivities of technical staff). The ability of technical staff at all three institutions to shape the issue definition and determine policy measures to address it, on account of their 'expert' knowledge, was also indicative of the garbage can model, as was the lack of consistency and coherence of

approaches to the regulation of Internet access and use and the lack of clear policy definition witnessed at the University College.

7.4.3 Extending the policy process model

The re-interpreted policy process model has thus proved useful as an analytical tool to identify and understand the characteristics and impact of features of the policymaking process at the different levels. Insights gained from the use of this model were used to extend the model to further illuminate the characteristics of the policy processes that were identified in the course of the work, whilst continuing to take into account the features of the existing models. Thus a new model, the reflexive spiral (figure 7.2), was designed. This incorporates the impact of both the internal, organisational context and that of external forces and is intended to illustrate the bi-directional, continually evolving nature found to be characteristic of the policy process in a fast-changing technological environment. In contrast to the staged, linear depiction of Lasswell's original model, this model is based on the spiral concept of the Action Research cycle (Kember, 2000, p.26) to show that, since it represents an ongoing cycle of review and evaluation leading to the adoption of new policy goals and a repetition of the policy stages, each new cycle begins from a changed position with a revised problem definition.

It should be noted that, although the model suggests smooth and continuous progress through the cycle, it is possible for policy makers to pay more attention to specific stages of the cycle. In real life, it has to be recognised that they may even omit a stage or stages altogether (as was indeed shown to be the reality of policy making in the case studies described here, particularly with regard to the consultation, dissemination and evaluation stages). In addition, while the policy process in some areas will be a continuous and evolving process, in other areas it will be a short term, finite process. In this case, the process will draw to a conclusion at the end of the first (or subsequent) iteration of the cycle.

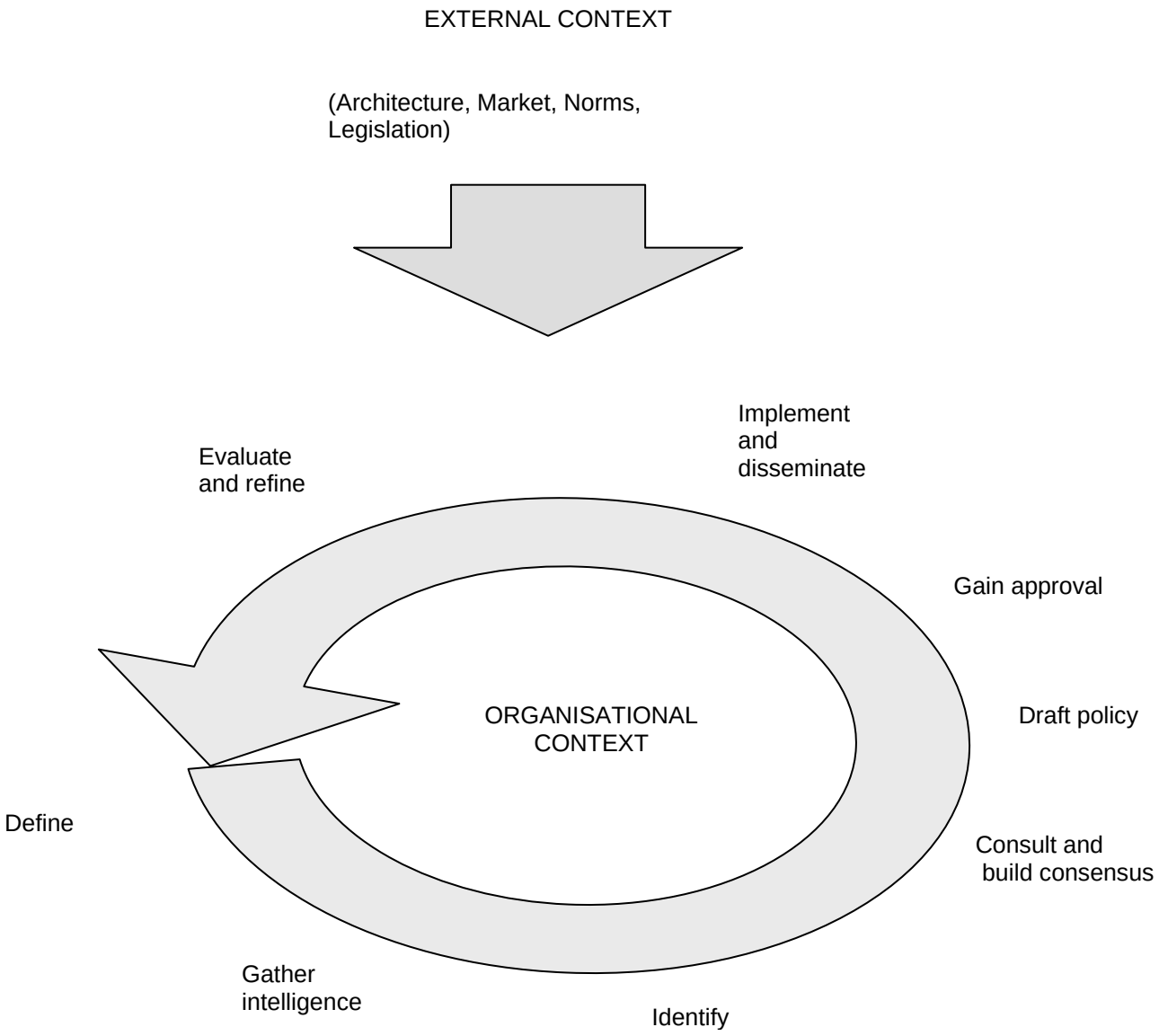


Fig. 7.2: The reflexive spiral model

This model shows policy as being shaped both within an organisational context (and therefore subject to the impact of factors such as organisational culture and individual policy actors) and by the impact of the external factors identified by Lessig (1999), that is architecture, social norms and values, market forces and legislative initiatives. Although in the model policy formulation and implementation are shown to go through the normal identified rational policy stages of problem definition, intelligence gathering, consideration of alternatives, and so on, these are not portrayed as finite stages, and the spiral can continue its iteration until the issue is no longer defined as a problem in need of a solution. Moreover, each 'cycle' of the iteration will take into account any changes in the problem definition that result from the evaluation and refinement stage of the previous cycle.

While this method of illustrating the policy process allows for the retention of the features of the rational actor, bureaucratic imperative and garbage can models, it is considered that it also offers new potential for recognising the problems inherent in formulating policy in a continually evolving environment. It allows for the integration of the features of the Lessig models, thus providing a powerful means of illustrating the different forces that impact to exert regulation in the policy environment. It is anticipated that the model could be used heuristically, both by researchers and by policy makers, to explore and define other areas of information policy. By providing an ongoing mapping of policy stages and by encouraging a consideration of both the organisational factors and the external factors that shape the policy context and policy options, it is intended to offer an analytical tool that engages with the current realities of the policy-making arena.

7.5 Appropriateness of methods adopted

It is a salient point to note that, without the existence of the very object under study, that is, the Internet as a source of information, a significant part of the research could not have been undertaken. As it was, the large amount of official

information made publicly available on the Internet by bodies such as the European Union, the Council of Europe, the UK government and a range of interest groups, brought the wide scope of the research within the realms of the manageable. Even so, it should be acknowledged that the academic study of a fast-changing information policy area such as this does entail considerable difficulties, especially when the study is necessarily carried out over a considerable period of time.

Involvement in the electronic consultation exercise staged by the Council of Europe illustrated the difficulties of research in which one does not have control over aspects such as the technical management of specific processes. Thus, in this instance, the delays and technical problems experienced by the Council invalidated much of this exercise. Although this insight into the workings of the Council did, in itself, represent a finding with regard to policy processes within the Council, it also inhibited the collection of more extensive data by the researcher. Had it not been for the opportunity to participate in the Helsinki Conference, the research into the policy formulation process within the Council would have been rendered very difficult.

With regard to methodology, the re-interpreted process model proved useful as an analytical tool that facilitated the identification of the many sources of complexity that were found to impact on the policy formulation process in this context. The model was also useful in providing an overarching framework within which to study this complexity. It afforded an enhanced theoretical understanding of information policy processes and ultimately led to the representation of the policy process via a new policy model with the potential this offers to provide theoretical insights for future academic information policy studies, as well as practical use for policy makers.

The use of the re-interpreted process model as a heuristic technique to explore policy formulation at each of the institutional, national and supranational levels has not been a feature in earlier applications of the model; this study has highlighted its usefulness as an appropriate tool for multi-level policy research, as

well as adding to the body of academic knowledge on the information policy process. This is of particular significance in the light of the limited frameworks and research tools currently available to inform the study of the information policy process (Turner, 1999). The combination of the use of the re-interpreted policy process model with the use of the models of direct and indirect regulation offered by Lessig (1999) to illustrate the impact and role of specific regulatory forces on the policy environment acted as a powerful mechanism for the analysis of policy formulation.

The consistency between the results found at the different levels of study (institutional, national and supranational), and in the different methodological components of the overall project (documentary analysis, participant observation, case study and questionnaire), suggests that the triangulation process has been useful to confirm the validity and reliability of the various findings. In particular, the combination of documentary analysis of formal policy statements with interview and questionnaire interrogation of those implicated in, or affected by, the formulation and enactment of policy, was instrumental in highlighting the difference between espoused policy and policy in action.

Turner (1999), among others, has noted the paucity of case studies that have been carried out in the information policy arena; it is anticipated that this study will contribute towards the existing limited stock of such research. The case study approach generated an in-depth insight into the policy formulation approach at each of the institutions, and in particular was crucial in gaining an appreciation of the viewpoint and experience of policy actors with very divergent agendas. This permitted a very real understanding of the multi-faceted and complex environment in which information policy is both formulated and implemented, particularly where sensitive and emotive issues such as pornography and freedom of expression are involved. It should, however, be acknowledged that the bounded nature of the case study as a research strategy inevitably limits the findings to a 'snapshot in time', as was the case here, rather than allowing for a longitudinal analysis of policy development over an extended period.

The use of semi-structured face-to-face interviews appeared to be an appropriate method, allowing a degree of consistency and adherence to the main research questions, whilst also allowing sufficient flexibility for interviewees to determine and develop the themes that they felt had been important in the policy process. The inductive and qualitative nature of the case study approach facilitated the intended emphasis and focus on the exploration of the policy process, and the impact of different forces and actors in shaping policy outcomes. Although it was never intended that the results of the case studies would afford a generalisable picture of policy formulation elsewhere, the use of the re-interpreted policy process model proved to be a robust interpretative tool with which to explore the implications of the findings.

The questionnaire study added a new dimension to the findings through its exploration of the practical reality of student use of the Internet. It should again be recognised that it is of limited valued in terms of generalisability, and some design shortcomings in the questionnaire instrument were identified in the course of carrying out the study. There was also a greater disparity in the composition of the student groups at the different institutions than would have been the ideal, but it was considered that the benefits of the researcher herself administering the questionnaire in a classroom environment were sufficient to justify the limitations imposed by this method. It also has to be acknowledged that piloting of the questionnaire instrument did not guarantee the prior identification of all potential analytical problems, as for example the ability to differentiate between an answer of 'don't know' and 'indifferent' on the Likert scale for questions 8 to 17. However, it is considered that, despite these limitations, the questionnaire proved to be a valid and reliable means of gaining an insight into the reality of the use by these students of university computer networks, and their experiences of, and attitudes towards, measures taken to regulate this use.

7.6 Conclusion

This discussion of the study's findings has suggested that the issue of regulating Internet content and use without risking an adverse impact on freedom of

expression and freedom of access to information was problematic at each of the levels studied. It is clearly not an issue that can be resolved through simplistic solutions, whether these are self-regulatory in approach or intended to achieve regulation through the imposition of the technical regulation of systems architecture.

The exploration of the policy process at the various levels indicated that the issue has occupied a high position on both public and institutional policy agendas, albeit with a changing focus of priority areas at the different levels and over time (e.g. on access by minors, or on the prevention of offence). Although a commitment to the value of protecting freedom of expression was voiced at each level, there was little evidence of this being a driving force in shaping policy, which was ultimately subject to influence from multiple policy actors and agendas.

The factors identified by Lessig (1999) as exerting regulation could all be seen to be involved in regulating Internet content and use, with legislation sometimes being used as an indirect means of influencing the other modalities of regulation. The use of the re-interpreted policy process highlighted the impossibility of achieving the ideal of totally rational policy formulation or implementation. Instead, it was found that organisational cultures and values, as well as the priorities of individual policy actors, were crucial in determining final policy outcomes.

CHAPTER EIGHT: CONCLUSIONS

> *Cyberspace has no intrinsic nature. It is as it is designed…An extraordinary amount of control can be built into the environment that people know [in cyberspace]. What data can be collected, what anonymity is possible, what access is granted, what speech will be heard – all these are choices, not "facts".*
>
> (Lessig, 1999, pp.216-217)

8.1 Introduction

This concluding chapter considers how the findings of the study contribute to the achievement of the research aims set out at the beginning, and outlines the conclusions reached in response to the overall research question. It also suggests some recommendations for policy makers concerning the process of policy formulation, and identifies some possible areas for future research.

8.2 Regulating the Internet: policy and practice

The study explored the 'problem' of regulation of Internet content and use and the policy responses to this issue in a variety of settings, over a period of time and at a range of levels. The research aimed to identify measures specifically intended to control and regulate access to illegal, 'harmful', 'undesirable' or 'inappropriate' content. The impact of such measures on intellectual freedom and freedom of expression were subject to particular examination during the course of the study. The following paragraphs summarise the principle substantive conclusions to the research.

1. The assertion that information policy formulation tends to be piecemeal, erratic and reactive to specific issues and lobbying by powerful stakeholders (Browne, 1997a) is supported by the findings of this study, both at the macro and at the micro level. The wide range of interested parties, policy actors and vested interests that were identified in the course

of the research could be seen to be impacting on policy in such a way that rational policy formulation was inhibited and policy goals were subverted.

2. In the course of exploring this specific aspect of information policy, the study indicated that regulation of the Internet is a problematic area for national governments and institutional organisations due to factors such as its inherently 'resistant' architectural structure, its transborder reach and the demands of conflicting legislative provisions.
3. Evidence did not support the notion that technical architecture can satisfactorily resolve the problem of reconciling content regulation with the protection of freedom of expression. Potential technical solutions have not yet been shown to be sufficiently robust and flexible to address the matter.
4. The policy measure of choice at all levels has tended to favour a self-regulatory approach, in some instances supported by other measures such as educational initiatives.
5. Nevertheless, the vision of Berners-Lee of the Web as 'a global space where people could share information, ideas and goods, unfettered by any central body' (Woolnough, 2001, cited on page 11 of the thesis) was not found to represent an accurate portrayal of the reality: on the contrary, it was demonstrated that the Internet, and within it the World Wide Web, is a closely regulated environment, subject to a multi-tiered governance structure. Indeed, the scope and impact of such regulatory measures appeared to be increasing at each of the levels investigated.
6. At the macro level, in particular, changes in policy emphases were identified, moving away from a focus on increasing access to network infrastructure and services, towards a focus on the prevention and detection of crime and terrorism. This had resulted in a significant shift away from a distributive perspective in favour of a more restrictive approach.
7. The findings indicate that no single policy measure has been successful in preventing the misuse of computer networks without simultaneously engendering a negative impact on freedom of expression or freedom of access to information.

8.2.1 Policy and practice – macro level approaches

At the **transnational level**, the **European Union** was seen to be involved in developing and implementing a number of initiatives with control of the use of the Internet at their centre. However, the longitudinal monitoring of EU policy revealed a continually changing cycle of shifts in emphases from initial measures aiming to develop the European network infrastructure and promote universal access to the Internet, moving towards a concentration on content regulation and the prevention of 'harm' to minors. The scope of content regulation has also been allowed to 'creep up' to include content areas such as violence and xenophobia. As the media focus on the Internet subsided and the subsequent moral panic lessened, a light-handed approach, based on self-regulation and aimed at producing a favourable environment for the encouragement of e-commerce, did appear to be emerging. However, the 'war on terrorism' declared by Western governments post-September 2001 has since led to increasingly restrictive measures on the part of the EU, particularly with regard to the monitoring and interception of Internet use and electronic communications.

At the **national level**, similar shifts in emphasis were seen in **United Kingdom** national approaches to the regulation of Internet content and use, from a perspective driven primarily by the demands of economic growth and competitiveness to one with a focus on security and the prevention of crime and terrorism. As with the EU the scope of content regulation in the UK has expanded to include that of defamatory, criminally racist and adult obscene content. Uncertainty over issues of legal liability has tended to encourage a cautious and restrictive approach with regard to the removal of Internet content on the part of ISPs in the UK. In addition, UK ISPs have been subject to extensive data retention, monitoring and interception legislative requirements.

At the level of a specific mission-driven **policy body**, the **Council of Europe** was shown to have freedom of expression as one of its founding priorities, and the safeguarding of this human right as being at the core of its mission. Nevertheless, with regard to the regulation of Internet content, this core value has come into

conflict with competing pressures to take action against 'undesirable' content, in particular pornographic material and content promoting violence and hate speech. Although the Council claims to afford the highest importance to the guarantee of freedom of expression (see, for example, Council of Europe, 1997f), the case study on the drafting and approval process for the *Guidelines on public access to and freedom of expression in networked information* demonstrated the dilution of this commitment in response to the pressure of alternative viewpoints expressed in the course of the consultation process. In particular, the right of minors to unfiltered public access to the Internet was significantly undermined in the course of the policy formulation process.

The research also indicated an extension of the realm of regulation with which the Council of Europe has concerned itself in regard to the Internet, with the *Convention on Cybercrime* representing involvement in a very broad area of crime prevention and control that would at one time have been considered as being outside the remit of the Council. It is perhaps surprising to find that an organisation with such a public commitment to human rights should produce 'the most far-reaching, comprehensive attempt to control communication over the Internet to date' (Castells, 2001, p.178; also cited on p.150 of this thesis).

At each of these levels a number of **common features** were apparent. The preferred measure of control at each of them has been that of voluntary self-regulation, together with support for the development of more sophisticated technological solutions. In this respect, a significant degree of coherence was found between the different bodies. However, it should also be noted that other legislative initiatives in force in the different arenas tended towards a different agenda or the favouring of different policy priorities (such as privacy and data protection), which in turn caused significant levels of policy confusion and uncertainty.

8.2.2 Policy and practice – micro level approaches

At the **organisational level**, actual and potential misuse of university computer networks was found to be a serious concern for UK Higher Education Institutions. As well as abiding by the provisions of the *Janet AUP*, such institutions are subject to a wide range of legislative measures that impact on their approaches to the control of the use of their computer facilities. In addition, at the institutions investigated by this study there was a demonstrable concern with the potential harm to institutional reputation, and to the work output of employees, that may result from misuse of their computer networks.

Within the institutions there was generally a low level of awareness among both academic staff and students of policy measures that were intended to regulate Internet content and use, although such awareness was more widespread in Institution B, which devoted considerable time and attention to policy promotion and dissemination. In all three institutions examples of serious misuse of computer networks were found to be taking place. Furthermore, whatever policy measures had been chosen to regulate Internet content and use in each of the institutions, and despite rhetoric supporting the principle of academic freedom, examples were found in each institution that indicated that academic enquiry was being inhibited as a result of such policy measures. In addition, these measures were found to be exerting a negative force on the trust-based relationship that had existed previously between academic and administrative personnel at the institutions.

8.3 Theoretical and methodological conclusions

The study has demonstrated that it is possible to use analytical tools such as policy models to gain a better understanding of the complex interaction of human, organisational and contextual factors that shape information policy formulation in a specific area. It has also shown how these same factors can act to impede policy implementation and the successful achievement of policy outcomes. The use of policy process models to simplify and explain the complexity of the environment

in which policy intended to regulate Internet access and use is formulated and implemented was found to be a useful and flexible heuristic technique.

Lessig's model illustrating the forces that can exert regulation on information flow has been shown to be applicable to, and illustrative of, the regulation of Internet content and use, particularly at the macro level. While the findings of the study do not support Lessig's premise of the supremacy of code as offering the highest potential level of protection to freedom in the electronic environment, his models have been shown to be relevant and of value in identifying the various forces that are exerted to restrict such freedom. His model of indirect regulation (see p.35), for example, has facilitated a better understanding of how, at the macro level, legislation can be used to manipulate a range of regulatory forces on information flow. It is particularly useful in alerting us to the potential dangers of a model of policy formulation and implementation lacking in transparency and accountability.

The re-interpreted policy process model (Rowlands and Turner, 1997), illustrated by the Rational Actor, the Bureaucratic Imperative and the Garbage Can models of policy formulation, has allowed for a critical analysis of the many varied and complex factors and policy actors involved in shaping policy towards Internet regulation, particularly at the organisational level. It has proved to be a useful tool for analysing a complex policy environment, and understanding the crucial impact of organisational factors on policy outcomes. Whilst characteristics of all three of these models of policy formulation and implementation were seen to exist in the institutions studied, the impact of bureaucratic expediency and the multitude of competing agendas found to be acting on policy formulation rendered the Bureaucratic Imperative and the Garbage Can processes as being the most useful models to illustrate the reality of this particular area of policy-making.

The use of this policy process model also facilitated the development of a new policy process model that can be used in the information policy field to illustrate and enhance the dynamic, evolving and bi-directional nature of policy formulation in an era of rapid technological development.

The results suggest that a policy approach that utilises a range of strategies incorporating legislative measures in specific domains, market control, self-regulatory practices and facilitating technologies is predominant with regard to the regulation of Internet content and access, and that this multiplicity of approaches is engendering a multi-tiered governance of the Internet both at the micro and at the macro level. In this highly regulated environment, it is crucial that policy measures should stress the benefits of the Internet as a medium rather than focus solely on suggested negative aspects, if the Internet is to fulfil its democratising potential to promote rational debate and recreate the public sphere.

8.4 Recommendations for policy makers

Given the importance of a consideration of specific social, cultural, technical and organisational contexts, combined with the accelerated rate of technological and social change in this policy area, it would be unwise to target any specific policy solutions as offering a panacea to the 'problem' of regulating Internet content. Instead, this section highlights some policy *process* issues that were identified in the course of the research as being crucial to the achievement of successful policy outcomes. Although a number of these may seem to amount to little more than common sense (and indeed could be seen as pivotal to the 'rational actor' model), the research revealed multiple instances of their being overlooked in practice.

Thus, in formulating policy, it is recommended that particular attention be given to:

1. Wide consultation with all relevant stakeholders in order to gain ultimate acceptance of chosen policy measures;
2. Evidence-gathering in order to ensure that policy solutions are based on an understanding of the *real* nature of the problem;
3. Dissemination and promotion of policy measures in order to achieve effective implementation and compliance with policy measures;
4. Flexibility and consideration of a wide range of alternative policy solutions rather than the hasty adoption of a seemingly expedient solution;

5. Continual re-evaluation of the nature of the problem and the effectiveness of policy measures – this is particularly important in an area such as that under consideration in this study, if technological, social and legal changes are to be accommodated;
6. Time frame – if all stages of the policy process are to be given adequate attention, it is essential to allow a realistic time-frame for the decision-making process;
7. Transparency in the decision-making process – this was notably lacking at two of the academic case study sites, leading to a lack of trust between policy-makers and stakeholders and ultimately, a rejection of policy solutions;
8. The role of values in the policy process, ensuring that the chosen policy measure is a true reflection of, and does not run counter to, intended underpinning values.

An example of the result of neglect of the latter principle could be seen in the case study of the drafting of the Council of Europe *Guidelines*, during which process the intended emphasis on freedom of expression was allowed to be subverted by other policy actors and influences.

8.5 Some areas for further research

From a methodological viewpoint, it has been concluded that the re-interpreted process model offers information policy researchers a valuable analytical tool with which to gain a better theoretical understanding of information policy processes at a range of levels. While it is believed that this study offers a significant contribution towards the development of a body of case studies exploring the formulation, implementation and evaluation of information policies at organisational, national and supra-national levels to fill the gap identified by Rowlands and Turner (1997), there remains a need for further such case studies. This has been shown to be particularly true in areas relating to ethical approaches to information use, for example with regard to attitudes towards the control of

filesharing and copyright infringement in the online environment. The application of the reinterpreted policy process model to such research could offer a powerful means of exploring the data obtained from such studies. In addition, such studies could provide an opportunity for testing the application of the reflexive spiral model to a wide range of areas of information policy formation.

It is recognised that the current study was limited in terms of the settings studied and it would be beneficial to extend the research into other case study sites, both within the UK and beyond. It would also be of potential value to follow up the institutional case studies with further research at the same sites to see how policy has changed in response to recent developments in technology, legislation and case law. Given the dynamic and ever-changing nature of policy and of technological developments with regard to the Internet, further longitudinal monitoring of policy at macro level could also prove to be useful and insightful.

The richness of the data obtained from the relatively limited sample of students surveyed with regard to their use of university computer network facilities, and their attitudes towards such use, suggests that it would be useful to extend the study across a much larger sample. In particular, the need for further objective research on the impact of music filesharing activity on music purchasing patterns has already been highlighted by Oppenheim and Robinson (2003). The current study supports the potential for such work, and suggests that the approach of using an anonymous questionnaire administered in a classroom setting offers a reliable means of data collection where relatively sensitive issues relating to illegal use of computer facilities are concerned. This would allow a better understanding of the reality of such use and its implications for policy and practice towards network regulation.

8.6 Conclusion

The distortion of public debate suggested by Habermas has been shown in the context of this study to be analogous to the impact of measures implemented to regulate access to Internet content. This is true not only as a result of the distorting

impact of governmental and organisational measures specifically aimed at exerting a regulatory impact on the Internet, but also as a result of such varied forces as use of the Web by multinational corporations to advertise and sell their products; the increased power of technocrats and Internet 'experts' to exert 'technological bamboozlement' (see p.217); and the ability of the mass media to construct a moral panic around the whole issue of Internet content. The condition of 'ideal speech' within the institutions studied was also shown as being inhibited by practical barriers such as inadequate technical infrastructures and a lack of user training and support. The concept of the Internet as a 'a contested terrain' (Castells, 2001, p.171) appears to be an accurate representation of a regulatory environment in which wide-ranging measures were found to apply to the control of Internet use and content. This was found to be true at each of the policy levels that were studied.

The findings of the study suggest that there is no perfect solution to the issues raised by the potential for misuse of computer networks, at either the macro or the micro level: even where policy had been formulated with considerable care and consultation, it was demonstrated that on the one hand misuse was still taking place, and on the other hand that there had been a negative impact on freedom of expression and freedom of access to information. This is consistent with the argument put forward by Mehta and Darier (1998) that electronic communication networks offer the potential for increased control, but also for increased resistance, and with the claims of Foucault (1977) that even the most sophisticated mechanisms of control can and will be resisted.

The study would tend to suggest that a flexible, constantly evolving, multi-tiered approach is required, and that measures taken should be subject to a critical approach with regard to their potential impact on freedom of expression and on freedom of access to information. In particular, close attention should be paid to the potential 'skewing' of policy towards the more closely regulated approach and strengthening of restrictions that may be the result of relocating the power balance towards those with expert technical knowledge. It is also imperative that concerns with issues such as the protection of institutional reputations and the avoidance of

potential legal action are not allowed to lead to an over-zealous approach towards Internet regulation. This is of critical importance to any information professional who supports the concept of freedom of expression as being at the heart of the profession and as representing the most fundamental guarantor of the preservation of democratic civilisation. While a comparison of the notion of the public sphere as a forum for the rational debate of public policy with the democratising potential of the Internet has been made, it is clear from the findings of this study that this potential was not being fully realised in the context under investigation.

BIBLIOGRAPHY

ACLU [online]. *American Civil Liberties Union.* <http://www.aclu.org> [Last accessed 5/7/2004].

ACLU (1997) [online]. *Fahrenheit 451.2: Is cyberspace burning? How rating and blocking proposals may torch free speech on the Internet.* ACLU. <http://archive.aclu.org/issues/cyber/burning.html> [Last accessed 5/7/2004].

Ahmed, Kamal (2002) Police to spy on all emails. *The Observer*, 9/6/2002, 1-2.

Akdeniz, Yaman (1997a) Governance of pornography and child pornography on the global Internet: a multi-layered approach. In: Lilian Edwards and Charlotte Waelde (eds) *Law and the Internet: regulating cyberspace.* Oxford: Hart.

Akdeniz, Yaman (1997b) [online]. The regulation of pornography and child pornography on the Internet. *Journal of Information, Law and Technology [JILT].* February 1997. <http://ltc.law.warwick.ac.uk/jilt/internet/97_1akdz/akdeniz.htm> [Last accessed 3/7/1998].

Akdeniz, Yaman (2001) Controlling illegal and harmful content on the Internet. In: David Wall (ed). *Crime and the Internet.* London: Routledge, Chapter 8.

Akdeniz (2003) [online]. *The Council of Europe's Cyber-Crime Convention 2001 and the additional protocol on the criminalisation of acts of a racist or xenophobic nature committed through computer systems.* Leeds: Cyber-Rights & Cyber-Liberties (UK). <http://www.cyber-rights.org/cybercrime/coe_handbook_crcl.pdf> [Last accessed 5/7/2004].

Akdeniz, Yaman and Nadine Strossen (2000) Sexually oriented expression. In: Yaman Akdeniz, Clive Walker and David Wall. *The internet, law and society.* Harlow: Pearson, Chapter 9, 207-230.

Akdeniz, Yaman and Clive Walker (2000) Whisper who dares: encryption, privacy rights and the new world disorder. In: Yaman Akdeniz, Clive Walker and David Wall. *The internet, law and society.* Harlow: Pearson, Chapter 14, 317-348.

Akdeniz, Yaman, Clive Walker and David Wall (2000) *The internet, law and society.* Harlow: Pearson.

American Library Association (1981) Statement on professional ethics. *American Libraries,* **12** (6) June, 335.

Amit, Vered (2000) The university as panopticon: moral claims and attacks on academic freedom. In: Marilyn Strathern. *Audit cultures: anthropological studies in accountability, ethics and the academy.* London: Routledge, 215-235.

Arrowsmith, S (1998) The regulation of the community: student discipline, staff discipline, grievances and harassment codes. In: D Palfreyman and D Warner (eds) *Higher education and the law: a guide for managers.* SRHE/Open University: Buckingham, 99-114.

Arthur, Charles, Andrew Marshall and Phil Reeves (1999) Who's looking over your shoulder? *Independent on Sunday,* 26/9/1999, 17.

Auld, Hampton (2003) Filters work: get over it. *American Libraries,* February, 38-42.

Australian Broadcasting Authority (1997) *The Internet and some international regulatory issues relating to content: A pilot comparative study commissioned by the United Nations Educational, Scientific and Cultural Organization.* Paris: UNESCO.

Bainbridge, Timothy (1995) *The Penguin companion to the European Union.* London: Penguin.

Baker, Edwin C (1989) *Human liberty and freedom of speech.* Oxford: Oxford University Press.

Bangemann, M (1995) Policies for a European Information Society In: PICT (Programme on Information and Communication Technologies) *1995 Charles Read Lecture.* Uxbridge: Brunel University, 5-12.

Baraschos, Emmanuel E (1998) *Media law and regulation in the European Union: national, transnational and US perspectives.* Ames: Iowa State University.

Barkham, Patrick (1998) Dissident and defiant slipping through the Net: Chinese man on trial for bypassing censor. *The Guardian,* 4/12/1998, 16.

Barnett, Ronald (1990) *The idea of higher education.* Buckingham: SRHE/Open University.

Barrett, Neil (1996) *State of the Cybernation: cultural, political and economic implications of the Internet.* London: Kogan Page.

Baty, Phil (2003) Northumbria threatens academic over email. *Times Higher Education Supplement*, 11/4/2003, 4.

Bawden, David (1997) Organizational perspectives: overview. In: Ian Rowlands (ed) *Understanding information policy.* London: Bowker Saur, 161-167.

BBC (2003a) [online]. Online child safety drive launched. *BBC News World Edition.* 6/1/2003. <http://news.bbc.co.uk/2/hi/uk_news/2629611.stm> [Last accessed 5/7/2004].

BBC (2003b) [online]. Extent of UK snooping revealed. *BBC News.* 16/5/2003. <http://news.bbc.co.uk/2/hi/technology/3030851.stm> [Last accessed 5/7/2004].

BBC (2003c) [online]. Academic jailed for child porn. *BBC News.* 30/5/03. <http://news.bbc.co.uk/2/hi/england/leicestershire/2951442.stm> [Last accessed 10/6/2003].

BBC (2003d) [online]. Music sharing tops net searches. *BBC News world edition.* 30/12/2003. <http://news.bbc.co.uk/2/hi/technology/ 3356397.stm> [Last accessed 4/1/2004].

Bekkers, V J J M (1997) The emergence of the Electronic Superhighway: do politics matter? In: Herbert Kubicek, William H Dutton, and Robin Williams. *The social shaping of information superhighways: European and American roads to the information society.* Frankfurt: Campus Verlag.

Bell, Judith (1993) *Doing your research project: a guide for first-time researchers in education and social science.* 2nd ed. Buckingham: Open University.

Bell, Daniel (1974) *The coming of post-industrial society: A venture in social forecasting.* London: Heinemann.

Bellamy, Christine and John A Taylor (1998) *Governing in the information age*. Buckingham: Open University.

Belson, William A (1986) *Validity in survey research: with special reference to the techniques of intensive interviewing and progressive modification for testing and constructing difficult or sensitive measures for use in survey research.* Aldershot: Gower.

Birley, Sir Robert (1972) *The real meaning of academic freedom.* London: World University Service.

Blanchette, Jean-Francois and Deborah G Johnson (2002) Data retention and the panoptic society: the social benefits of forgetfulness. *The Information Society,* **18**, 33-45.

Borchardt, Klaus-Dieter (2000) *The ABC of Community law.* Brussels: European Commission.

Bozovic, M (ed) (1995) *The panopticon writings.* London: Verso.

Browne, Mairead (1997a) The field of information policy: 1. Fundamental concepts. *Journal of Information Science.* **23** (4), 261-275.

Browne, Mariead (1997b) The field of information policy: 2. Redfining the boundaries and methodologies. *Journal of Information Science.* **23** (5), 339-351.

Bundy, M L and F J Stielow (eds) (1987) *Activism in American Librarianship, 1962-1973.* New York: Greenwood Press.

Burger, R H (1993) *Information policy: a framework for evaluation and policy research.* Norwood: Ablex Publishing Company.

Burnheim, Sally (1997) [online]. Freedom of expression on trial: caselaw under the European Convention on Human Rights. *Koaga Roneeta.* Series 1: Civil and Political Rights. <http://www.derechos.org/koaga/i/burnheim.html> [Last accessed 5/7/2004].

Burt, David (1997) In defense of filtering. *American Libraries,* **28** (7), August, 46-47.

Cabinet Office Performance and Innovation Unit (1999) [online]. *E-commerce@its.best.uk: the Government's strategy.* September 1999. <http://www.number-10.gov.uk/su/ecomm/ec_body.pdf> [Last accessed 5/7/2004].

Campaign for Internet Freedom [online] <http:// www.netfreedom.org/> [Last accessed 5/7/2004].

Campbell, Duncan (1998a) Author's porn films seized by police. *The Guardian,* 9/3/1998, 10.

Campbell, Duncan (1998b) Police tighten the Net. *The Guardian: Online supplement,* 17/9/1998, 2-3.

Campbell, Penny and Emmanuelle Machet (1999) European policy on regulation of content on the Internet. In: Liberty. *Liberating cyberspace: civil liberties, human rights and the Internet*. London: Pluto, Chapter 1, 13-43.

Capitanchik, David and Michael Whine (1996) *The Governance of cyberspace: Racism on the Internet.* London: Institute for Jewish Policy Research.

Castells, M (1997) *The power of identity.* Blackwell: Oxford.

Castells, M (2001) *The Internet galaxy: reflections on the Internet, business and society.* Oxford: Oxford University Press.

Center for Democracy and Technology [online]. <http://www.cdt.org> [Last accessed 5/7/2004].

Charlesworth, Andrew (2000a) The governance of the Internet in Europe. In: Yaman Akdeniz, Clive Walker, and David Wall. *The internet, law and society.* Harlow: Pearson, Chapter 3, 47-78.

Charlesworth, Andrew (2000b) [online]. New developments in UK Internet law. *Senior Management Briefing Paper 10.* JISC: April 2000. <http://www.jisc.ac.uk/index.cfm?name=pub_smbp10ukinternetlaw> [Last accessed 5/7/2004].

CILIP (2003) [online] *CILIP's Code of Professional Ethics: draft for consultation*. <http://www.cilip.org.uk/about/ethicsccode.html> [Accessed 30/6/2003].

Cincera, Patrizia (1999) The European Union content regulation in the converged communication environment. In: K A Eliassen and M Sjovaag (eds) *European Union telecommunications liberalisation.* London: Routledge, Chapter 5, 74-90.

Citizens Internet Empowerment Coalition (1997) [online]. *The Internet is not a television.* CIEC. <http://www.ciec.org/more_background.shtml> [Last accessed 5/7/2004].

Clarke, Arthur C (1965) *Voices from the sky.* New York: Harper & Row.

Cohen, Michael D, James G March and Johan P Olsen (1972) A garbage can model of organizational choice. *Administrative Science Quarterly,* **17** (1), 1-25.

Cohen, Stanley (1980) *Folk devils and moral panic: the creation of the Mods and Rockers.* 2nd ed. Oxford: Martin Robertson.

Collins, Richard and Cristina Murroni (1996) *New media, new policies: media and communication strategies for the future.* Cambridge: Polity.

Computers and Academic Freedom [online]. *Computers and Academic Freedom Archive.* EFF. <http://www.eff.org/CAF/> [Last accessed 5/7/2004].

Consumer Reports Online (2001) [online]. *Digital chaperones for kids; which Internet filters protect the best? Which get in the way?* <http://www.consumerreports.org/Special/ConsumerInterest/Reports/0103fil0.html> [Last accessed 5/7/2004].

Cooke, Louise (2001). Internet access policy and its effects on the search for knowledge in the academic environment. *Open 2001: Knowledge, information*

and democracy in the Open Society: the role of the library and information sector. Proceedings of the 9th International BOBCATSSS Symposium on Library and Information Science. Vilnius University, January 29-31 2001. Vilnius: BOBCATSSS.

Copdel, Jason (1999) *The Human Rights Act 1998: enforcing the European Convention in the domestic courts.* Chichester: Wiley.

Council of Europe (1950) *Convention for the protection of human rights and fundamental freedoms.* Strasbourg: Council of Europe. Also available online: <http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm> [Last accessed 5/7/2004].

Council of Europe (1961) *European Social Charter.* Strasbourg: Council of Europe. Also available online: http://conventions.coe.int/Treaty/en/Treaties/Html/035.htm [Last accessed 23/9/2004].

Council of Europe (1997a) *Recommendation (97) 19 on the portrayal of violence in the electronic media.* Strasbourg: Council of Europe.

Council of Europe (1997b) *Recommendation (97) 20 on "hate speech".* Strasbourg: Council of Europe.

Council of Europe (1997c) *Recommendation (97) 21 on the media and the promotion of a culture of tolerance.* Strasbourg: Council of Europe.

Council of Europe (1997d) [online]. *Media violence and intolerance: the Council of Europe urges its member states to act.* Press Release. Strasbourg: Council of Europe. <http://www.coe.fr/cp/97/634a%2897.htm> [Last accessed 13/8/2003].

Council of Europe (1997e) *Recommendation 1332 (97) on the scientific and technical aspects of the new information and communication technologies.* Strasbourg: Council of Europe. Also available online:

<http://assembly.coe.int/documents/adoptedtext/ta97/erec1332.htm> [Last accessed 20/4/2004].

Council of Europe (1997f) [online]. *Ministers pledge to promote new communications technologies and curb misuse.* Strasbourg: Council of Europe. <http://www.coe.fr/cp/97/731a%2897%29.htm> [Last accessed 12/8/2003].

Council of Europe (1999a) [online]. *Presentation of the International Conference on public access and freedom of expression in cultural institutions, Helsinki (Finland), 10-11 June 1999.* Strasbourg: Council of Europe. <http://www.coe.int/T/E/Cultural_Co-operation/Culture/New_Technologies/N.I.T/Working_strands/Public_access/Hel_presentation.asp> [Last accessed 19/8/2003].

Council of Europe (1999b) [online]. *Declaration on a European Policy for New Information Technologies.* Strasbourg: Council of Europe. Adopted by the Committee of Ministers on 7/5/1999 at its 104th Session, Budapest. < http://cm.coe.int/ta/decl/1999/99dec3.htm> [Last accessed 5/7/2004].

Council of Europe (2001a) *Recommendation (2001)8 of the Committee of Ministers to member states on self-regulation concerning cyber content (self-regulation and user protection against illegal or harmful content on new communications and information services).* Strasbourg: Council of Europe. Adopted by the Committee of Ministers 5/9/2001. Also available online: <http://cm.coe.int/ta/rec/2001/2001r8.htm> [Last accessed 5/7/2004].

Council of Europe (2001b) *Convention on Cybercrime.* Strasbourg: Council of Europe. Agreed in Budapest, 23/11/2001. Also available online: <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm> [Last accessed 5/7/2004].

Council of Europe (2001c) *Convention on Cybercrime: explanatory report.* Strasbourg: Council of Europe. Available online: <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm> [Last accessed 5/7/2004].

Council of Europe (2002a) [online]. *Self-regulation and user protection against illegal or harmful content.* Strasbourg: Council of Europe. <http://www.coe.int/T/e/human%5Frights/media/4%5FCyberfora/1%5FSelf%2Dregulation/3_Country_information/default.asp#TopOfPage> [Last accessed 5/7/2004].

Council of Europe (2002b) [online]. *The Council of Europe fights against racism and xenophobia on the Internet.* Strasbourg: Council of Europe. Press release. <http://press.coe.int/cp/2002/554a(2002).htm> [Last accessed 5/7/2004].

Council of Europe (2003a) [online]. *Council of Europe: an overview.* Strasbourg: Council of Europe. <http://www.coe.int/T/E/Communication_and_Research/Contacts_with_the_public/About_Council_of_Europe/An_overview/> [Last accessed 8/8/2003].

Council of Europe (2003b) [online]. *Declaration on freedom of communication on the Internet.* Strasbourg: Council of Europe. Adopted by the Committee of Ministers, 28/5/2003. <http://www.coe.int/T/E/Communication_and_Research/Press/News/2003/20030528_declaration.asp> [Last accessed 27/8/2003].

Council of Europe (2003c) [online]. *New Council of Europe response to the regulatory challenges posed by the Internet.* Strasbourg: Council of Europe. Press release. <http://press.coe.int/cp/2003/291a(2003).htm> [Last accessed 5/7/2004].

Craven, Jenny (1998) Surfing the ethical minefield. *Library Association Record,* **100** (5), May, Library and Information Show supplement, 27.

Creswell, John W (1997) *Qualitative inquiry and research design: choosing among five traditions.* London: Sage.

CSIRO (2001) [online]. *Filtering software products: assessment of effectiveness.* Australian Broadcasting Authority.

<http://www.aba.gov.au/internet/research/filtering/index.htm> [Last accessed 5/7/2004].

Curry, Ann (1997) *The limits of tolerance: censorship and intellectual freedom in public libraries.* London: Scarecrow.

Curtis, Polly (2004) University bans staff websites after anti-semitism row. *The Guardian,* 11/3/2004, 8.

Cyber-Rights & Cyber-Liberties [online]. *Cyber-Rights & Cyber-Liberties (UK).* <http://www.cyber-rights.org> [Last accessed 5/7/2004].

Datamonitor (2002) [online]. *Internet filtering: preventing porn and pushing productivity.* <http://www.commentwire.com/commwire_story.asp?commentwire_ID=3647> [Last accessed 5/7/2004].

Davies, Simon (2000) Why I believe email snooping is a threat to academic freedom. *Times Higher Education Supplement*, 10/11/2000, 18.

Davies, Simon (2002) A year after 9/11: where are we now? *Communications of the ACM*, September, 35-39.

Dean, Mitchell (1999) *Governmentality: Power and rule in modern society.* London: Sage.

Dearnley, James (1999) Teaching issues regarding obscenity and pornography in a LIS Department: can I teach it? How can I teach it? In: Maj Klasson, Brendan Loughridge and Staffan Lööf. *New fields for research in the 21st Century.* Procs. of the 3rd British-Nordic Conference on LIS, 12-14 April 1999, Boras, Sweden.

Dearnley, James and John Feather (2001) *The wired world: an introduction to the theory and practice of the information society.* London: Library Association.

Dempsey, Lorcan and Rachel Heery (1998) Metadata: a current view of practice and issues. *Journal of Documentation,* **54** (2), March 1998, 145-172.

Denscombe, Martyn (1998) *The good research guide for small-scale social research projects.* Buckingham: Open University.

Department of Trade and Industry (2003) [online]. *E-business: background and policy.* London: DTI. <http://www.dti.gov.uk/industries/ecommunications/ebusiness.html> [Last accessed 5/7/2004].

Dhavan, Rajeev and Christine Davies (eds) (1978) *Censorship and obscenity.* London: Martin Robertson.

Du Mont, Rosemary R (1991) Ethics in librarianship: a management model. *Library Trends,* **40**(2), Fall, 201-215.

Dunne, Steve (2001) Nobody rules OK? *The Guardian: Media supplement.* 16/7/2001, 52.

Dworkin, Andrea (1981) *Pornography: men possessing women.* London: Women's Press.

Dyer, Clare (2003) Code on 'spying' on staff emails. *The Guardian,* 12/6/2003, 7.

Edwards, Lilian and Charlotte Waelde (eds) (1997) *Law and the Internet: regulating cyberspace.* Oxford: Hart.

Electronic Frontier Foundation [online]. <http://www.eff.org> [Last accessed 5/7/2004].

Electronic Frontier Foundation (1996) [online]. *All about the Electronic Frontier Foundation.* San Francisco: EFF. <http://www.eff.org/ EFFdocs/ about_eff.html> [Last accessed 19/2/1998].

EPIC (1997) [online]. *Faulty Filters: how content filters block access to kid-friendly information on the Internet.* <http://www.epic.org/reports/filter-report.html> [Last accessed 18/7/2003].

EPIC (2001) *Filters and freedom 2.0: free speech perspectives on Internet content controls.* Washington, DC: EPIC.

EPIC and Privacy International (2002) *Privacy and human rights: an international survey of privacy laws and developments.* Washington, DC: EPIC.

Esposito, Gianluca (2003) [online]. Racist and xenophobic content on the Internet – problems and solutions: the Additional Protocol to the Convention on cybercrime. *International Journal of Communications Law and Policy.* January 2003. <http://www.ijclp.rog/7_2003/ijclp_webdoc_9_7_2003.htm> [Last accessed 3/2/2003].

European Commission (1992) *Treaty on European Union*. [Maastricht Treaty] Cm.1934. London: Stationery Office. Also available online: <http://europa.eu.int/abc/treaties_en.htm> [Last accessed 5/7/2004].

European Commission (1995) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Union,* L281, 23/11/1995.

European Commission (1996a) *Communication on the implications of the Information Society for European Union policies – preparing the next steps.* COM (96) 395, Brussels.

European Commission (1996b) *Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: Illegal and harmful content on the Internet.* COM (96) 487, Brussels.

European Commission (1996c) *Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services.* COM (96) 483. Brussells.

European Commission (1997a) [online] *Action plan on promoting safe use of the Internet.* <http://www.europa.eu.int/information_society/programmes/iap/docs/html/decision/276_1999_EC.htm> [Last accessed 5/7/2004].

European Commission (1997b) [online]. Illegal and harmful content on the Internet: Interim report on initiatives in EU Member States with respect to combating illegal and harmful content on the Internet. *Info 2000*, version 7, 4/6/97. <http://www.echo.lu/legal/en/internet/wp2en.html> [Last accessed 29/1/1999].

European Commission (1997c) *Commission Communication to the European Parliament, the Council and the Economic and Social Committee on the follow-up to the Green Paper on the protection of minors and human dignity in audiovisual and information services including a Proposal for a Recommendation.* COM (97) 570 final, 18.11.1997. Also available online: <http://europa.eu.int/scadplus/leg/en/lvb/ 124030.htm> [Last accessed 9/7/2003].

European Commission (1997d) [online] *Illegal and harmful content on the Internet: Interim report on initiatives in EU Member States.* Version 7, 4 June 1997. <http://europa.eu.int/ISPO/legal/en/internet/wp2en.html> [Last accessed 5/7/2004].

European Commission (1998a) [online]. *OII Guide to labelling, rating and filtering.* Brussels: European Commission. <http://www2.echo.lu/oii/en/labels.html> [Last accessed 28/9/1998].

European Commission (1998b) Proposal for a European Parliament and Council Directive on certain aspects of electronic commerce in the internal market. COM (1998) 0586. Brussels, 18/11/1998. *Official Journal of the European Union*, C030, 5/2/1999.

European Commission (1999) Decision No. 276/1999/EC of the European Parliament and of the Council adopting a Multiannual Community Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks. *Official Journal,* 1999 L33/1.

European Commission (2000a) [online]. *Fifth Framework Programme: schematic overview.* <http://europa.eu.int/comm/research/fp5/key.html> [Last accessed 5/7/2004].

European Commission (2000b) Directive 2000/31/EC of the European Parliament and the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market. *Official Journal of the European Union,* L178, 17/7/2000.

European Commission (2001) *Communication from the Commission to the Council and the European Parliament on the application of the Council Recommendation of 24 September 1998 concerning the protection of minors and human dignity.* COM (2001) 106 – C5 – 0191/2001 – 2001/2087 (COS).

European Commission (2002a) *Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions: Follow-up to the multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks.* COM (152) 2002, Brussels, 22/3/02. Also available online: <http://europa.eu.int/information_society/programmes/iap/programmes/followup/index_en.htm> [Last accessed 5/7/2004].

European Commission (2002b) Decision No 1513/2002/EC of the European Parliament and of the Council concerning the sixth framework programme of the EC for research, technological development and demonstration activities, contributing to the creation of the European research area and to innovation (2002-2006). *Official Journal of the European Union,* L 232/1, 29/8/2002.

European Commission (2003a) [online]. *Protection of minors: European Commission to propose improved framework during the first quarter of 2004*. Press release IP/03/1733, Brussells, 16/12/2003. < http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/03/1733&format=HTML&aged=0&language=EN&guiLanguage=en > [Last accessed 5/7/2004].

European Commission (2003b) Decision No 115/2003/EC of the European Parliament and of the Council amending Decision No 276/1999/EC adopting multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks. *Official Journal of the European Union,* L 162/1, 1/7/2003. Also available online: <http://www.europa.eu.int/information_society/programmes/iap/programmes/decision/index_en.htm> [Last accessed 5/7/2004].

European Commission Legal and Advisory Board (1997) [online]. *Response to the Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services.* <http://www2.echo.lu/legal/en/internet/gplabreply.html> [Last accessed 30/11/1998].

European Economic and Social Committee (2003) [online]. *Protection of children on the Internet.* Press Release 37/2003, Brussels, 2/6/2003. <http://www.esc.eu.int/pages/en/acs/press_rels/cp_eesc_37_2003_en.doc> [Last accessed 5/7/2004]

European Parliament (1996) *Resolution on the Commission Communication on illegal and harmful content on the Internet*. COM (96) 0487 – C4 – 0592/96.

European Parliament (1998a) [online]. *Resolution on the Information Society, the management of the Internet and democracy.* <http://www.europarl.eu.int/plenary/en/default.htm> [Last accessed 1/7/1998].

European Parliament (1998b) The Internet - tackling pornography and other abuses. Consultation Procedure [A4-0234/98 - Schmid]. *Session News: The Week*, Brussels 1-2 July 1998, pp.9-10.

European Parliament (1998c) Promoting safe use of the Internet. Co-decision procedure - second reading [A4-0377/98- Schmid]. *Session News: Strasbourg Briefing,* 16-20 November 1998, p.18.

European Parliament (2002) [online]. Self-regulation best for audio-visual industries. *Europarl Daily Notebook,* 11/4/2002. <http://www.europarl.eu.int/press/index_publi_en.htm> [Last accessed 5/7/2004].

Everall, Ian (1996) [online]. *Project EARL: Policy issues/public access strategies.* EARL, September 1996. <http://www.walsplsm.demon.co.uk/#INTRO> [Last accessed 12/2/1998].

Faulhaber, G R (1997) *Public policy for a networked nation.* Fontainbleau: Insead.

Fine, Philip (2000) Cyber Patrol halts student. *Times Higher Education Supplement,* 5/5/2000, 13.

Fine, Philip (2001) Academe branded unpatriotic. *Times Higher Education Supplement*, 23/11/2001, 56.

Finkelstein, Seth (1998) [online]. *Information about labelling and rating systems.* MIT Student Association for Freedom of Expression.

<http://www.mit.edu/activities/safe/labeling/summary.html> [Last accessed 5/7/2004].

Fisher, Mark (2002) No hiding place. *Index on censorship.* **2002** (1), 13-19.

Forum des Droits sur l'Internet. [online]. *Launch of the European Internet Coregulation Network to promote European collaboration on key Internet issues.* Press Release, December 2003. <http://www.foruminternet.org> [Last accessed 5/7/2004].

Foucault, Michel (1997) *Discipline and punish: the birth of the prison.* Harmondsworth: Penguin.

Foucault, M (1991) Governmentality. In: G Burchell, C Gordon and P Miller (eds) *The Foucault effect: Studies in governmentality.* London: Harvester Wheatsheaf, 87-104.

Gavison, Ruth (1998) Incitement and the limits of law. In: Robert C Post. *Censorship and silencing: practices of cultural regulation.* Los Angeles: Getty Research Institute, 43-65.

Gibson, William (1984) *Neuromancer.* New York: Ace Books.

Glaser, B G and A L Strauss (1967) *The discovery of grounded theory.* Chicago: Aldine.

Global Internet Liberties Campaign [online]. <http://www.gilc.org> [Last accessed 5/7/2004].

Goddard, Chris (2003) *Police request for monitoring site accesses*. Email communication posted to the Peoplesnetwork Jiscmail discussion list, 24/1/2003, forwarded to Lislink Jiscmail discussion list by Charles Oppenheim, 27/1/2003.

Golding, Martin P (2000) *Free speech on campus.* Lanham: Rowman & Littlefield.

Gomien, Donna, David Harris and Zwaak, Leo (1996) *Law and practice of the European Convention on Human Rights and the European Social Charter.* Strasbourg: Council of Europe.

Green, Stephen (1999) A plague on the Panopticon: surveillance and power in the global information economy. *Information, Communication and Society,* **2** (1), Spring, 26-44.

Greenslade, Roy (2000) 'I arrest you for emailing'. *The Guardian: Media Supplement,* 31/7/2002, 7.

Gringras, Clive (2003) *The laws of the Internet,* 2nd ed. London: Butterworths LexisNexis.

Guardian (1999) Academic fined over child porn. *The Guardian,* 28/5/1999, 13.

Habermas, Jürgen (1989) *The Structural transformation of the public sphere.* Cambridge: Polity.

Habermas, Jürgen (1984 and 1987) *The Theory of Communicative Action, vols. 1 and 2.* Cambridge: Polity.

Hamel, Jacques (1993) *Case study methods.* Newbury Park: Sage.

Hamilton, Stuart (2003) Culture's complications: the problem of global data collection in a world of difference. *New Library World,* **104** (1187/1188), 149-155.

Hannabuss, Stuart and Mary Allard (2001) Issues of censorship. *Library Review,* **50** (2), 81-89.

Harris, D J, M O'Boyle and C Warbrick (1995) *The European Convention on Human Rights.* London: Butterworth.

Harvard Law Review (1999) The law of cyberspace. *Harvard Law Review,* **112** (7), 1574-1704.

Harvey, Lee and Morag MacDonald (1993) *Doing sociology: a practical introduction.* Basingstoke: Macmillan.

Heins, Marjorie (2001) Criminalizing online speech to "protect" the young: what are the benefits and costs? In: David Wall (ed) *Crime and the Internet.* London: Routledge, 101-113.

Heins, Marjorie and Christina Cho (2001) [online]. *Internet filters: a public policy report.* New York: National Coalition Against Censorship. <http://www.ncac.org/issues/internetfilters.html> [Last accessed 5/7/2004].

Henley, J (2000) Search on for cybercrime fix. *The Guardian,* 16/5/2000, 12.

Hertz, Frederick (1962) *The Development of the German public mind: the Age of Enlightenment.* London: Allen & Unwin.

Hill, K A and J E Hughes (1998) *Cyberpolitics: citizen activism in the age of the Internet.* Oxford: Rowman & Littlefield.

Hill, M J (ed) (1993) *New agendas in the study of the policy process.* New York: Harvester Wheatsheaf.

Hill, Michael W (1994) *National information policies and strategies: an overview and bibliographic survey.* London: Bowker Saur.

Hogwood, B W and L A Gunn (1984) *Policy analysis for the real world.* Oxford: Oxford University Press.

Hosein, Ian, Prodromos Tsiavos and Edgar A Whitley (2003) Regulating architecture and architectures of regulation: contributions from information systems. *International Review of Laws, Computers & Technology,* **17** (1), 85-97.

Hunter, Christopher D (2000) Internet filter effectiveness – testing over- and underinclusive blocking decisions of four popular web filters. *Social Science Computer Review,* **18** (2), 214-222.

ICRA (2003) [online]. *About ICRA.* Internet Content Rating Association. <http://www.icra.org/about/> [Last accessed 5/7/2004].

IFLA (2003) [online]. *Digital Libraries: Metadata resources.* International Federation of Library Associations. <http://www.ifla.org/II/metadata.htm> [Last accessed 5/7/2004].

Information Commissioner (2003) [online]. *Monitoring at work.* Employment Practices Data Protection Code, part 3. <http://www.dataprotection.gov.uk/dpr/dpdoc.nsf> [Last accessed 5/7/2004].

Internet Watch Foundation (2003) [online]. *Report Statistics 2002.* <http://www.iwf.org.uk/about/annual_report/statistics/stat_report02.html> [Last accessed 5/7/2004].

Jaspers, K (1965) *The idea of the University.* London: Peter Owen.

JISC (2001) The Regulation of Investigatory Powers (RIP) Act: email and telephone monitoring. *Senior Management Briefing Paper, 14,* July 2001. Also available online: <http://www.jisc.ac.uk/index.cfm?name=pub_smbp_ripa> [Last accessed 5/7/2004].

Jordan, Tim (1999) *Cyberpower: the Culture and politics of cyberspace and the Internet.* London: Routledge.

Kahn, Robert et al (1997) The evolution of the Internet as a global information system. *International Information and Library Review,* **29**, 129-151.

Kember, David (2000) *Action learning and action research.* London: Kogan Page.

Kingdon, J W (1984) *Agendas, alternatives and public policies.* Boston, Ma.: Little Brown.

Knight, Peter (1998) When a book is worth a sentence. *Times Higher Education Supplement,* 27/3/1998, 20.

Lam, C K M & B C Y Tan (2001) The Internet is changing the music industry. *Communications of the ACM,* August, 62-68.

Lan, Zhiyong & Santa Falcone (1997) Factors influencing Internet use - a policy model for electronic government information provision. *Journal of Government Information,* **24** (4), July/August, 251-257.

Lasica, J D (1997) Censorship devices on the Internet. *American Journalism Review,* **19** (7), September, 56.

Lasswell, H D (1970) The emerging conception of the policy sciences. *Policy Sciences,* **1**(1), 3-14.

Laudon, Kenneth C (1995) Ethical concepts and information technology. *Communications of the ACM*, **38** (12), December, 33-39.

Left, Sarah (2002) [online]. Satirical website escapes closure. *Guardian Unlimited,* 2/10/2002. <http://www.guardian.co.uk/internetnews/story/0,7369,803132,00.html> [Last accessed 5/7/2004].

Lessig, Lawrence (1999) *Code and other laws of cyberspace.* New York: Basic Books.

Library and Information Commission (1997). *New Library: the People's Network.* London: LIC. Also available online: <http://www.ukoln.ac.uk/services/lic/newlibrary/> [Last accessed 5/7/2004].

Library and Information Commission (1999) *Keystone for the Information Age: a National Information Policy for the UK.* London: LIC. Also available online: <http://www.lic.gov.uk/publications/policyreports/keystone.html> [Last accessed 29/7/2003].

Library Association (1996) *Code of Professional Conduct and Guidance Notes,* 2nd ed. London: Library Association.

Library Association Record (1998a) Anger at art book confiscation. *Library Association Record,* **100** (4), April, 170.

Library Association Record (1998b) Watchdog starts filtering moves. *Library Association Record,* **100** (4), April, 174.

Library Association Record (1998c) ICT News. *Library Association Record,* **100**(9), September, 456.

Library Association Record (1998d) Internet censorship: US legislates as Britain volunteers. *Library Association Record,* **100** (9), September, 457.

Library Association Record (1998e) Internet censorship: EU promotes filtering. *Library Association Record,* **100** (11), November, 565.

Library Association Record (2001) Porn scare hits free access. *Library Association Record,* **103** (4), April, 192.

Livingstone, Sonia (2001) *Online freedom and safety for children*. London: Institute of Public Policy Research. Also available online: <http://www.ippr.org/research/files/team25/project72/IPPR.pdf> [Last accessed 5/7/2004].

Loney, Matt (2002) [online]. *ISPs spell out true costs of data retention*. London: ZDNetUK. <http://news.zdnet.co.uk/business/legal/0,39020651, 2127408,00.htm> [Last accessed 4/8/2003].

MacKinnon, Catherine (1993) *Only words.* Cambridge, Ma.: Harvard University Press.

Mahon, Barry (1997) European information policy: The role of institutional factors. In: Ian Rowlands (ed) *Understanding information policy.* London: Bowker-Saur, 101-113.

Manasian, David (2003) [online]. Digital Dilemmas. *The Economist,* 23/1/2003. <http://www.economist.com> [Last accessed 3/2/2003].

March, J G and J P Olsen (eds) (1976) *Ambiguity and choice in organizations.* Oslo: Universitetsforlaget.

March, J G and H A Simon (1958) *Organizations.* New York: John Wiley.

McGowan, W (1991) The part as prologue: the impact of international telecommunications. In: H Chaloner (ed) *Telecom 91 Global Review.* London: Kline.

McIver, William J Jnr, William F Birdsall and Merrilee Rasmussen (2003) [online]. The Internet and the right to communicate. *First Monday,* **8**(12), December. <http://firstmonday.org/issues/issue8_12/mciver/index.html> [Last accessed 5/7/2004].

McLuhan, Marshall and Bruce R Powers (1989) *The Global Village: transformations in world life and the media in the Twenty-first Century.* Oxford: Oxford University Press.

Mehta, Michael D and Eric Darier (1998) Virtual control and disciplining on the Internet: electronic governmentality in the new wired world. *The Information Society,* **14**, 107-116.

Mezey, Matthew (1998) Filtering comes under a legal challenge. *Library Association Record*, **100** (3), March, 122.

Middlehurst, R (1993) *Leading academics.* Buckingham: SRHE/Open University.

Mill, John Stuart (1859) *On liberty.* London: J W Parker.

Millar, Stuart (2001a) Handheld PC bridges digital divide. *The Guardian*, 9/7/2001, 6.

Millar, Stuart (2001b) Police get sweeping access to net data. *The Guardian,* 7/11/2001, 9.

Millar, Stuart (2002a) Europe votes to end data privacy. *The Guardian,* 31/5/2002, 1.

Millar, Stuart (2002b) Government sweeps aside privacy rights. *The Guardian,* 11/6/2002, 1-2.

Millar, Stuart (2002c) Snooping laws may be illegal. *The Guardian,* 31/7/2002, 2.

Millar, Stuart (2002d) Internet providers say no to Blunkett. *The Guardian,* 22/10/2002, 9.

Millar, Stuart and Nick Hopkins (2002) Blunkett secrecy attack. *The Guardian,* 14/10/2002, 1.

Millar, Stuart, Lucy Ward and Richard Norton-Taylor (2002) Blunkett shelves access to data plans. *The Guardian,* 19/6/2002, 1.

Miller, Steven E (1996) *Civilizing Cyberspace: policy, power and the Information Superhighway*. New York: ACM Press.

Milton, John (1973) *Areopagitica: for the liberty of unlicensed printing.* Oxford: Clarendon. Originally published 1644.

MIT SAFE [Online]. *MIT Student Association for Freedom of Expression.* Boston: Massachusetts Institute of Technology. <http://www.mit.edu:8001/activities/safe/home.html> [Last accessed 5/7/2004].

Moore, Nick (1991) Introduction. In: Ian Rowlands and Sandra Vogel. *Information policies: a sourcebook.* London: Taylor Graham.

Moore, Nick (1993) Information policy and strategic development: a framework for the analysis of policy objectives. *Aslib Proceedings,* **45** (11/12), November-December, 281-285.

Moser, Claus and G Kalton (1971) *Survey methods in social investigation.* 2nd ed. London: Heinemann.

NCH Action for Children (1998) *Children on the Internet: opportunities and hazards.* London: NCH Action for Children.

Newey, Adam (1999) Freedom of expression: censorship in private hands. In: Liberty. *Liberating cyberspace: civil liberties, human rights and the Internet*. London: Pluto, Chapter1, 13-43.

Nielsen//Netratings (2003) *Netview: home and work data.* New York: Nielson.

Norton-Taylor, Richard (2000). Spies seek access to all phone, email and net links. *The Guardian,* 1/12/2000, p.8.

Norton-Taylor, Richard and Stuart Millar (2002). Privacy fear over plan to store email. *The Guardian,* 20/8/2002, 1.

Office for National Statistics (2002) [online]. *Home Net access up: 11.1 million UK homes now online.* National Statistics Online. <http://www.statistics.gov.uk/cci/nugget.asp?id=8> [Last accessed 27/10/2002].

O'Leary, John (1998) Police want to destroy 'obscene' university book. *The Times,* 3/3/1998, 1-2.

Oppenheim, Charles (1998) Current UK and EU information policy. In: Maureen Grieves (ed) *Information policy in the Electronic Age.* London: British Library.

Oppenheim, Charles and Melissa Robinson (2003) [online] Loughborough University students' attitudes to P2P music file sharing. *Journal of Information Law and Technology [JILT]*, **8** (2). <http://elj.warwick.ac.uk/jilt/03-2/oppenheimandrobinson.html> [Last accessed 15/7/2004].

O'Toole, Laurence (1998) *Pornocopia: porn, sex, technology and desire.* London: Serpent's Tail.

Outhwaite, William (1994) *Habermas: a critical introduction.* Cambridge: Polity.

Overman, E Sam and Anthony G Cahill (1990) Information policy: a study of values in the policy process. *Policy Studies Review,* **9** (4), Summer, 803-818.

Pallant, Julie (2001) *SPSS survival manual: a step by step guide to data analysis using SPSS for Windows*. Buckingham: Open University.

Pallister, David (2003) New limits may allay fear on snooping. *The Guardian,* 12/3/2003, 8.

Parliament (1959) *Obscene Publications Act.* London: Stationery Office.

Parliament (1964) *Obscene Publications Act.* London: Stationery Office.

Parliament (1976) *Race Relations Act.* London: Stationery Office. Also available online: <http://www.homeoffice.gov.uk/docs/racerel1.html> [Last accessed 29/9/2004].

Parliament (1978) *Protection of Children Act.* London: Stationery Office.

Parliament (1984) *Video Recordings Act.* London: Stationery Office.

Parliament (1985) *Interception of Communications Act.* London: Stationery Office.

Parliament (1988a) *Malicious Communications Act.* London: Stationery Office. Available online: <http://www.hmso.gov.uk/acts/acts1988/Ukpga_19880027_ en_1.htm> [Last accessed 29/9/2004].

Parliament (1988b) *Copyright, Designs and Patents Act.* London: Stationery Office. Available online: <http://www.hmso.gov.uk/acts/acts1988/Ukpga_ 19880048_en_ 1.htm> [Last accessed 29/9/2004].

Parliament (1989) *Official Secrets Act.* London: Stationery Office. Available online: <http://www.hmso.gov.uk/acts/acts1989/Ukpga_19890006_en_1.htm> [Last accessed 29/9/2004].

Parliament (1990) *Computer Misuse Act.* London: Stationery Office. Available online: <http://www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm> [Last accessed 29/9/2004].

Parliament (1994a) *Criminal Justice and Public Order Act.* London: Stationery Office. Available online: <http://www.hmso.gov.uk/acts/acts1994/Ukpga_19940033_en_1.htm> [Last accessed 5/7/2004].

Parliament (1994b) *Trade Marks Act.* London: Stationery Office. Available online: <http://www.hmso.gov.uk/acts/acts1994/Ukpga_19940026_en_1.htm> [Last accessed 29/9/2004].

Parliament (1996a) *Broadcasting Act.* London: Stationery Office. Available online: <http://www.hmso.gov.uk/acts/acts1996/1996055.htm> [Last accessed 29/9/2004].

Parliament (1996b) *Defamation Act.* London: Stationery Office. Available online: <http://www.hmso.gov.uk/acts/acts1996/1996031.htm> [Last accessed 29/9/2004].

Parliament (1998a) *Human Rights Act.* London: Stationery Office. Also available online: <http://www.hmso.gov.uk/acts/acts1998/19980042.htm> [Last accessed 5/7/2004].

Parliament (1998b) *Data Protection Act.* London: Stationery Office. Available online: <http://www.hmso.gov.uk/acts/acts1998/19980029.htm> [Last accessed 29/9/2004].

Parliament (2000a) *Regulation of Investigatory Powers Act.* London: Stationery Office. Also available online: <http://www.legislation.hmso.gov.uk/acts/acts2000/20000023.htm > [Last accessed 5/7/2004].

Parliament (2000b) *Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations*. SI 2000 no.2699. London: Stationery Office. Available online: <http://www.hmso.gov.uk/si/si2000/20002699.htm> [Last accessed 29/9/2004].

Parliament (2001) *Anti-Terrorism, Crime and Security Act.* London: Stationery Office. Available online: <http://www.legislation.hmso.gov.uk/acts/acts2001/20010024.htm> [Last accessed 5/7/2004].

Parliament: House of Lords (1996) *Agenda for Action: Information Society, 5th Report.* Select Committee on Science and Technology. London: Stationery Office. Also available online: <http://www.parliament.the-stationery-office.co.uk/pa/ld199697/ldselect/inforsoc/inforsoc.htm> [Last accessed 5/7/2004].

Parsons, Wayne (1995) *Public policy: an introduction to the theory and practice of policy analysis.* Cheltenham: Edward Elgar.

Peace, Graham (1997) Academia, censorship and the Internet. *Journal of Information Ethics*, **6** (2), 35-47.

Peacefire [online]. <http://www.peacefire.org> [Last accessed 5/7/2004].

The People's Network (2002) [online]. *The People's Network: about us.* <http://www.peoplesnetwork.gov.uk/about/index.asp> [Last accessed 5/7/2004].

Pierce, Jennifer Burek (2003) Blaise Cronin: defender of CIPA. *American Libraries,* February, 41.

Pitman, Alan A (1997) *Feasibility of censoring and jamming pornography and racism in informatics: Draft final report to the STOA Panel of the European Parliament* [HA014D005b/0.1 Draft]. Smith System Engineering Ltd, May 1997.

Prior, Mary (2001) Surveillance in the Workplace: experience in a University context. In: Terrell Ward Bynum et al (eds) *Proceedings of the Fifth International Conference on The social and ethical impacts of Information and Communication Technologies: Ethicomp 2001.* Gdansk, June 18-20, 2001, 102-111.

QAA (1999) [online] University of Lincolnshire and Humberside and Skyline College, Sarjah, United Arab Emirates: Institutional Review Reports, September 1998. <http://www.qaa.ac.uk/revreps/oseas/LincHumUAE/LincHumUAE_ textonly.htm> [Last accessed 5/7/2004]

Quick Links [online] <http://www.qlinks.net> [Last accessed 5/7/2004].

Quinn, Sue (1999) Academic says child porn was for research. *The Guardian,* 27/5/1999, 13.

Reidenberg, J R (1996) Governing networks and cyberspace rule-making. *Emory Law Journal,* **45** (911). Also available online at: <http://web.archive.org/web/19971119123936/http://www.law.emory.edu/ELJ/volumes/sum96/reiden.html> [Last accessed 27/7/2004].

Resnick, P and H R Varian (eds) (1997) Recommender systems. *Communications of the ACM,* **40**, March, Special section, 56-89.

Robbins, Lord (1966) *Of academic freedom: an inaugural lecture under the 'Thank-offering to Britain Fund'.* London: Oxford University Press, for the British Academy.

Robertson, Geoffrey (1993) *Freedom, the individual and the law.* 7th ed. London: Penguin.

Rommetveit, Kåre (1976) Decision making under changing norms. In: J G March and J P Olsen (eds) (1976) *Ambiguity and choice in organizations.* Oslo: Universitetsforlaget, 140-155.

Rowlands, Ian (1996) Understanding information policy: concepts, frameworks and research tools. *Journal of Information Science,* **22** (1), 13-25.

Rowlands, Ian (ed) (1997) *Understanding information policy.* London: Bowker Saur.

Rowlands, Ian and Turner, Paul (1997) Models and frameworks for information policy research. In: Ian Rowlands (ed) *Understanding information policy.* London: Bowker Saur, 46-60.

Ryynänen, Mirja (1998) Green Paper on the Role of libraries in the modern world. 23 June 1998. *Official Journal of the European Union,* C313, 12/10/98. Also available online: <http://www.lib.hel.fi/syke/english/publications/report.htm> [Last accessed 26/10/1998].

Sabatier, Paul A (ed) (1999) *Theories of the policy process.* Oxford: Westview.

Saunders, Nick (1999) The Human Rights Act: research, freedom of speech and academic freedom. *Education and the Law,* **11**(3), 187-197.

Saxby, Stephen (2000) The roles of government in national/international Internet administration. In: Yaman Akdeniz, Clive Walker and David Wall. *The internet, law and society.* Harlow: Pearson, Chapter 2, 27-46.

Schneider, Karen (1997) *A Practical guide to internet filters.* New York: Neal Schuman.

Schramm, W (1971) *Notes on case studies of instructional media projects.* Working Paper, December 1971. Washington DC: Academy for Educational Development.

Shapiro, Andrew L (1999) *The Control Revolution: how the Internet is putting individuals in charge and changing the world we know.* New York: Century Foundation/Public Affairs.

Sheffield Today (2003) [online]. Ex-university head is jailed for child porn. *Sheffield Today,* 16/6/2003. <http://www.sheffieldtoday.net/ViewArticle.aspx?SectionID=58&ArticleID=533597> [Last accessed 31/7/2003].

Sherwin, Adam (2003) [online] Universities to be sued over music downloads. *Times Online,* 28/3/2003. <http://www.timesonline.co.uk/article/0,,2-625793,00.html> [Last accessed 5/7/2004].

Simon, Herbert A (1957) *Models of man: social and rational.* New York: Wiley.

Simon, Herbert A (1976) *Administrative behavior: a study of decision-making processes in administrative organization.* 3rd ed. New York: Free Press.

Slevin, James (2000) *The Internet and society.* Cambridge: Polity Press.

Smithers, Rebecca (1999) Parents told how to police Internet. *The Guardian,* 11/10/1999, 7.

Sola Pool, Ithiel de (1983) *Technologies of freedom: on free speech in an electronic age.* Cambridge, Ma.: Belknap.

Sommer, Peter (2000) Protection or persecution? *The Guardian: Online supplement,* 30/3/2000, 2-4.

Stewart, George R (1950) *The year of the oath: the fight for academic freedom at the University of California.* New York: Doubleday.

Stoker, David (1999) Filtering out minorities (editorial). *Journal of Librarianship and Information Science,* **31**(1), March, 3-6.

Strathern, Marilyn (2000) *Audit cultures: anthropological studies in accountability, ethics and the academy.* London: Routledge.

Strossen, Nadine (1996) *Defending pornography: free speech, sex and the fight for women's rights.* London: Abacus.

Sturges, Paul (1998a) *Freedom of Expression and the Communications Networks.* Strasbourg: Council of Europe. Also available online: <http://www.coe.int/T/E/Cultural_Co-operation/culture/Completed_projects/NIT/Sturges98_18.asp#TopOfPage> [Last accessed 5/7/2004].

Sturges, Paul (1998b) The political economy of information: Malawi under Kamuzu Banda, 1964-94. *International Information & Library Review,* **30**, 185-201.

Sturges, Paul (1999) *The Internet and academic freedom: implications for the university library.* Unpublished paper. Loughborough University, Dept. of Information Science.

Sturges, Paul (2000a) Public access to and freedom of expression in networked information: Guidelines for a European cultural policy. *Focus on International and Comparative Librarianship,* **31**(3), pp.149-152. The Guidelines are also available online: <http://www.coe.int/T/E/Cultural_Co-operation/Culture/Resources/Texts/CDCC-BU(2000)8_EN.pdf?L=E > [Last accessed 5/7/2004].

Sturges, Paul (2000b) The Council of Europe, freedom of expression and public access to networked information. *IFLA Journal,* **26** (4), 280-283.

Sturges, Paul (2001) The library and freedom of information: agent or icon? *Alexandria,* **13**(1), 3-15.

Sturges, Paul (2002) Public Internet access in libraries and information services. London: Facet.

Sturges, Paul, Eric Davies, James Dearnley, Ursula Iliffe, Charles Oppenheim and Rachel Hardy (2003) User privacy in the digital library environment: an investigation of policies and preparedness. *Library Management,* **24**(1/2), 44-50.

Sussman, Gerald (1997) *Communication, technology and politics in the information age.* London: Sage.

Swetenham, Richard (2003) *Safer Internet plus 2005-2008.* Email communication to the QuickLinks mail list, 11/8/2003.

Taylor, Andrew (1997) Pornography study launched. *Financial Times,* 14/2/1997, 7.

Teather, David (2003) Music swappers face legal action. *The Guardian,* 16/12/2003, 17.

Thomason, Sarah (2001) How can filtering help? *Library Association Record,* **103,**(6), 364-5.

Thompson, Kenneth (ed) (1997) *Media and cultural regulation.* London: Sage.

TIFAP (1997) [online]. *Learning from The Internet Filter Assessment Project.* <http://www.bluehighways.com/tifap/learn.htm> [Last accessed 5/7/2004].

Tight, Malcolm ed. (1998) *Academic freedom and responsibility.* Buckingham: SRHE/Open University.

Times Higher Education Supplement (2001a) Derby suspends six over net porn claims. *Times Higher Education Supplement,* 27/4/2001, 4.

Times Higher Education Supplement (2001b) Glasgow PhD student 'did not breach code'. *Times Higher Education Supplement,* 9/11/2001, 2.

Travis, Alan (2000) Watchdog moves to curb racist websites. *The Guardian,* 26/1/2000, 6.

Travis, Alan and Clare Dyer (2000) Ministers face policy challenges. *The Guardian,* 11/9/2000, 7.

Traynor, Ian (1998) Pornography test case for Internet providers. *The Guardian,* 13/5/98, 14.

Turner, Paul (1999) *Theory and practice in the analysis of Information Policy in the digital age: a case study on the formulation of the European Directive on the Legal Protection of Databases.* 2 vols. PhD Thesis, City University.

Valauskas, Edward J (1996) [online]. Lex Networkia: understanding the Internet community. *First Monday,* **4**. <http://www.firstmonday.dk/issues/issue4/valauskas/index.html> [Last accessed 5/7/2004].

Vidal, John (2000) The world at war. *The Guardian*, *Society supplement.* 19/1/2000, 4-5.

Vitiello, Giuseppe (1997) Freedom of expression online: how the ALA threw down the gauntlet to the US Government. *Focus on International and Comparative Librarianship*, **28**(3), December, 130-142.

Vitiello, Guiseppe (2000) Library policy and legislation: a European perspective. *International Information & Library Review,* **32**, 1-38.

Volokh, E (1997) [online]. Freedom of speech, shielding children and transcending balance. *Supreme Court Review*, **141**, 141-197. <http://www.law.ucla.edu/faculty/volokh/shield.htm> [Last accessed 5/7/2004].

Voorhof, Dick (1995) *Critical perspectives on the scope and interpretation of Article 10 of the European Convention on Human Rights*. Strasbourg: Council of Europe.

Walker, Clive (2000) Cyber-constitutionalism and digital democracy. In: Yaman Akdeniz, Clive Walker and David Wall. *The internet, law and society.* Harlow: Pearson, Chapter 6, 125-153.

Walker, Clive and Yaman Akdeniz (2003) Anti-terrorism laws and data retention: war is over? *Northern Ireland Legal Quarterly*, **54**(2), 159-182.

Walker, Clive, David Wall and Yaman Akdeniz (2000) The Internet, law and society. In: Yaman Akdeniz, Clive Walker and David Wall. *The internet, law and society.* Harlow: Pearson, Chapter 1, 3-24.

Wall, David (1997) Policing the virtual community: the Internet, Cyberspace and cybercrime. In: P Francis, P Davies and V Jupp. *Policing futures: the Police, law enforcement and the 21st Century*. Basingstoke: Macmillan, 208-236.

Wall, David (1998). Catching cybercriminals: policing the Internet. *International Review of Laws, Computers & Technology* **12**(2), 201-218.

Wall, David (2000) Policing the Internet: maintaining law and order on the cyberbeat. In: Yaman Akdeniz, Clive Walker and David Wall. *The internet, law and society.* Harlow: Pearson, Chapter 7, 154-174.

Wall, David (ed) (2001) *Crime and the Internet.* London: Routledge.

Wallace, J and M Mangan (1996) *Sex, laws and cyberspace.* New York: Henry Holt.

Walmsley, David (1998) Police confiscate Mapplethorpe book. *Daily Telegraph,* 3/3/1998.

Watson, Don (1996a) Cleaning up the global metropolis. *Library Association Record,* **98**(10), October, 498-499.

Watson, Don (1996b) How tight is the Safety Net? *Library Association Record,* **98**(11), November, 554.

Weingarten, F W (1989) Federal information policy development: The Congressional perspective. In: C McClure, P Hernon and H Relyea (eds) *United States government information policies.* Norwood: Ablex Publishing Company.

Wells, Matt (2000a) Freedom fear on website closure. *The Guardian,* 3/4/2000, 8.

Wells, Matt (2000b) Alarm as libel threats curb web's freedom of speech. *The Guardian,* 15/4/2000, 8.

Wojtas, Olga (1998) Key factors in the fall of a 'scientific racist'. *Times Higher Education Supplement,* 10/4/1998, 6.

Wood, Shirley (ed) (2003) [online]. *JANET Acceptable Use Policy v. 7.0.* UKERNA. <http://www.janet.ac.uk/documents/use_policy.pdf> [Last accessed 5/7/2004].

Woodward, Will (2000) Net firm pays out for alleged libel. *The Guardian,* 31/3/2000, 1.

Woodward, Will (2001) Children 'should be freer to roam Internet'. *The Guardian,* 30/1/2001, 14.

Woolnough, Roisin (2001) Web driver issues free ticket to ride. *Times Higher Education Supplement,* 30/3/2001, 17.

Wray, Richard (2003) Hewitt wants Internet access for all by 2008. *The Guardian*, 16/12/2003, 17.

Yin, Robert K (1993) *Applications of case study research.* Newbury Park: Sage.

Yin, Robert K (1994) *Case study research: Design and methods.* Thousand Oaks: Sage.

Zia-Zarifi, Saman (2001) In the information wars, we are on the front line. *Times Higher Education Supplement*, 19/1/2001, 14.