Identifying the Limits of Governmental Interference with on-line Privacy

Varvara Mitliaga

Βαρβάρα Μητλιάγκα

A thesis submitted for the degree of Doctor of Philosophy

The University of Edinburgh

October 2003

Abstract

This thesis addresses the issue of on-line privacy, in an effort to identify the limits of governmental interference with this kind of right. Traditional privacy has been a well accepted and legally recognized human right for many years now. However, the exposure of privacy to the Internet has created new threats that mould the nature of 'on-line privacy': a user is less aware of the dangers faced in cyberspace, due to the instinctive feeling of being alone when in front of a computer; the distinction between private and public places is blurred, cyberspace looks like a public space, but is actually an aggregation of privately owned digital spaces, open to public access. Taking this as a basis, the thesis explores the route to be followed in order for a well-balanced interference with on-line privacy to be designed. First, an analysis of computer-related crime, the major reason (or excuse) on which governments base the need to interfere and delimit privacy in the on-line environment. On-line delinquency may be a serious problem, but it has to be examined closer than it has been up to present if it is to choose effective measures to combat it. Second, the thesis analyses the legal reasons justifying governmental interference with on-line privacy. National security, public safety and the economic well being of a country are the most popular reasons appearing in laws regulating interference with an otherwise protected right, and they will play a prominent role in justifying interference with privacy in cyberspace; an approach on the meaning, use and difficulties met in their application can be a starting point in an effort to avoid the same problems in the on-line environment. The European Convention of Human Rights, being one of the most complete and effective legal forums for human rights protection, is then used to show how the legally acceptable justifications for interference with privacy are being implemented. The thesis goes on to examine cryptography: being one of the most valuable tools for the protection of on-line privacy, regulating its use and dissemination is a way of governmental interference. An approach of the efforts made to limit the use and dissemination of strong encryption shows how on-line privacy has been affected. It is further suggested that restrictions in the use of strong encryption have a much more detrimental effect for legitimate users than for those using it to conceal illegal activity. The effectiveness of these measures is, therefore, under question. Next, the UK Regulation of Investigatory Powers Act 2000 is analysed, mainly those parts that affect on-line privacy. RIPA regulates the use of investigatory powers in the on-line environment such as interception of communications, acquisition of communications data and governmental access to keys. Being one of the few examples of such legislation, a lot can be learnt from the mistakes made. Last, the thesis explores the threat posed to on-line privacy by systems of covert governmental surveillance. The Echelon and other major international surveillance systems is probably the most real threat for privacy in the on-line environment.

Declaration of originality

I hereby declare that the research recorded in this thesis and the thesis itself was composed and originated entirely by myself in the Faculty of Law at the University of Edinburgh.

Varvara Z. Mitliaga

dedication

to my parents Zissis and Artemisia Mitliaga

στους γονείς μου Ζήση και Αρτεμισία Μητλιάγκα

Acknowledgements

After three years of continuous effort to find something of real value among the vast amount of articles, books and thoughts, and manage to write it down, it seems unbelievable when you have finally reached the end. It is at this stage that you realise how important has been the help of the people who have accompanied you in this trip.

First I would like to thank my supervisors, Professor Hector MacQueen and Ms Lilian Edwards, for their valuable guidance through the paths of legal thinking. Their support has been unremitting throughout these three years, and their precious knowledge and experience has helped me go through the difficulties I met.

Next, I would like to thank IKY (The Greek State Scholarships Foundation) for its invaluable economic support for the whole three years of my studies. I would have never been able to take on this task without the scholarship I was awarded.

I also feel the need to express my thanks to all the friends around me who have made my days pleasant and helped me keep my wits about me, not letting me to forget that studying is not everything in this life. Especially I would like to thank George Vardoulias and Nomiki Karpathiou, Emmanouel Melissaris, Stassinos Stavrianeas, Konstantina Kyriakou, Korina Toliou, Sifis Fitsanakis, for encouraging me and for always being there when I needed them.

A huge thanks to my family, my parents Zissis and Artemisia and my sisters Dina and Natassa, for their endless and uncompromising support for everything I have chosen to do in my life, for believing in me and for accepting both my successes and failures, my ups and downs, my happiness and my sadness, with the same positive attitude always.

Last but certainly not least, I would like to thank Apostolos Georgiadis for always being there by my side, for loving me and caring for me, for accepting all the aspects of my character, for sharing his life and routine with me and helping me go through all the difficulties. He taught me to believe in my potential to do anything I decide. I thank him for encouraging me throughout this effort; I dare to say that if it hadn't been for him, I am not sure I would have written this PhD thesis.

Contents

Acronyms and abbreviations

ECJ	European Court of Justice
RIPA	Regulation of Investigatory Powers Act 2000
IOCA	Interception of Communications Act 1985
ISP	Internet Service Provider
ECHR	European Convention of Human Rights
EU	European Union
EC	European Community
OECD	Organisation for Economic Cooperation and Development
CCTV	Closed-Circuit Television
ID	Identity
NCIS	National Criminal Intelligence Service
ARPA	US Advanced Research Project Agency
DoS	Denial of Service Attack
FBI	Federal Bureau of Investigation
TEC	Treaty of the European Community

Chapter 1
Introduction

The literature around information technology and the Internet as a communication medium is already ample for those wishing to have a general picture on how the medium is evolving as part of our everyday life. However, discussion is not exhausted and probably it will never be, since this worldwide computer network is undergoing constant change. Especially when it comes to law we are still at a very early stage; the drafting and application of laws in the on-line environment is an issue that has just opened for discussion.

As obvious from the title of this thesis, the issue to be discussed is 'on-line privacy'. The reason why I decided to tackle privacy as it emerges in the on-line environment is simple. The majority of contemporary literature sees privacy as a whole, meaning as a single issue irrespective of the environment in which it is being exposed. It is not argued here that it is not; in the second chapter of the thesis it becomes very clear that on-line privacy is not much different from its off-line counterpart, especially when it comes to the underlying values and interests it seeks to protect. However, I consider that the special nature of the Internet affects privacy in a way different to that of the off-line world. For example, traditional assumptions, such as the existence of public or private spaces that tend to define the borders of our privacy exposure, are not valid for the on-line environment. The average user is usually unaware of how far his privacy is being exposed or violated during an Internet 'session'. On-line privacy is an issue needing separate attention, especially if we are to implement legislation affecting its protection.

The discussion on the nature of on-line privacy is a vital part of the thesis, however, it does not also fulfil its primary aspiration; it works as the starting point on which to base the rest of the analysis. The principal aim of the thesis, as revealed from its title, is to identify the limits of governmental interference with on-line privacy. Let us explain this agenda a bit further. The Internet has invaded our lives in a way that a considerable amount of everyday activity, both at home and work, involves a computer connected to this electronic 'superhighway' of information. As this activity is moving from real world to cyberspace it carries along, little by little, the legal context that surrounds it. This does not mean that existing laws are or should

be directly enforced in cyberspace, but rather that it is created a need, an expectation of secured rights and existing rules to be enforceable in this new environment. For example, when people buy and sell products or services through the Internet, they expect the same rules (with the necessary adaptation) to be operational in the on-line environment. However, the enforcement of existing rules in cyberspace cannot be an automated process for many reasons. First of all, the Internet is a transnational community, there is a lack of national boundaries; rules and legislation are not uniform in all countries, it is indeed difficult to combine them in a multinational society. Second, the architecture of cyberspace/ the underlying technology is under a constant and rapid development, there is no use in enforcing a law that may be ineffective in a few months. And third, two apparently analogous cases - in the real world and cyberspace respectively - may have substantial differences that prohibit the enforcement of existing rules in the on-line environment. In this context, this thesis tries to explore how far a government can and should go when interfering with privacy in the on-line environment.

A government can 'interfere' with the citizens' privacy in two ways: negatively and positively. The privacy of individuals, even though respected and protected in most of the world, is a legal right that needs to be forfeited in certain cases for the sake of the general good. A person's residence, for example, needs to be searched when that person is suspected to have committed a crime. Personal information on citizens' income must be obtained by the state in order to impose taxes. The state in these cases is interfering with the privacy of citizens in order to meet the needs and promote the general well-being of a country. A government, operating as the personalisation of a state, is that who 'interferes' with privacy through its agencies (law enforcement, security services, tax agencies etc.). Let us call this 'negative interference' in a sense that privacy is compromised by the state. The privacy of individuals, however, is not only compromised by the state; third parties, either individuals or legal entities, can also violate privacy in many ways. Privacy, for example, is invaded when a person is being unwillingly photographed, or when personal information about his person are being unwillingly gathered, or when his communications are being overheard, etc. The role of the state in these cases is to provide the legal framework for the protection of privacy from violations of this kind. Let us call this 'positive interference' in a sense that privacy is protected by the state.

When we move to cyberspace, the same speculation comes to one's mind. Privacy on the

Internet (on-line privacy) is a right that, even though respected, will have to be forfeited as well in many cases (i.e. the investigation and prosecution of on-line crimes), and is going to be invaded by third parties (i.e. on-line companies who place cookies in their visitor's computers or gather personal information, people who intercept on-line communications etc.). The former is again a type of negative interference by the state, whereas the latter needs to be 'delimited' by positive interference. However, there are certain limits as to how far negative and positive interference can go; they cannot be arbitrary. Especially when it comes to negative interference, the balance between acceptable and unacceptable interference is very fragile. A state is by default in a considerably superior position compared to the citizens; it is the state that imposes laws and usually controls the dissemination of technological development (i.e. encryption as will be seen in chapter 5). A state, of course, is supposedly acting to promote the well-being of its citizens and not suppress them, however, authority can always be abused or handled badly. As will be seen in chapter 7, many states (especially the powerful ones such as US, UK and many European countries) operate or participate to systems of secret surveillance targeting both foreigners and their own nationals, in order to gather intelligence and gain diplomatic advantages. Apart from that, governments do change hands and democracy can never be absolutely guaranteed. It is dangerous to allow the creation of possibilities that could be easily abused in the future, were things to change. Positive interference has some limits as well. There are certain cases where a state needs to interfere and regulate how far privacy can be compromised or not by third parties, and certain cases where it should not. For example, when it comes to the compromise of privacy by third parties who are stronger than individual citizens (like the press, or big companies, employers etc.), a state would rather need to interfere in order to protect people's privacy by regulation.

The main focus of this thesis is 'negative interference', how far a government can and should go when itself is compromising the on-line privacy of its citizens. However, positive interference is not completely left out since it is an integral part of the discussion on on-line privacy. The major aspiration of the theses is to explore the *route* that ought to be followed, in order for a legal framework of interference to be effectively designed. In other words, the aim of the thesis is to analyse the steps to be followed and the issues that should be taken into consideration in order for this framework to be designed in the best possible way (rather than propose an exact legal framework for governmental interference with on-line privacy).

The first step of this analysis (chapter 2) is an approach on-line privacy as such in order to

understand what it is, its differences and similarities with off-line privacy, and its special needs and nature, so as to decide if and in what way it should be treated differently in terms of law. Chapter 2 begins with a general discussion on privacy, analysing what it is and the protection it is afforded by law on an international and European level, and especially within the UK and US. An effort is made to explain the three aspects of privacy: informational, accessibility and expressive. The discussion proceeds on this base by analysing on-line privacy, how its separate aspects are exposed in the on-line environment, and what is its special nature.

Once on-line privacy is explained, the second step of the process is to analyse the reasons why a government would want to interfere with this right. Chapter 3 discusses computer-related delinquency, presented as the actual and most popular reason why interference with on-line privacy is considered essential by governments. According to this line of argument, on-line privacy needs to be compromised to a certain extent in order to combat computer-related crime. Computer crime and several other forms of criminal behaviour that are enhanced by the use of computers and the Internet (such as terrorism or organised crime and paedophilia) constitute the most popular reasons why governments (basically law enforcement agencies) consider it essential to compromise on-line privacy. This compromise can take many forms like access to private communication or data travelling through the Internet, on-line surveillance, seizure of encryption keys, acquisition of personal and communications data from ISPs etc. By this compromise, all aspects of privacy can be offended: informational (when personal data or encryption keys are seized), accessibility (with on-line surveillance) and expressive (when a person's on-line anonymity is compromised). It has to be explained at this point that this chapter is not about crimes against the state. A government has usually many reasons to interfere with citizens' privacy, and one of them is when the interests of the state as such are offended. However, one of the major responsibilities of a state is to preserve the security and safety of people; in this context it needs to combat delinquency of all kinds, from simple crimes between individuals to complex threats against the society. This chapter tackles with criminal behaviour in cyberspace and tries to discuss how big a problem computer-related delinquency is and how far interference with privacy as a response can be justified.

The next step to be followed (chapter 4) is to explore the legal justifications allowing this interference and see whether and how they could apply in the on-line environment. Chapter 4

analyses three major reasons that are regularly used in the context of law in order to justify interference with otherwise protected rights (national security, public safety and the economic well-being of a country). In addition to that, it includes an analysis on the European Convention of Human Rights and the way its Court has interpreted the conditions under which interference with privacy is allowed. The reason why this approach is taken is because the Convention is one of the most complete legal forums in terms of human rights protection and is always a reference point for human rights legislation in Europe. So the way these conditions have been interpreted by the European Court of Human Rights can be used as a starting point on which to build possible legislation about interference with on-line privacy.

Moving on to chapter 5, the issue of cryptography and its use in the on-line environment is approached. Cryptography is one of the most popular and effective technological tools available for protecting on-line privacy. In effect, regulating the use and availability of encryption constitutes an interference with on-line privacy, since it has a major effect on how on-line privacy can be protected. This chapter tries to present the efforts made up to present to regulate encryption and discusses their effect on on-line privacy. Chapter 6 is dedicated to a new law recently enacted in the UK, the Regulation of Investigatory Powers Act 2000. Being one of the few existing concrete pieces of legislation affecting on-line privacy by allowing interference by the government, this law is analysed here as an example of how far this interference can go and whether it is acceptable or not. The aim of chapter 6 is to find out whether the special needs of on-line privacy have been taken into consideration by the drafters of this law, and discuss the effects of the regulation for the protection of on-line privacy.

Finally, Chapter 7 is an effort to present and explore an, often neglected, factor that should play an important role as far as on-line privacy is concerned. This factor is the existence of major covert surveillance systems, operated by the Secret Services of countries, and the threat that they pose for on-line privacy. This is an issue that is usually left aside when a law is being drafted. However, this author believes it should play an important role since it is vital to know how and by whom can privacy be compromised when it is being exposed to certain vulnerabilities created by law. Since this is a sensitive issue, it is important to make clear at this point that this author is not obsessed and fascinated by conspiracy theories; an effort is made to simply discuss information that has already seen the light of publicity and has been verified by dependable sources.

Before proceeding to the actual discussion, it is also vital to clarify a few things that may enhance a better understanding of this thesis's position. First of all, the author is very much aware of the fact that the on-line environment is in a process of constant change. The research for the writing of this thesis was completed in May 2003. Since then, many things may have changed, others substantially and others only superficially. Even though a considerable effort has been made to keep up with this constant change, the reader may still identify certain gaps or omissions. I would like to think that there is still space for commenting and evaluation, even for the things that have slightly evolved. Second, for the needs of the analysis, reference will be made many times in the thesis to the 'Internet user'. This is the average user; he is neither a computer freak who spends 24 hours a day in front of the monitor, nor a person who only knows how to log on and off the Internet, and does that once a month. The average user is a person who makes reasonable use of the Internet and computers, and has a fair knowledge about the mechanics, the underlying technology and the possibilities offered. Third, even though throughout the thesis several examples and comparisons are used in the course of the discussion, the author believes that, when using examples, there is always something missing. Two apparently comparable situations may have slight but substantial differences that prevent an analogy from being utterly successful. The reason this is underlined is because the author would prefer the reader to comprehend the analogies used in the thesis loosely and not strictly.

It is also important to add a comment on the nature of the sources used for the writing of this thesis. Since on-line privacy is not yet an issue with definite and clear aspects, views remain polarised. There are those who believe that, since cyberspace is an open area, there is no such thing as 'on-line privacy' (an approach that may prove very dangerous if we take it for granted, according to this author's point of view). There is also another group of commentators who are strongly pro cyber-rights and cyber-liberties, and whose main aspiration is to promote the protection of rights and liberties on the Internet. Even though this is not a dangerous position, a lot of the material that derives from these sources may not be considered objective enough to be included in a PhD thesis. A serious effort has been made to use the sources in an objective way, irrespective of their origin, extracting the useful information and not the pre-biased comments, even though it has not always been easy.

A final, maybe unnecessary, but still important note: while I was writing this thesis, one thought kept coming into my mind. Even though we consider the Internet as a very powerful

medium that has invaded our everyday lives, the amount of people that it affects on a worldwide scale is actually only a small percentage of the global population. Computers and the Internet may play a vital role for the everyday life of a citizen of the western world, but things are very different for the average Latin American, Asian or African citizen. For people in the developing world privacy is a luxury rather than a commodity, in a sense that people tend to discuss about matters such as privacy only after having solved vital issues such as securing their food, shelter, peace and democracy. By saying that I do not mean to downgrade the discussion on privacy but simply to put it in the right perspective. I am sure that people need and cherish their privacy irrespective of the circumstances of their lives. It is, however, useful to appreciate the fact that we are in the privileged position to spend time discussing about privacy.

Chapter 2

Aspects of on-line privacy: the need for protection

privacy n. : 1) a state of being private and undisturbed
2) a person's right to this
3) freedom of intrusion or public attention
4) avoidance of publicity
(in Oxford English Dictionary)

2.1 Preface

Having a clear picture of the nature and idiosyncratic features that characterise so-called *on-line* privacy is an essential prerequisite of engaging in an elaborate effort to set out the limits and conditions of governmental interference with this kind of privacy. The aspiration of Chapter 2 is to satisfy this very precondition, to the extent allowed by the space limits of this thesis. At first glance, this chapter may seem irrelevant or superfluous to the rest of the thesis, due to the fact that it does not provide the reader with particular answers to the questions posed by the title. However, this author considers it as an indispensable starting point, since it provides the reader with the background on which the rest of the analysis will be based. In other words, it is an effort to explain on-line privacy as a right that derives from, but is not the same with traditional privacy, and present its special needs in terms of legal protection. This chapter was considered essential because, although there is much discussion about the way our privacy is being affected by or violated through the Internet, there is little literature on what exact aspects of a person's private sphere are being exposed when one goes on-line and how important this can be. In effect, although it does not refer to governmental interference with on-line privacy as such, chapter 2 gives the background on which the reader will be based to comprehend why interference with this right can be detrimental. But before touching the issue of on-line privacy specifically, an effort will be made to reach an understanding of traditional privacy and briefly present the legal protection it is afforded. A thesis on on-line privacy would be incomplete without a general discussion on the traditional right. The experience gained from existing preconceptions and legal frameworks may well be used as a guideline in the effort to identify a right balance between on-line privacy and the acceptable limits of governmental interference.

2.2 Thoughts on on-line privacy

Let us begin with a few thoughts. The word *on-line*, added as an adjective before the well-known term *privacy*, gives rise to a number of questions both for analysts and simple users. Is on-line privacy indeed a novel value, or is it merely an extension, a new aspect of the traditional concept of privacy? How does it feel to an average user? Is it a value worthy of protection? And if so, to what extent can it be effectively covered by the existing legal protection afforded to traditional privacy? Despite the fact that the answer to these questions cannot be either straightforward or conclusive (due to the comparatively new and constantly changing nature of the Internet), it remains essential to examine the present nature of on-line privacy and make out the existing differences and similarities with its off-line counterpart, at least those that have been prominent by now.

In survey after survey, Internet users cite privacy as one of the most important issues facing the medium today;[1] indeed, over three-quarters would go on-line more often if they felt that the confidentiality of their personal information and communications was secure,[2] either from private companies who apply several techniques in order to gather personal data, or governments who are interested in monitoring on-line behaviour of their own or foreign citizens. In fact, as will be later discussed, on-line privacy can be interfered either by state or private/commercial actors. (As explained at the introduction this thesis will focus on the former, although some reference to the latter will also be made.) Even though the problem has been clearly identified by users, it is doubtful whether the same people would give an equally clear answer if asked to define on-line privacy. Personal information and communications are certainly two of its aspects but they do not suffice to complete the picture. It is like real world privacy: we may all understand what it means, especially when we lose it, but we find it very difficult to define in an all-encompassing way. It has not been much easier for legal scholars to give an effective definition. A perpetual problem following any discussion of the subject is that there are as many definitions of the notion of privacy as

[1] See Graphic, Visualisation & Usability Centre (GVU) , 8th WWW User Survey, para.11 (11 Oct. 1997), (available at <http://www.gvu.gatech.edu/user_surveys/survey-1997-10/>, last visited on 23/04/2002).

[2] See E J Sinrod and B D Jolish, "Controlling Chaos: The Emerging Law of Privacy and Speech in Cyberspace", (1999) *Stanford Technology Law Review* 1 (available at <http://stlr.stanford.edu/STLR/Articles/99_STLR_1/article_pdf.pdf>, last visited on 23/04/2002).

there are commentators on the issue.[3] One of the first and still most famous efforts to define privacy was made in 1890 in the United States by Louis Brandeis and Samuel Warren in a law review article.[4] They explained privacy as 'the right to be left alone', as it was then conceived in the context of invasions to the privacy of individuals perpetrated by the press. But it is undisputed by now that privacy is much more than that.

Furthermore, as a commentator observed when contemplating the connotations of privacy it is of considerable importance to make clear whether one is discussing a state or condition, a desire, a claim or a right. Everyone understands the state of privacy, how it feels to be withdrawn from the society of others, to avoid publicity, be solitary or retire from the world's activities. The desire of achieving such a state is also easily conceived. But it is one thing to desire and another to claim or even have a right to privacy. To claim means to be entitled to achieve it as one desires, and to be given a right means that this claim is recognised by the law, even against adverse claimants.[5] There is an interconnection between these four elements: the picture is incomplete if one is missing. Understanding the state of privacy is a prerequisite for desire; desire leads to the formulation of claims; and when these claims are recognised by law the picture of a right to privacy is complete.

Perception of these elements may differ significantly, however. It is well accepted that privacy is culture-specific, in the sense that what particular societies regard as private vary widely. We do not need to go very far in order to grasp the reality of this statement; differences in the perception of privacy, and much more in its legal recognition as a right, exist between similar cultures as well as between starkly different societies. Let us take an example within the western culture. In the UK there has been serious resistance to the idea of carrying and routinely presenting a photo ID, an objection based on the view that such a request would constitute an intrusion into people's privacy; whereas in France, US and many other western countries this idea is more acceptable, as it is not considered a serious threat to

[3] M A Hogg, "The Very Private Life of the Right to Privacy", in H L MacQueen (editor) *Privacy and Property*, Hume Papers on Public Policy: Volume 2 No. 3 Autumn 1994, Edinburgh University Press, at p.2.
[4] L D Brandeis and S D Warren, "The Right to Privacy", (1890) 4 *Harvard Law Review* 193.
[5] J Michael, *Privacy and Human Rights (An International and comparative study, with special reference to developments in information technology)* (1994) UNESCO, at p.2.

privacy.[6] This author was born in Greece where it is compulsory for every person above the age of fourteen to have an ID card (which until recently included such private data as the religion of the holder). Even though people are not obliged to carry it constantly, it has so many uses that the majority of the population turn out to keep it in their wallet (and so do I). Interestingly enough, I never considered my ID card as a threat for my privacy, at least not until I started studying privacy. If I were born in Britain I would probably resist to the idea of the state introducing identity cards. Different perceptions of privacy are formulated within societies.

This variety of perceptions has a much more direct impact in the context of the Internet; it is one of the most significant factors that render on-line privacy a complex issue. The Internet has a trans-national nature, there are no physical borders in cyberspace; as a result it combines many cultures with different perceptions on basic issues. It is a 'space' where physical boundaries and traditional constraints of distance have disappeared, and different perceptions of privacy are met to mould a new one. In effect, cyberspace is developing a culture of its own, one that is still in the process of formulation.

To put things in perspective, though, it should be mentioned that the Internet was created and is still dominated by the western world. Furthermore, even though many governments like the US, UK and most European countries share the aspiration of making it the medium of the future, it is still an elite environment in the world-wide context, in a sense that only those who can afford a computer, a modem and a connection are using it as a part of their everyday activity. This percentage may be high (especially in the US and Europe), but it is not high enough to cover the majority of the population.[7] Having said that, it is not implied that a concept of on-line privacy is not emerging; the comment is simply made to show the background where this formation takes place and put things in the right perspective.

But let us turn to a more concrete approach. As already said, it will unfold through an explanation of traditional privacy and a brief encounter of the legal protection that it has been

---

[6] See V Bellotti, "Design for Privacy in Multimedia Computing and Communications Environments", in P E Agre and M Rotenberg (editors) *Technology and Privacy: The New Landscape* (1998) MIT Press, at p.67.

[7] According to Nua Surveys, the number of Internet users world-wide, as of February 2002, is 544.2 million. Of these 171.35 users are in Europe, 181.23 in Canada & USA, and 157.49 in Asia and Pacific. The rest 34.13 million are in Latin America, Africa and the Middle East. It is reminded that the total population of the globe is more than 6 billion. (available at <http://www.nua.ie/surveys/how_many_online > visited on 05/06/2002).

afforded by society, before carrying on to a detailed analysis of on-line privacy as such.

2.3 Understanding privacy

Privacy has been explained and defined in so many different ways that it has become very difficult to pick out the most effective one. A good way to begin is by comprehending that it comprises more than one 'aspect' or otherwise 'zone' of protection, that tend to fit with the various aspects of our everyday life and activities. Gavison proposed a tripartite view of the concept of privacy that remains a very helpful starting point.[8] According to her view, privacy encapsulates the notion of *inaccessibility* of an individual, in a sense that a person enjoys privacy when it is completely inaccessible to others. This inaccessibility extends to three aspects of one's life, that is: i) no-one has *physical* access to the person (not touches the person), ii) no-one pays any *attention* to the person (not sees, hears or senses the person), and iii) no-one possesses any *information* about the person (not knows about the person). Hogg proposed a further aspect to complete this concept of privacy: one that has to do with personal *property*.[9] According to his view, inaccessibility of personal property is also safeguarding privacy. But, as he suggests, the boundaries of this inaccessibility are more difficult to define. That is because not all access to property violates privacy, but only that which breaches the boundaries a person has decided to erect around his or her property, whether it is space or objects. It is not an invasion of privacy if someone handles or looks at property that is in public view or disposal. For example, entering a private property that is open to public view in order to be sold does not constitute an invasion into the proprietor's privacy. Nor would a friend, urged by us to enter our bedroom to view the new furniture, be considered as violating our privacy. The same conduct, however, would feel different for the proprietor if it lacked his explicit urging or consent.

The difference between the former three aspects and the latter, as it is being approached, is that the latter adds to the concept of privacy the element of *control*. According to this author's point of view, this element is present as a decisive factor not only in this last aspect of privacy in relation to personal property, but in all the other three as well. If *inaccessibility* were regarded as absolute it would automatically erase the sociability that is inherent in any individual. To be private in one's home does not mean to be absolutely inaccessible from

[8] R Gavison, "Privacy and the limits of the law", (1980) 89 *Yale Law Journal* 421.
[9] Hogg, supra, note 3, at p.3.

anyone outside the home, but to be able to *control* and *choose* who is going to have access and when. When a friend is coming over to pay a visit it is not an invasion of privacy, but if this friend decides to pay this visit in the middle of the night, using the key we have entrusted to him in case of an emergency, this would probably violate our privacy, except if we have explicitly given him the permission to do so. The same idea applies to inaccessibility in one's physical existence, or body. Privacy satisfies the need to control who has access to our body or our physical operations. It is not about keeping the body completely inaccessible but is about choosing how to dispose of it, who has access to it and in what way. If we do not recognise in privacy the element of control, any physical contact would seem to violate privacy, which is certainly not the case. Intimate relations between members of a family, friends or lovers are part of human nature. Control as an element of privacy may be easier to understand when it comes to information. The essence of privacy here is not about concealing all information about one's self, since a percentage of personal information such as one's age, sex or colour is anyway divulged by the mere participation in social life. It is about controlling how much information has been divulged and how it is going to be used. When we give data to our bank manager we do not consider our privacy compromised but we may do so if the bank manager uses the data in an unexpected way, and without our explicit consent.

To avoid any misunderstanding, though, it has to be clarified that this element of control is also not absolute. One does not have to exercise complete control over his accessibility in order to preserve privacy. Maintaining control does not mean that any access to our privacy spheres has to have pre-passed through the filter of our acceptability in order not to be considered as a violation of privacy. An uninvited friend or an unexpected cuddle is hardly an invasion of privacy; even the spread of a piece of news or information about us, like winning a prize or taking up a new job, is usually not an invasion of privacy, even if the spread goes beyond our control. It is very much a subjective matter and one that varies from case to case. And apart from that, *control* has more the sense of being able to exercise certain personal and pre-conceived limits, rather than being able to control everything. We could say that every person has a minimum private sphere, whose limits are decided by the person itself, within the boundaries of what society is ready to accept as being a private sphere (no exaggerating or irrational aspirations).

Another way to understand privacy is by dividing it into groups of *claims*. There is an

obvious overlap between this and the preceding approach, but it is still worthy of reference as it seems to contribute to a further understanding. Privacy claims tend to fall into three general categories:[10]

a) The first is *territorial* privacy claims that have traditionally been associated with the physical right to be left alone or undisturbed. Trespassers, loud noises or even environmental toxins are considered to minimise the control we have on our physical surroundings. Without being invited or given permission, no one should be allowed in our territory or proprietary space.

b) The second category of privacy claims relates to our *existence* as individual persons. This category of claims encompasses several diverse situations, but with one single idea behind them: the protection of an individual's perceived dignity and control over its own personality. Freedom of movement and expression, prohibitions against both physical assaults and harassment in a non-physical sense, restraints against unlawful searches or seizures, are all paradigms of privacy claims that fall under this category.

c) The third category encompasses claims that are also based on the idea of preserving the dignity and integrity of an individual, but they do not refer to physical invasions or to a direct assault upon a person. This category covers the claims of control over the disclosure, distribution, use and abuse of *information* about the person.

All three categories of claims have again a common denominator that is control. Whatever the space seeking protection either physical territory, personal integrity or information, the essence of privacy claims is again to ensure control over the disposition of this private space.

It should be clear by now that privacy can be loosely separated into broad categories: territorial, bodily or personal, and informational. But why do we need privacy? Why do we need this control over our private spheres? What are the values underneath privacy that seek protection? Privacy obviously serves a number of values, like our need for space and time to

[10] See J I Rosenbaum, "Privacy on the Internet: Whose Information is it Anyway?", (1998) 38 *Jurimetrics Journal* 565-573.

reflect, meditate and plan what we want to do.[11] It enables us to get away from our public and social roles and release feelings and emotions that cannot appropriately be expressed in our public life. It enables us to form and develop intimate friendships, sexual relations and family bonds. But that does not mean that *private* should be seen as a mere opposite to *public*. There is a bond of interconnection between private and public life. Without privacy an individual is unable to participate in social life in a healthy way. All these thoughts have to do with the relationship that privacy has with liberty, personal autonomy and dignity, a relationship that needs a clearer explanation in order to achieve a better understanding of privacy.

In its classic formulation as a right to be let alone, privacy comes closer than any other right to the essence of liberty itself.[12] Our sense of social liberty is partly defined by the ability to control our own lives, whether this be the kind of work we undertake, the kind of religious and political beliefs we hold, or the information we wish to divulge about ourselves. Some times it is indeed very difficult to distinguish between privacy and liberty because the former tends to merge with the latter:[13] the right to be let alone has very much the sense of being free to do whatever one wants. However, liberty is a much more general idea than privacy, a value that is interconnected with and is inherent in many other rights as well, such as the freedom of expression, the right to develop political intercourses, the freedom of religion and many more. Privacy and liberty can be easily confused; some times it is difficult to discern whether a situation is one where privacy or liberty is at stake. For example, an employer who controls what his employees do during the break is really invading their privacy, or is it rather their personal freedom that is at stake? According to this author's opinion, both privacy and liberty are at stake. As discussed before, inherent in the notion of privacy, is the element of control; a person should be free to choose the limits of his accessibility. And lunchtime is certainly a period where people would not want to be 'accessed' by their employer. In effect, both personal freedom and privacy can be invaded at the same time, since the former is a value inherent in the latter. However, this does not mean that privacy and liberty are so interconnected that whenever the former is at stake the latter is affected as well and *vice versa*. Liberty is involved with many more rights, and privacy is expressed through other values as well.

---

[11] See E Barendt, "Privacy as a Constitutional Right and Value", in P Birks (editor) *Privacy and Loyalty* (1997) Clarendon Press - Oxford, at p.6.
[12] See D Feldman, "Secrecy, Dignity, or Autonomy? Views of Privacy as a Civil Liberty", in *Current Legal Problems* 1994 – Volume 47, Part 2: Collected Papers, edited by M D A Freeman.
[13] See R Dworkin, *Taking Rights Seriously*, (London: Duckworth, 1977), pp. 266-78.

Another important value that is closely related to privacy is the idea of personal autonomy. Autonomy (in its Kantian form) involves a capacity for self-determination, and a willingness to act according to principles which one accepts as rational, and regards as appropriate to guide one's own and other people's behaviour. The autonomous person enjoys a certain level of moral and physical capacity, reflectiveness, and self-awareness (which presupposes access to a decent level of social and moral education, and perhaps also to health care and other facilities).[14] The notion of autonomy is tied to that of dignity. One aspect of dignity is self-respect, which includes respect for both one's own and other people's moral rights, and a commitment to our own personal standards. Dignity also encompasses a desire to be esteemed by others according to the standards we approve.[15] These attributes make it possible for people to regard their own choices as important, which is a necessary condition for the exercise of autonomy. Apart from dignity, autonomy is also closely related to the idea of liberty; being autonomous means *inter alia* being free to choose to think and act as one wants. The desire for a private area in life -both physically and mentally- is to a great extend rooted and justified to the notion of personal autonomy and dignity.[16] All three types of privacy claims (territorial, existence and information) are related to the need of a person to be autonomous in society and have the freedom to lead his life as one wants.

Yet, it needs to be pointed out that privacy may be autonomy and dignity-related, but so are many other civil liberties (such as freedom of expression, religion and conscience). Identifying those values does not suffice to explain the nature of the concept of privacy but simply helps to complete the picture. Privacy, being a liberty and autonomy-related right, is often said to be predominantly individualistic;[17] however, it is better conceptualised as part of a balance between the interests of individuals, groups and the state. A person needs privacy in order to develop his personality and participate healthily in society. We should not underestimate the importance of privacy to maintaining a functioning community; as Feldman said, privacy is socially valuable.[18] It is also important to understand that privacy is not independent of society. As an autonomy-related right it has both a negative and a positive

[14] D Feldman, *supra* note 12, at p.54.
[15] See T E Hill Jr, *Autonomy and Self-Respect* (Cambridge: Cambridge University Press, 1991), chapters 1 and 2.
[16] See D Feldman, *Civil Liberties and Human Rights in England and Wales* (Oxford University Press 2002), 2nd edition, chapter 9.
[17] See S Lukes, *Individualism* (Oxford: Basil Blackwell, 1973).
[18] See D Feldman, "Privacy-related Rights and their Social Value", in P Birks (editor), *Privacy and Loyalty* (Oxford: Calendon Press, 1997), pp. 16-28.

aspect: the negative aspect is freedom from intrusion, the right to be left alone which has been identified as the core sense of privacy;[19] but the positive aspect, which is more elusive and controversial, encompasses a duty of the state and other individuals to foster the conditions in which privacy can be enjoyed.[20] As said before, *private* is not a mere opposite to *public*; being private does not only mean being away from society, but also participate in society and develop a personality according to one's will and choices.

In the same context, it is also important to point out that it would be difficult, if not wrong, to place these rights and values in an absolute order. Whether privacy, liberty or autonomy are primary or secondary values compared to other rights may differ from case to case. For example, legislation compelling the wearing of seatbelts or crash helmets does affect individual autonomy, but the majority of people have accepted that it is in the public interest. On the contrary, a possible measure allowing employers to observe what their employees drink or eat during lunch in order to preserve productivity would affect personal freedom in a way unacceptable to most individuals. Which right prevails is usually a decision to be made *in concreto*.

To sum up, it is important to keep in mind that privacy encompasses but does not coincide with the values of liberty, autonomy and dignity. Liberty, autonomy and dignity are not independent rights by their selves, but moral values that are expressed and safeguarded through many rights and liberties. These values are interconnected between them (autonomy can be described *inter alia* as freedom of choice) and can be easily confused with privacy itself.

Let us continue with another issue. In order to have a better understanding of privacy it would also be helpful to comprehend its relation to geographical spaces. As we already saw, a considerable amount of the discussion about privacy is devoted to physical space, so associating privacy with places is a common misconception. But privacy is not about protecting spaces or places; it is about protecting people. People need and expect a percentage of privacy even when they find themselves in a public sphere. Of course they have a different expectation of privacy in a public rather than in a private place, but a zone of protection exists even in the former. As Feldman observed,[21] privacy in public spaces is less

[19] See W L Prosser, "Privacy" [1960] 48 *California Law Review* 383-423.
[20] See D Feldman, *supra* note 16, p. 515.
[21] See D Feldman, *supra* note 12, at p. 59.

extensive than in private spaces, because we cannot normally claim to control who shares the public space with us, and we acknowledge that we owe duties to fellow-users not to behave in ways which are gratuitously offensive to them. When we are walking on the street for example, we may expect and accept that other people are looking at us or that they hear what we say if we speak loud, but we would probably feel that our privacy was violated if someone was trying to overhear an intimate conversation that was simply taking place between two people in a public environment, like a café for example. A restaurant may well be a public place, but people dining there certainly do not expect to be monitored in their every word or movement. Another example is the workplace. People are of course aware that they are being monitored, either by their employer or colleagues, but there is still a limit beyond which there is a violation of privacy. For example, an employer may check the time we go to and come back from lunch but it would be an invasion of privacy if he wanted to control what we eat or what we read during our break or how many times we visit the toilet. The existence of privacy in public places has also been recognised by the courts. The US Supreme Court, for example, in a landmark case in 1967 accepted that a telephone conversation is private even when one of the persons is using a public telephone booth.[22] Overall, the level of privacy that a person enjoys in public may be lower but is still existent. Privacy is not absolutely defined by the borders of private and public places. This distinction will play an important role in the discussion below about on-line privacy, since the Internet is an environment where traditional perceptions of public and private places are significantly blurred.

To reach a conclusion, an all encompassing way to understand privacy is by dividing it into three types:[23] informational privacy, accessibility privacy (body and space) and, as DeCew has described it, expressive privacy. The first is about a person's ability to control the circulation of information relating to it, and the second about controlling who has physical or intellectual access to a person. The third is a more general category; it has to do with freedom from coercion and discrimination when making personal decisions. In other words, it encompasses the freedom and autonomy of the person. A key feature of expressive privacy seems to concern the free development of one's identity.[24] Informational privacy is by many

[22] *Katz v United States*, 1967, 389 US 347.
[23] See J DeCew, *In Pursuit of Privacy- Law, Ethics, and the Rise of Technology* (1997) Ithaca: Cornell University Press.
[24] See E A Mohammed, "An Examination of Surveillance Technology and their Implications for Privacy and Related Issues - The Philosophical Legal Perspective", (1999) 2 *Journal of Information*

considered to be the most profoundly affected or most dangerously threatened by recent developments in information technology, but this is an issue that will be discussed later in this chapter.

2.4 Legal protection afforded to privacy

It is one thing to talk about the concept of privacy as a situation, desire or claim, and another about privacy as a legal right. Privacy is not an absolute condition. Apart from the fact that each person can decide for itself how much privacy it needs, the amount of privacy that it is entitled to may also be limited by external factors. First and foremost, individual privacy comes in conflict with other people's rights and social needs. A person's home or correspondence, for example, may need to be searched in the process of investigating and prosecuting a crime, an action that satisfies the social need to fight and prevent crime. Information concerning the private life of a well-known individual, like a politician, may need to be revealed by the press, in order to serve the public's right to know when it comes to matters of public interest. There is an on-going conflict between freedom of expression and the privacy of public figures.[25] All these are controversial issues. Law becomes essential because it decides how much privacy a person is entitled to and how far this privacy can be limited in certain circumstances and in relation to other rights.

Privacy now enjoys a considerable level of legal recognition and protection around the world, both in national and international level. It is protected in various ways within national jurisdictions,[26] but for the needs of the present study it suffices to present a general picture of

---

Law and Technology (available at <http:/elj.warwick.ac.uk/jilt/99-2/mohammed.html>, last visited on 23/04/2002).

[25] See the recent case *Naomi Campbell v Mirror Group Newspapers Ltd* [2002] EWHC 499 (QB), where Naomi Campbell, a famous fashion model, won a case against a magazine that published pictures of her during her staying at a rehabilitation centre for alcoholics, which was latter overturned by the Court of Appeal, *Naomi Campbell v Mirror Group Newspapers Ltd* [2002] EWCA Civ 1373. Apart from this one, there is a series of cases in the UK (others decided by the court and other by the Press Complaints Commission) concerning the exposure of the private life of famous people in the press, like *JK Rowling v OK! Magazine* PCC 17/08/01(a famous writer who was cought by the lens enjoying vacation with her 8 year old daughter in Spain), *R(on the application of Anna Ford)v The Press complaints Commission* [2001] EWHC Admin 683, CO/1143/2001 (a BBC newsreader who was photographed at a public beach with her austronaut boyfriend), *Jamie Theakston v MGN Ltd* [2002] EWHC 137 (QB) (a tv presenter who tried to suppress an article about his visit to a brothel), *Gary Flitcroft v MGN Ltd* (2002) 2 All ER 545 (a married football player whose affair with a lap dancer and a nanny was revealed by the press).

[26] For a detailed analysis see M Henry, *International Privacy, Publicity & Personality Laws* (2001) Butterworths.

the way it is dealt with in legal documents of an intergovernmental nature (since they are usually the source for national laws), with specific reference only to the jurisdictions of the UK and US.

2.4.1 Protection at the international level

Privacy was recognised as a fundamental right for the first time in international level[27] by the *Universal Declaration of Human Rights*, a non-binding legal document signed in 1948 by the members of the United Nations. A fundamental right is one that may be waived or limited, under certain circumstances, as opposed to an absolute right that is inviolable.[28] This seems to be a correct approach, to begin with, since it fits with the nature of privacy and the element of choice, as described above. According to Article 12 of the Declaration: *"no one shall be subject to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour or reputation. Everyone has the right to the protection of the law against such interference or attacks"*. There is no further definition of the term privacy within the Declaration. However, apart from privacy, this Article refers to the protection of family, home, correspondence and honour or reputation. Even though these latter interests are not included in the Article as an explanation to the word privacy (but rather as values deserving protection on their own), the wording can be interpreted to assume that the drafters intended to cover more than one aspect of individual privacy. The actual effect of this document is limited, though, due to its nature as a non-binding commitment for the signatory states, a soft international law rather than a legally binding treaty.

This deficit was in a sense covered by the *International Covenant on Civil and Political Rights*, whose main objective was to reinforce the *Universal Declaration* by specific treaty law, legally binding for the contracting states.[29] The wording of Article 17 referring to privacy is almost identical to that of the Declaration: the only difference is the word *unlawful* added after the word *arbitrary* (*...no one shall be subject to arbitrary or unlawful interference...*). Both the Declaration and the Covenant provide for a considerable level of privacy protection and they attempt to define, although in general terms, the obligations of a

[27] I do not mean here that by the *Universal Declaration of Human Rights* privacy was recognised for the first time in history as a right, but that it was its first recognition of an inter-state nature. It was earlier recognised as a right within the jurisdiction of individual states (i.e. in 1890 in the US).
[28] See A Gauntlett, *Net Spies - Who's Watching you on the Web?* (1999) VISION Paperbacks.
[29] It came into effect in 1976, 129 states are parties to the Covenant.

state in relation to such protection. A state is supposed to provide laws to protect its inhabitants against invasions to their privacy. Although the preconditions of interfering with this right are not explicitly laid out, it is rather clear from the wording that interference can be allowed when it is explicitly permitted by law and it does not go beyond the limits of rational action. The use of both 'arbitrary' and 'unlawful' in the Covenant does not seem to be redundant, even though the opposite was argued during the drafting of the Covenant. According to this author's point of view, these words manage to cover all possible situations since they have two distinctive implications. Taking as an example the interpretation of the *European Convention of Human Rights* Article 8, (as will be later analysed), 'unlawful' can be interpreted to preclude invasions of privacy perpetrated by private entities as well as by governments, and can also be taken to impose an obligation on states to take positive steps to protect their inhabitants against such invasions; whereas 'arbitrary' may be constructed to include invasions of privacy that are committed within the law, for example when an abuse of administrative discretion is involved.[30] As a general comment it can be said that, even though the Covenant manages to recognise individual privacy to a considerable level, it is not completely sufficient due to its failure to provide for an independent enforcement and control mechanism.

Moving towards a more localised approach, another important legal document that recognised privacy as a definite right is the *European Convention of Human Rights and Fundamental Freedoms*,[31] signed in 1950 by a considerable number of European states. The ECHR is a binding legal document, in a sense that a contracting state is committed to abide by its rules once it encompasses it in its internal legislation. This procedure was almost automatic for most of the signatory states, due to the fact that their written constitutions were in compliance with the Convention. It is interesting to note that the UK, due to its lack of a written constitution, only recently proceeded to full internal implementation with the adoption of the Human Rights Act in 1998. The major strength of this Convention rests on the fact that it provides for an effective enforcement mechanism governed by independent institutions. The *European Court of Human Rights* is an independent institution vested with the power to adjudicate cases of infringement. Both states and individuals can file complaints against a state that has failed to respect its Convention obligations, after having exhausted the

[30] See also J Michael, *supra*, note 5, at p.20.
[31] Henceforth referred to as the ECHR.

available judicial means in front of national courts. The existence of the Court reinforces the ECHR in two ways: first, it makes sure that it is adequately implemented by the signatory states and second, it provides for a detailed and homogenous interpretation of the rights it protects.

The ECHR enshrines a slightly different kind of protection for privacy from the one provided for by the International Covenant. Article 8, par. 1, recognises that *"everyone has the right to respect for his private and family life, his home and his correspondence"*. It then goes on (by paragraph 2) to set out in detail the conditions under which privacy can be interfered with by public authorities. In order to be acceptable, any interference with privacy has to be necessary in a democratic society, explicitly regulated by law and designed to serve one of the particularly defined reasons, such as *inter alia* national security, public safety or the economic well-being of a country.[32] Although there is again no further definition of privacy, it can be said that it is quite apparent from the wording of Article 8 that it recognises several of its different aspects (private life, home, correspondence). In addition to that, the Court has chosen to interpret the first paragraph of Article 8 in a broad rather than a strict way, and it has accepted protection for a considerable number of cases that would not explicitly fall under one of the particular words used by the Convention. 'Correspondence,' for example, has been expanded to include more than its literal meaning (exchanging letters), such as telephone communications.[33] 'Private life,' apart from the traditional concepts of private space or sexual activities, has been also taken to include interests of personal identity, moral or physical integrity, and the collection and use of personal information.[34] It is also important to note that, besides the negative obligations not to interfere with privacy unless the conditions of paragraph 2 are met, the Court has accepted that there is also a positive obligation for states inherent in paragraph 1: a state is also required to take definite steps to provide privacy rights or privileges for individuals and to protect persons against activities of other private individuals which prevent the effective enjoyment of these rights. The source of these positive obligations is found in the language of Article 8(1): it protects the right *to*

[32] Article 8 paragraph 2 of the ECHR states that : "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 interest 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 freedom of others".

[33] For example in *Klass v. Germany* (1978), A28 para 41.

[34] See D J Harris, M O'Boyle and C Warbrick, *Law of the European Convention of Human Rights* (1995), Butterworths - London, pp. 305-311.

respect for each of the interests mentioned, not just the right to private life etc.[35] For example, in *Kroon v. Netherland*[36] the Court stated that the essential object of Article 8 was "...to protect the individual against arbitrary action by the public authorities. There may in addition be positive obligations inherent in 'effective' respect for family (and the other Article 8(1) values)".

A recent development in the arena of human rights protection in the European level is the creation of a *Charter of Fundamental Rights of the European Union*,[37] adopted by a solemn proclamation of the Commission, Council and European Parliament in the European Council of Nice on 7 December 2000. All member states of the EU are signatory parties to the ECHR, and the European Court of Justice has long since recognised respect for the fundamental rights protected by the member states' constitutions by regarding them as part of the general principles of Community law on the basis of Article 220 EC.[38] However, the lack of a specific catalogue of fundamental rights, which the EU institutions would have to respect, was felt as a gap that had to be filled.[39] In general terms, the Charter has the status of a non-binding 'soft-law' instrument in the Community legal order. The sated purpose, as eventually reflected in its preamble, was to strengthen the protection of fundamental rights in the EU, not by changing the rights as such, but by making them more visible to the EU citizens. The exact legal status of the Charter and the way it is going to be implemented are the subject of an on-going discussion, irrelevant for the needs of the present analysis. It suffices to say that, as long as it exists, it cannot be ignored by the institutions of the EU in the enforcement of Community law, but it still remains to be seen how things will turn out in practice.

Privacy in this Charter is recognised as a fundamental right protected under the title of 'freedoms'. Article 7 provides that "*everyone has the right to respect for his or her private and family life, home and communications*". Even though the explicit source of this article is Article 8 of the ECHR, there are two differences between them that worth a comment. First

[35] ibid., p. 302.
[36] Case *Kroon v. Netherlands*, A 297-C para 31 (1994).
[37] Henceforth referred to as the Charter or the Charter of Fundamental Rights.
[38] In the mid 1990's, the accession of the European Community to the ECHR as a legal person was under discussion. The European Court of Justice was asked whether that was possible, but it made clear (Opinion 2/94 [1996] ECR I-1759) that the European Community has no human rights competence, express or implied, on which specific measures can be taken. However, it said that the ECHR forms, in a way, part of the EC law because it initiates the general principles of law.
[39] See K Lenaerts and E E De Smijter, "A 'Bill of Rights' for the European Union", (2001) *Common Market Law Review* 273, pp. 276-77.

of all, the word 'correspondence' has been replaced by the more up to date 'communications', obviously to include all the forms of communication that have resulted from recent developments in technology, such as electronic mail or mobile telephony. Second, there is no second paragraph, similar to that of the ECHR Article 8, to lay out the conditions for interference by public authorities. However, the practical implications of this omission are minimal; by virtue of Article 52(3) of the Charter,[40] whatever the formulation of a right in the Charter, if it corresponds to a right guaranteed by the ECHR, the latter serves as a minimum in determining the meaning and scope of the right in question.[41] Apart from these differences, it is also worth noticing that the Charter recognises the protection of personal data as a separate fundamental right (in Article 8), whereas in the ECHR personal data are protected as part of the private life of an individual (following the Court's interpretation). Even though the protection of personal data is not new for the EU, since it emanates directly from the Data Protection Directive (95/46/EC),[42] in force in the EU since 1998, the protection of personal data as an explicit fundamental right is a very significant development not to be underestimated, since it is the first time it receives independent recognition in a human rights document.[43]

2.4.2 Legal protection for privacy in the US and UK

Let us now turn to a brief presentation of more specific approaches. There is still much debate about the coherence and scope of privacy protection in the United States. Even though the word privacy, and of course a right to it, is never explicitly mentioned in the American Constitution, some level of protection can be inferred from a number of constitutional guarantees that seem to create certain 'zones' of privacy. The First Amendment's privacy values of freedom of expression, association and religion, the Fourth Amendment's right to

[40] Article 52(3) reads as follows: "Insofar as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection".

[41] For an analysis on the issue see K Lenaerts and E E De Smijter, *supra* note 39, pp.290-8.

[42] This Directive will be analysed in more detail below in this chapter.

[43] This is a very significant development, since personal data are becoming all the more important in the European legal context. See for example the recent case in the UK *Naomi Campbell v MGN Ltd* [2002] EWHC 499 (QB), where Naomi Campbell was awarded by the High Court compensation against the "Mirror", a magazine that had published details of her attendance at a narcotics treatment programme. The case was decided on grounds of confidentiality and not a right to privacy as such, but still its outcome and importance remain intact. The ruling was later overturned by the Court of Appeal (*Naomi Campbell v MGN Ltd* [2002] EWCA Civ. 1373), due to the fact that the model had made untrue pronouncements about her private life.

be free from unwarranted searches and seizures, and the Fourteenth Amendment's concept of personal liberty, have been interpreted to provide for several forms of privacy protection within the Constitution. Additionally, almost a century ago the Courts recognised a privacy right in tort, principally against the publication by the media of embarrassing private facts.[44] In general, the US in federal level has chosen to deny a general protection for privacy and react with particular legislation every time that it considers it essential to respond to a perceived need or particular abuse. An example is the protection afforded to records with personal data; such protection can be found scattered in several laws. The first to be adopted was the Privacy Act of 1974, which sets out a comprehensive regime limiting the collection, use and dissemination of personal information held by government agencies. But legislation is not equally homogenous with regard to data handled by the private sector; it is rather scattered in several statutes like the Video Privacy Protection Act 1988 (protection of video rental records), or the Medical Privacy Act of 1997 (protection of medical records), or the Social Security Safeguards Act of 1997. An initial comment would suggest that this sectional approach and the lack of general principles leaves this aspect of privacy semi-regulated, since it fails to cover all possible invasions perpetrated by private entities (even though it manages to cover the governmental sector), and leaves a lot of loopholes that could easily be abused.[45] However, it needs to be noticed that this 'gap' in federal law is in several cases filled by legislation at US state level. For example, California state law provides for a coherent and comprehensive protection of privacy. First and foremost, the California State Constitution (Article 1, section 1) gives each citizen an alienable right to pursue and obtain privacy; apart from that, there are a considerable number of laws (most of them included in the state Civil and Penal Code) for the protection of privacy such as the Confidentiality of Medical Information Act, the Confidentiality of Social Security Numbers, the Destruction of Customer Records, the Identity Theft and many more.[46] Overall, even though there is an ascertained lack of coherent approach to privacy in federal level, this does not necessarily mean lack of comprehensive protection.

Privacy protection in the UK remains an interesting issue. The common law does not recognise a general right to privacy and the UK Parliament has long been unwilling to

[44] See L D Brandeis and S D Warren, *supra*, note 4.
[45] See R M Gellman, "Can Privacy be regulated effectively on a National Level? Thoughts on the Possible Need for International Privacy Rules", (1996) 41 *Vill. Law Review* 129, at p.131.
[46] See the list of laws at the California Office of Privacy Protection at <http://www.privacy.ca.gov/laws.htm>, (last visited on 08/04/2003)

introduce a broad statutory right. Several issues of privacy have been dealt with by the Courts, such as the right to be left alone, the right to communicate privately, the right to respect for private life and the role of privacy in preserving freedom of speech and access to public information; however, the potential broadness of the definition of privacy has been seen as a negative factor for the introduction of a general right.[47] The inability to express the concept of privacy in terms that are both adequately precise and sufficient has been a major constraint for the passage of any satisfactory legislation, even though a number of official inquiries and several Parliamentary Bills proposed by private members in the last thirty years[48] indicated a level of disquiet about the state of the law. Privacy has never been a fundamental and recognised right in English law, but the possible need for some sort of individual privacy has been discussed several times, as for example in the 1993 Consultation Paper of the Lord Chancellor's Department on Infringement of Privacy.[49] However, the rights that a general law of privacy would safeguard already come to a certain extent under the umbrella of some existing causes of action in English law or, otherwise, receive some measure of protection.[50] These causes of action include trespass, nuisance, harassment, breach of confidence, defamation and malicious falsehood.[51] It has to be pointed out, though, that this protection is much more limited than a recognition of a general right or freedom. A claim in tort in English law has to be based on some conduct of the defendant that infringes some right of the plaintiff, around which the law has thrown the cloak of a specific cause of action. This means that the plaintiff has to show that the defendant has committed some specific wrong against him, which entitles him to sue.[52] This limits substantially the circumstances where an individual is entitled to judicial protection for its privacy.

However, the situation is in a process of change since the full implementation of the ECHR

---

[47] See Report of the Committee on Privacy, Chairman Kenneth Younger, Cmnd. 5012, London: HMSO 1972, ch. 4.

[48] See R Clayton and H Tomlinson, *Privacy and Freedom of Expression* (2001), Oxford University Press, pp. 6-7.

[49] See Lord Chancellor's Department on Infringement of Privacy: Consultation Paper, July 1993, London: HMSO, para. 3.3 page 8. The potential need for individual privacy was also discussed by several other Committees. See Report of the Committee on Privacy, Chairman Kenneth Younger (*supra* note 37), Report of the Committee on Privacy and Related Matters, Chairman David Calcutt QC, 1990, Cmnd, 1102, London: HMSO, page 7, and the Government Response to the National Heritage Select Committee, Privacy and Media Intrusion, Cmnd. 2918, 1995, London: HMSO.

[50] See Sir B Neill, "Privacy: A Challenge for the Next Century", in B Markesinis *Protecting Privacy* (1999), Oxford University Press, p. 4.

[51] ibid., pp. 4-12.

[52] ibid., p.4.

into UK law on October 2000, by the Human Rights Act of 1998. Even though the Convention had been ratified by the UK since 1951, it took almost fifty years before it was fully implemented, partly due to concerns about its potential effect on common law. Prior to October 2000 it was merely a persuasive authority that could be used to clarify statute or common law in cases of ambiguity. Now, apart from the fact that any legislation has to comply with the Convention, the Courts as public bodies are also obliged to take it into account in their decision-making (s 6(1) of the Human Rights Act 1998), which is believed by many to allow for the development of a common law right to privacy.[53] In fact, a change of attitude by the Courts began to emerge soon after the Human Rights Act became fully effective in October 2000. The first English case where this change of attitude was observed is the decision of the Court of Appeal in *Douglas and others v Hello! Ltd.*[54] The case concerned the publication of unauthorised photographs of the wedding of Michael Douglas and Catherine Zeta-Jones by *Hello!* magazine. The celebrity couple had sold the exclusive rights to publish their wedding photographs to *OK!* magazine (the third claimant in the case). However, in spite of elaborate security arrangements, *Hello!* magazine obtained unofficial photographs, which it sought to publish right after the wedding. It was the publication of these photographs that the claimants sought to restrain by an injunction. The injunction was granted at the first instance, but the Court of Appeal discharged it on discretionary grounds. Even though the Court refused the injunctions sought to stop *Hello!* from publishing photographs of the celebrity wedding that it had acquired by questionable methods, Lord Justice Sedley said that the claimants had arguable claims for breach of their rights to privacy, despite the fact that they had sold the rights to photograph their wedding to *OK!* magazine. Recognising the fact that Courts now have to take into account Article 8 of the ECHR when interpreting common law, the court was faced with a dilemma: whether to recognise a tort of privacy or to stick with the traditional protection afforded by the tort of breach of confidence. Even though it opted for the latter, the court did not reject the former option in its entirety. It left, however, the matter to be decided at the final trial.[55] The court also gave some indication as to how Convention jurisprudence might be taken into account by the Courts in deciding issues of privacy and it briefly addressed the issue of 'horizontal effect' of Convention rights (rights between private persons, as opposed to the 'vertical' right

[53] Lord Irvine, Hansard House of Lords, 24 November 1997, Col 748.
[54] [2001] 2 All ER 289; [2001] FLR 982.
[55] See T A Baloch, "What Price for Privacy?", (2001) *New Law Journal* 50.

of a person against the state).[56] Whatever the result, the importance of this case is that privacy was for the first time confronted - even though not explicitly recognised - as a potential right. Quoting the words of Lord Justice Sedley:[57]

> "The Law recognises and will appropriately protect a right to privacy. ... A concept of privacy accords recognition to the fact that the law has to protect not only those people whose trust has been abused, but also those who simply find themselves subjected to unwanted intrusion into their personal lives. The law no longer needs to construct an artificial relationship of confidentiality between intruder and victim: it can recognise privacy itself as a legal principle drawn from the fundamental value of personal autonomy."

Since then a right of privacy in a sense of an equitable remedy for breach of confidence has been recognised, even in the absence of any pre-existing confidential relationship, in *Venables and another v News Group Newspapers*[58], *A v B plc*[59] and *Campbell v MGN Ltd.*[60] In the *Venables* Case injunctions were granted against the whole world to prevent the publication of confidential information, which might lead to the identification of two notorious child murderers, after their release from custody. It is worth noticing that in this case the Internet was very much involved, as a potential medium in which confidential information could be published from all over the world and reach the UK public. In *Campbell v MGN Ltd*, a case concerning the disclosure by articles published in *Mirror* that Naomi Campbell, a famous fashion model, had become addicted to drugs and was receiving therapy by Narcotics Anonymous, it is interesting to note that Lord Justice Phillips was certainly quite hesitant in recognising a right to privacy as such. As he said in his judgement:

> "The courts are in a process of identifying, on a case by case basis, the principles by which the law of confidentiality must accommodate the art 8 and the art 10 rights (of the ECHR). One principle, which has been recognised by the parties in this case, is that, when a public figure chooses to make untrue pronouncements about his or her private life, the press will normally be entitled to put the record straight."[61]

Even before the adoption of the Human Rights Act, the UK had enacted legislation covering a major aspect of privacy: the protection of personal information, as a matter of its EC obligations. The first Data Protection Act of 1984, enacted to comply with the Council of

---

[56] See M Elliott, "Privacy, Confidentiality and Horizontality: the Case of the Celebrity Wedding Photographs", (2001) 60/2 *The Cambridge Law Journal* 231.
[57] See paras 125/126 of *Douglas and others v Hello! Ltd* [2001] 2 All ER 289.
[58] [2001] 1 All ER 908, [2001] 2 WLR 1038.
[59] [2002] 2 All ER 545.
[60] [2002] EWCA Civ. 1373.
[61] Ibid., para. 43.

Europe 1981 *Convention of the Protection of Individuals with Regard to Automated Processing of Personal Data*, was recently replaced by the Data Protection Act of 1998 that was designed to implement the EU Data Protection Directive (95/46/EC), a legal document that provides for a considerable quality of privacy protection. The UK has also enacted specific laws regulating the interception of private communications, dealt with in due detail below (chapter 6).[62]

2.4.3 Data protection regulations

Since an effort is being made to present briefly the level of protection that privacy enjoys around the world, it would be an omission to leave out the existing legal protection afforded to one of the major aspects of privacy: informational. This aspect was considered by many as the first to be affected by the advent of information technology. Although the use and abuse of personal data is certainly not the sole issue of on-line privacy, it is still one seriously affected by specific legislative efforts, even though none of these efforts had on-line privacy as their only target.

In international circles, concerns about the potential effect of automated processing of data upon the right to privacy began to grow during the late 1960s and early 1970s. The reason why this specific aspect of privacy drew international attention was not a pure privacy concern. There was also an economic aspect in the flow of information between countries: national data protection laws could be used as non-tariff trade barriers between countries; in effect, the development of international standards would diminish potential hindrances.[63] The first effort was made by the OECD,[64] which adopted in 1980 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*,[65] worded in the language of recommendation rather than obligation. At about the same time, the Council of Europe adopted the *Convention for the Protection of Individuals with regard to Automatic*

[62] It has to be mentioned at this point that all the recent privacy cases dealt with by the UK courts, were decided on confidentiality grounds rather than privacy as such (see the cases brought by Naomi Campbell, Gary Flitcroft, Jamie Theakston). It seems that the courts still feel more comfortable to follow a well known route than to step on fresh grounds.
[63] See J Michael, *supra*, note 5, at p. 32.
[64] Organisation for Economic Co-operation and Development.
[65] Recommendations of Council Guidelines on the Protection of Privacy and Transborder flows of Personal Data, 1981 I.L.M. 422, O.E.C.D. Doc. No. C(80) 58 final.

Processing of Personal Data.[66] This was not meant to be a 'European' convention, in a sense that it was open for adherence and ratification by non-European countries. These two documents contain very similar principles for fair information practices, although the Guidelines are written in less specific terms. There are also differences, however. First of all the Convention is legally binding for countries that have ratified it, by requiring nations to establish domestic data protection legislation, while the Guidelines are not. Apart from that, while the Convention applies only to automated processing of personal data, the Guidelines are not so limited. Nevertheless, neither document offers specific details on practical application of the established standards and they contain very general provisions on enforcement.[67] In general terms, the Convention and the Guidelines try to make sure that personal data are obtained fairly and lawfully, are stored for specified and legitimate purposes and are not used in a way incompatible with those purposes, are accurate and kept up to date, and are preserved in a form which permits identification of the data subjects for no longer than is required for the designated purposes.

In 1995 the European Union concretised and strengthened these principles by adopting the Data Protection Directive (95/46/EC).[68] Member states were allowed a period of no more than three years to implement it by domestic legislation. This Directive has been characterised as one of the most sufficient and effective data protection laws in the world because, apart from the fact that it reinforces the existing principles of fair information practices, it provides for a very effective enforcement and control mechanism. An independent supervisory authority has to be established in each member state and vested with the power to supervise the observance of the principles by those who control or process personal data. Apart from that, it also prescribes that personal data may be transferred to countries outside the EU only if the country in question ensures an adequate level of protection, which is assessed according to the commands of the Directive. This is expected to cause problems because personal data are nowhere better protected than in the EU. The US

[66] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, February 1980, 1981 I.L.M. 377, Euro. T.S. No. 108 (Jan. 28, 1981).
[67] See R Gellman, "Conflict and Overlap in Privacy Regulation: National. International, and Private", in B Kahin and C Nesson (editors) *Borders in Cyberspace - Information Policy and the Global Information Infrastructure* (1997), MIT Press, at p. 265.
[68] Directive 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 Communities, 95/C 93/02, April 13, 1995. (Final text: July 17, 1995).

for example does not have a concise legislation regulating the handling of personal data.[69] The situation is even more problematic when it comes to the Internet, an area where is very difficult to carry out any kind of control on the trans-border flow of information. Take the US for example: while the protection of private data held by public authorities has to comply with the Fair Information Practices Act, a self-regulating approach still applies on the protection of data held by the private sector. It is debatable whether self-regulation is able to meet the standards of the Directive since it does not have to comply with any specific principles and does not provide for a formal control mechanism.[70]

However, which of the two approaches (EU or US) ensures better protection for individual privacy is a different question altogether. Research conducted during 2000 by an independent organisation (Consumers International) concluded that, despite tight EU legislation, sites within the EU are no better at providing decent information to their customers on privacy policies than sites based in the US. Indeed some of the best privacy policies were found on US sites. The overall conclusion of the research was that Internet sites selling products to consumers fall woefully short of international standards on data protection in both sides of the Atlantic.[71]

Even though the contribution of data protection legislative efforts to the overall privacy protection is well recognised, there are still certain problems associated with the core principles of existing laws. Basically, they tend to allow many privacy violations to occur through exemptions for law enforcement, for example, or taxation purposes. Additionally, they do almost nothing to prevent or limit the collection of information as such.[72] Once information enters a database, the ability of the data subject to apply any kind of control is significantly minimised. As Froomkin observed, the easiest way to control databases is to

---

[69] See H H Perritt, Jr and M G Stewart, "False Alarm?", (available at <http://www.law.indiana.edu/fclj/pubs/v51/no3/stemac7.PDF>, last visited on 23/04/2002).

[70] See Testimony of Marc Rotenberg, Executive Director of the Electronic Privacy Information Centre, "Hearing on Privacy in the Commercial World" March 2001, (available at <http://www.epic.org/privacy/testimony_0301.html>, last visited on 23/04/2002).

[71] "Privacy@net: An international comparative study of consumer privacy on the Internet", a survey prepared by Consumers International (CI), (available at http://www.consumersinternational.org/news/pressreleases/fprivreport.pdf last visited on 23/04/2002).

[72] See S G Davies, "Re-Engineering the Right to Privacy: How Privacy has been transformed from a Right to a Commodity", in P A Agre and M Rotenberg (editors) *Technology and Privacy: The New Landscape* (1997), MIT Press, at p. 156.

keep information to oneself: if information never gets collected in the first place, database issues need never arise.[73] Especially when it comes to new technologies, a Dutch privacy expert commented that privacy legislation corrects mistakes and misuses but does not attack the way in which technology is used. On the contrary, experiences with data protection law in several countries show that these laws tend to legalise existing practices rather than protect privacy itself.[74]

These comments bring us back to the initial speculation. It is obvious that privacy enjoys an overall considerable level of protection, which is certainly not the same for all aspects of privacy and in every jurisdiction. The on-line environment is, no doubt, very different from everything we have known until now. Are the existing legislative approaches to privacy adequate to cover the new concerns and challenges posed by information technology? It is difficult to give an effective answer to this question without examining the nature of on-line privacy, and the degree to which it is similar or different from traditional privacy. The only thing that can be said with certainty is that nowhere is on-line privacy defined – much less protected - by law as such.

2.5 Privacy in the on-line environment

It is almost a cliché in contemporary literature that advances in information technology have a great impact on individual privacy, by introducing new threats and revealing new vulnerabilities for Internet users. Most of the analysis, however, seems to be based on the assumption that on-line privacy functions in the same way as its off-line counterpart. Even if that is eventually the case, there are still important differences that ought to be made out. Before engaging in a detailed analysis of this impact, it is worthwhile making two remarks that could enhance understanding.

First of all, the Internet has no physical existence whatsoever. Although we usually refer to it as a 'space' or new 'environment', it is important to keep in mind that it lacks traditional characteristics of a physical place. Even though the concept of traditional privacy is not exclusively affected by physical existence, much of our understanding is directly connected with physical environment and material objects. We tend to visualise privacy as a situation of

[73] See A M Froomkin, "The Death of Privacy?", (2000) 52/5 *Stanford Law Review* 1461, p. 1464.
[74] See J Holvast, "Vulnerability of information society", in R Clarke and J Cameron (editors) *Managing Information Technology's Organisational Impact* (1991), North-Holland.

the physical world; being in solitude and away from public view is probably one of the first pictures connected with the idea of privacy. The lack of such physical existence is an important feature in realising the differences between on-line and off-line privacy. Being in front of a computer monitor, for example, feels much more private than it turns out to be; people, as a result, tend to be much less aware of public view than in the physical environment.

Second, the interests protected by privacy, the underlying values that are inherent in privacy, remain the same. Even though cyberspace is a virtual world, in the sense that people experience it with their minds rather than with their bodies, the activities conducted there by individuals are no less real than those conducted in the real world. That is because cyberspace is practically not another world, but an extension of the existing one. It is a space where real people engage in activities that have a very material impact in the off-line world: people communicate, exchange views, buy and sell products, transfer money with a very real value, provide or receive services, entertain or educate themselves and many more.[75] To quote an example, the result of buying a book from an on-line store is not much different than buying it from a store next door: a transaction will be effected between the seller and the buyer and a hard copy will end up in the hands of the latter. As a considerable percentage of everyday activities moves towards cyberspace, the importance of on-line privacy becomes more and more apparent. Irrespective of the environment where one finds oneself, the interests protected by privacy, the underlying values such as freedom, autonomy, dignity and self-determination, remain immutable. This of course also means that on-line privacy is not an absolute right in a sense that it may be waived when more important rights or issues are at stake, as for example the public interest. As we saw above (page 17), legislation compelling the wearing of seatbelts may affect autonomy, but the majority of people accept it is in the public interest. In the same way, legislation allowing law enforcement agencies to retrieve on-line communications during criminal investigations may affect on-line privacy, but it is also accepted that it serves the public good.

Not many efforts have been made up to present to define and analyse the nature of on-line

[75] It has to be pointed out that this approach is not absolute. There are a number of on-line activities that do not have an extension in the real world, as for example the participation in on-line games of virtual reality with a fake identity. The focus of this analysis, however, is concerns of privacy for the common user, who uses the Internet and information technology as a medium for usual everyday activity.

privacy. Lessig,[76] working from the definition of Katsh[77] who sees privacy as the power to control what others can come to know about you, begins his approach by observing that people can gain knowledge about you either by monitoring or by searching. There is a part in everyone's life that is monitored and a part that can be searched. The former is that part of one's daily existence that others can see or notice, and the latter that part that leaves or is a record that can be searched. According to Lessig's approach, traditional constraints on others' ability to monitor and search may change as we move from real world to cyberspace. Monitoring can be more unobtrusive and searching more effective, since on-line behaviour leaves a lot of traces behind for those who know how and have the means to search it. This is a key element to understand on-line privacy. It is true that a lot of things change as we move towards cyberspace; traditional assumptions are refuted and new abilities and possibilities play a significant role for privacy. Let us analyse these changes in two major areas, where an impact on privacy is very much apparent: communications and personal information.

2.5.1 Electronic communications

One of the most popular and common uses of the Internet is that of a communication medium. Email is gradually superseding traditional means of communication and correspondence, like letters, fax, and even telephone in certain cases, apparently due to its unequalled capability for direct and fast transmission of messages, large amounts of data, and picture or sound files. Although electronic mail was initially considered as the digital equivalent of postal mail, this analogy seems to be gradually vanishing. The most substantive difference between conventional and email rests more on the way it is perceived by users rather than on technical details. People use it almost as they use the telephone; the content of email messages is like the content of an ordinary telephone call, unplanned, unthinking, the ordinary chatter between friends.[78] It has become a much more elaborate and even formal procedure to write a letter than to send an email. But apart from that, email has also replaced a considerable percentage of professional correspondence due to the capabilities it offers for instantaneous and fairly cheap transmission of anything that can be put in a digital form.

Despite apparent similarities with other means of communication, however, electronic messaging has a unique nature, distinctive of both telephone communications and postage

[76] See L Lessig, *Code and other laws of cyberspace* (1999), Basic Books, chapter 11.
[77] See M E Katsh, *Law in a Digital World* (1995), New York: Oxford University Press.
[78] See Lawrence Lessig, *supra*, note 76, at p.145.

mail; one that significantly affects traditional assumptions of privacy. Comparing it with conventional letters first, one realises that, unlike them, it has no physical existence: an electronic message is neither written on paper nor sealed in an envelope.[79] Email loses the uniqueness of a letter; it exists in multiple copies as it travels from the sender's to the recipient's computer. Controlling all these copies is a very difficult, if not impossible, task. Apart from the fact that the computer automatically keeps a record of all the messages sent and received, Internet service providers and network administrators who control the distribution of email messages usually keep copies for several purposes. So, the mere 'deletion' of a message that was sent or received is not enough to control its dissemination. If there were analogy with physical mail, it would mean that the post office would be authorised to keep a copy of each message handled at each point where the message was transferred, plus permanent official copies in the send and recipient points.[80] Apart from that, email messages lack the protection that was traditionally afforded to letters by the mere existence of an envelope. Society has recognised that the physical existence of envelopes expresses a choice for privacy that requires respect. Its weakness as a means of protection was never considered as a source of doubt about the strength of its implications.[81] This explicit protection does not exist for electronic correspondence. It is often said that email messages travel in cyberspace like postcards travel in the real world.

As for its resemblance with telephone communications, although the content of electronic communications is often similar to the conversations conducted on the phone, there is a substantive difference between them. While no record of a telephone conversation is kept by default, with email the content of a communication is automatically saved, which means that it can be monitored, archived and searched quite easily. It is of course possible to keep a record of a telephone conversation but this is certainly not done automatically; it entails special planning and effort, that is usually time - and money - consuming. These physical constraints, that operated as a safety valve up to now, seem to have vanished in the on-line environment. In the professional environment, for example, it has never been cost-effective to intercept all communications of the employees in order to enhance and control productivity.

---

[79] See M H Barrera and J M Okai, "Digital Correspondence: Recreating Privacy Paradigms", (1999) *International Journal of Communications Law and Policy*, Issue 3 (available at <http://www.digital-law.net/IJCLP/3_1999/pdf/ijclp_webdoc_4_3_1999.pdf>, last visited on 23/04/2002).

[80] ibid., p.6.

[81] ibid., p.3.

The advent of electronic communication has made this possible. It is not accidental that the professional environment was one of the first spheres where electronic surveillance was applied.[82]

A general comment on the above comparison would suggest that communications conducted on-line are much more vulnerable in terms of privacy protection than those conducted with more traditional media. Email messages are by their very nature already in a form that machines can utilise and analyse, so the widespread use of email enhances the electronic systems of mass surveillance by reducing the difficulties of conducting it.[83] The use of email is transforming the nature of private communications by rendering them more easily monitorable and searchable. Apart from that, it has become very difficult to know, and even more to control, who may gain access to such communication.

Strangely enough, the actual use of electronic communication does not seem to be inhibited by this assumption. Electronic mail has become too convenient to avoid. And besides that, the vulnerabilities discussed became apparent only after the use of electronic communications had already become widespread. Even now, a lot of users seem to be unaware of the dangers inherent in using email, or they simply seem to 'forget' them in the name of convenience. But does this mean that users are or should be entitled to less privacy? Courts in the US[84] have exploited the knowing exposure and the assumption of risk rationales to deny an expectation of privacy in electronic information voluntarily exposed on-line, such as email or Internet postings. This argument analogises email to postal mail and holds that the sender assumes the risk that the recipient may reveal the content of the message, as he considers appropriate.[85] In other words, in the Internet environment, as longs as the sender is aware that his message will pass through several 'in-between' recipients (who can probably keep a copy) in order to reach its final destination, he can be taken to have agreed that his message is in the disposition of anyone who received a copy as part of this procedure. Even though rational, the application of this argument may prove very dangerous

---

[82] See A Rogers, "You Got Mail but Your Employer Does Too: Electronic Communication and Privacy in the 21st Century", (2000) 5.1 *Journal of Technology Law and Policy* 1 (available at <http://grove.ufl.edu/~techlaw/vol5/emailfinal.htm>, last visited on 23/04/2002).
[83] See A Gauntlett, *supra*, note 28, at p.52.
[84] See for example U.S. Supreme Court Case *Katz v. United States*, 389 U.S. 347 (1967), 351-52.
[85] See G Skok, "Establishing a Legitimate Expectation of Privacy in Clickstream Data", (2000) 6 *Michigan Telecommunications Technology Law Review* (available at <http://www.mttlr.org/volsix/skok.html>, last visited on 23/04/2002).

in the context of electronic mail. An electronic message sent by a user is first received by a service provider or a system administrator, who then redirects it to the intended recipient. Furthermore, the same message will probably pass through several other junctions before reaching its final destination. The fact that a common user is aware of this procedure does not mean, however, that one has surrendered any expectation of privacy for his communication and accepted that the content of the message is in the disposition of anyone who may have obtained a copy. Evidently, the privacy of on-line communications seems to be in a greater jeopardy than that of conventional communications, which is a combined result of the technology involved and arbitrary human assumptions. And still, there is no evident reason why on-line communications deserve less privacy than their off-line counterpart. It is obvious that the concept of reasonable expectation has a serious role to play in deciding how far on-line privacy deserves protection. But let us see how another aspect of privacy is affected in the on-line environment, before turning to that issue.

2.5.2 Private information

Informational privacy, as discussed at the beginning of this chapter, is one of the aspects of privacy. It is the right to control personal information, who gains access to them and how they are being used. Galkin (1996)[86] has observed that most private information has no value if retained by the individual, and only acquires a negative one if released to others. He seems to suggest that the only reason a person wants to maintain control on his personal data is to prevent it acquiring a negative, damaging value if released to the public. The value of personal information, as opposed to privacy itself, is either zero or a negative value. Maybe this is one of the reasons why the area of informational privacy is said to be narrower.[87] Informational privacy, however, also has a possible extended meaning: everything 'known' or held about a person can be seen as information, from pictures to communications or stored data etc. If we accept this meaning, informational privacy automatically acquires a positive value. Although these are interesting comments for a general discussion on informational privacy, they certainly do not seriously affect this discussion. Whatever the theory one accepts, the value of informational privacy for the preservation of dignity and autonomy remains the same. Informational privacy is considered as the aspect most directly affected by the use of the Internet and information technology, basically because it is more prone to

[86] See W S Galkin, "Privacy issues in the Digital Age", (1996) 29(5) *Maryland Bar Journal* 46-51.
[87] See J Michael, *supra*, note 5, at p.3.

compromise when people go on-line.

Private information on the Internet can be gathered in various ways and by many parties. There are several different categorisations for personal data collected on-line depending, for example, on who is the gatherer (governmental authorities or private parties), or on what is the scope for their collection (marketing, transactional, or simply statistical purposes). The categorisation followed here is one depended on the nature of the information itself. Private data gathered on-line can be roughly divided in three categories, although the distinction is easily blurred and there is often an overlap between them. The first category includes personal data or personally identifying information, the second traffic or transactional data and the third clickstream data. Each category has a distinctive value both for the data subject and the data collector and controller.

Personal identifiable information

The category of personal identifiable information includes data such as the user's name, address, telephone number or email address, marital or economic status, health details, employment, colour, preferences, credit or debit card number and even national insurance number. Such data are usually revealed voluntarily by a person 'moving round' in the on-line environment. Users are asked to reveal a considerable amount of personal information in order to engage in most of the usual on-line activities, as for example when registering with a service provider, when purchasing goods or services, or when subscribing in chatrooms, newsgroups or on-line periodicals. It is of course necessary to reveal one's name, address and credit card details in order to purchase a tangible product on-line, but further details such as marital status or employment are certainly irrelevant. Besides that, it seems that not only sites which sell a product or provide a service ask for such details; many Internet sites request personal information from their visitors simply to allow them navigate through their contents or to use the site in its full extent. This information gathering may vary from simple questions on their preferences to questions on their actual name, economic status and contact details. All these data are of course revealed voluntarily, but this does not diminish the negative value they can acquire if misused by those who handle them. Anyway users do not often have an actual choice, since revealing information is compulsory in order to enjoy the services. Even the argument that, even so, users may simply opt not to use the service, has a severe flaw. It fails to take into account the fact that the average user is most of the time ready to exchange personal information for the full use of a site that is already at his disposal, and is

unaware of how this information is going to be used or the risks of it being mistreated. Additionally, the value attributed to a single item of information by its subject is much less than the value it acquires when put in a collective database.[88] People tend to trade off their privacy for much less than its real value in the market: a database of names and addresses of ski-lovers, for example, may be sold for a lot of money and be used to increase profits of a company by directed marketing; the subjects, however, may have given away their personal details for a concession in the price of a ski-suit, or, even worse, for viewing some pictures of the ski resorts in the Alps. Using the Internet to read the news, search for information, purchase certain products or services and many more activities, are too convenient to avoid once there. And if the price to be paid for enjoying this convenience is the loss of an amount of privacy, more users are certainly willing to pay it. Of course, this is an 'informed' choice in a sense that people give away personal information knowingly; it is doubtful, however, that the average user is aware of the exact consequences that this is going to have for his privacy.

This information gathering is of course not completely new; files were kept on individuals even before the advent of information technology. The difference is that now filing has become easier to achieve but more difficult to control. Until recently, the massive amount of data stored on individuals on various private and public networks has been kept separate, and this dispersal of data has afforded some protection of privacy. With the advent of the Internet these networks have been brought together. Modern database management systems are able to access seamlessly many of these widely dispersed databases making the entire web appear as one huge, central databank. Protection of data by dispersal is no longer an adequate safeguard.[89] Computers have made it possible to match the dispersed data, which eliminates the individual's ability to control their dissemination. Apart from potential misuses, the proliferation of information facilitates error, which can have a devastating effect for privacy.[90]

---

[88] See A M Froomkin, *supra* note 73, pp. 1502-3.
[89] See A Gauntlett, *supra*, note 28, at p.20.
[90] See S M Thompson, "The Digital Explosion comes with a Cost: The Loss of Privacy", (1999) 4 *Journal of Technology Law & Policy* 3 (available at <http://journal.law.ufl.edu/~techlaw/4/Thompson.html>, last visited on 23/04/2002).

'Transactional' data

The second category of personal information that can be gathered from an individual's on-line activity includes the so-called 'transactional' or 'traffic' data The major difference between the previous and this category is that the former includes information that is voluntarily revealed by the data subject (in a sense that it requires a positive action from the user in order for the information to be collected), while the latter comprises information that is usually collected independently of the subject's express volition or concrete knowledge. To make things clearer, the terms 'transactional' or 'traffic' data refer to the transactional records that are kept from an on-line activity. It can be, for example, a catalogue with the transactional details of the electronic messages sent and received by a user during a certain period of time (meaning, for example, the date, time and address of the sender and recipient), a detailed record of how many times and for how long a person was on-line, a record of on-line bank or credit card transactions or the goods and services purchased using the Internet, or even a full record of the web sites a person has visited. Such information is routinely gathered by Internet service providers for billing purposes, such as telephone companies keep detailed transactional records of the telephones made by their subscribers. Users are not particularly asked to reveal such information since the collection is usually done automatically, without requiring any special action from the users. Detailed transactional records are also kept by many, mostly commercial, web sites for several purposes, such as advertisement or business planning. Although apparently innocent, traffic data can reveal many personal details for an individual's behaviour, especially when they are combined with databases containing personal identifiable information. Users, however, have complete lack of control over the use of such data, since it is very difficult to know when, by whom and what exact information is being gathered, and how long it is kept. The gathering of transactional data is not a novel phenomenon; telephone companies, for example, have always kept records of traffic data, and many commercial stores have been gathering information on their clients by offering something in exchange, such as a royalty card or a voucher for future buys. The Internet, however, has opened new possibilities. Since, for example, all on-line purchases are done by the use of credit or debit cards, an on-line store can keep a detailed record of all purchases very easily, while conventional stores may find it difficult to do so without discomforting their clients by asking too many questions at the cash point.

'Clickstream' data

The second categoty is often blurred with the third category of personal information that can be gathered from on-line activity, the so-called 'clickstream data'. Although similar in many ways, clickstream data have a distinctive nature. The word clickstream refers to the series of mouse clicks users make as they travel on the web. A clickstream is the aggregation of electronic information generated as a user communicates with other computers and networks over the Internet.[91] Each click can be translated to a certain on-line action, so a record of clickstreams can be shockingly revealing, providing a record of a person's entire on-line experience. Clickstreams can reveal not only what sites were visited by a user, but also for how long, in what order and how often a page was revisited, or which links were followed from each site. A whole on-line experience can be recreated, such as for example a search, which reveals much more substantive information on a person's habits, preferences, condition, health or character, than transactional data or simple personal information. Clickstream data can be successfully analogised to library records, although they are more than simply revealing the titles of the books read by a patron. If the analogy were absolutely accurate, it would be like also knowing when exactly the books were read, how long was spent in reading each one and each page, and the sequence in which the books or their pages were read.[92] Much of such data collection is taking place without the users' knowledge or consent and is mainly used by private entities for targeted advertising. This is achieved by the use of 'cookies'. Roughly described, a cookie is data that are placed with the use of software on a consumer's hard disc; in that way the movements of the user in cyberspace can be monitored and reported back to the party that installed the cookie. Many sites use cookies without their visitors' informed knowledge or consent. Those who inform users do not usually ask for their explicit consent, and even if they do, in general it has the form of an opt out rather than an opt in choice.[93] A user can of course set his browser to deny the installation of cookies, but that presupposes familiarisation with web-site habits and above average technical knowledge, elements that most users do not possess.

The collection of clickstream data seems to cross the narrow limits of informational privacy (according to the view of Galkin) since it is not merely about personal information but also

[91] See G Skok, *supra*, note 85.
[92] ibid., p.6.
[93] See Consumers International Survey, *supra* note 71.

about personal behaviour. An individual's conduct is monitored and recorded in considerable detail. As this monitoring is perpetrated by machines, it overcomes traditional weaknesses that are related with human nature, such as a faulty memory or power of observation and subjectivity.

Even though none of these three categories constitutes an entirely new kind of personal information, the advent of information technology and the Internet has changed the way they can affect our privacy. Schauer[94] has observed that the Internet poses new challenges for informational privacy in two major ways: in terms of *quantity* and *quality*. The Internet has made access to numerous databases far easier than it was previously, and this ease of access, combined with increased computer usage within the population, has expanded in terms of magnitude the actual access to numerous databases and the communication of the information they contain. But the problem is not a lesser one just because it is one of magnitude. The degree of accessibility is substantially affecting the ways this information can be used or manipulated, by opening new possibilities. Apart from that, information technology has a qualitative impact on informational privacy by creating the ability to do things that would not have been possible before and in an easier and faster way. Techniques of data mining and on-line profiling[95] allow the use of gathered information in much more creative ways.

As a counter-argument to that, it is often said that the amount of information available has become so vast that it is very difficult, if not impossible, to handle and manipulate in a productive way. In addition, many people think that nobody would care to search and use all the information about them that is dispersed in various places, at least not in a way that it would expose them or invade their privacy. But things change once a person becomes the target of a public 'dispute'. There are tremendous possibilities that, if exploited, can cause serious damage to an individual's privacy. Some time ago, a television documentary on the issue of on-line privacy presented a very interesting interview with Monica Lewinsky, who described how, after the incidents that attracted public attention on her person, the information that was dispersed about her on the Internet was easily gathered to compile a

[94] See F Schauer, "Internet Privacy and the Public-Private Distinction", (1998) 38 *Jurimetrics Journal* 555-564.

[95] For on-line profiling see A Shen, on behalf of the Electronic Privacy Information Centre (EPIC), "On-line Profiling Project - Comment", *P994809 / Docket No. 990811219-9219-01* (available at

database readily used by anyone interested. And there were certainly a lot. This compilation included anything, from electronic messages sent to chatrooms or newsgroups to catalogues of her shopping preferences. If you type the word 'Monica Lewinsky' in a search engine, like Google for example, the result is more than 134.000 web pages. This case is of course the exception rather than the rule (most people will probably never find themselves in a similar situation); it reveals, however, the tremendous possibilities opened by the way our informational privacy is exposed on the Internet.

Although individual behaviour has not been considerably affected by the use of computers and the Internet (people still buy products, transfer money, read newspapers and so on), the way in which this behaviour can be monitored has changed dramatically. It seems like the zone of privacy is being jeopardised as people move to cyberspace. But are these changes affecting the nature of privacy itself? Should people be entitled to less privacy when they go on-line just because they know or should be aware of what to expect? In fact, the majority of users do not really know many things about the installation of cookies in their hardware, but they do know how to fill a form with their personal data, even though they do not really think about the consequences. How all these affect the nature of on-line privacy?

2.5.3 Factors affecting the nature of on-line privacy

Subjective and objective expectation

Expectation of privacy seems to play a significant role in deciding how far privacy deserves protection. The US Supreme Court, in the landmark *Katz Case*[96] (1967), developed a two-stage test to decide whether there is a legitimate expectation of privacy, a necessary precondition in order to accept protection in terms of the Fourth Amendment of the American Constitution. Although the present discussion is not about testing the implementation of the American Constitution in relation to on-line privacy, the test developed by the Supreme Court is indicative of how subjective feelings and objective conditions interact in order to formulate a legal right to privacy by deciding the level of reasonable expectation. In particular, in order to have a legitimate expectation of privacy, a) a person must exhibit an actual expectation of privacy and b) this expectation must be one that society is prepared to

<http://www.epic.org/privacy/internet/profiling_reply_comment.PDF>, last visited on 23/04/2002).

[96] *Katz v United States*, 389 US 347 (1967).

recognise. This test examines two distinctive elements of the expectation, a subjective and an objective one. In order to deserve legal protection, not only does a person have to exhibit a subjective expectation of privacy but also this expectation has to be one that society is ready to accept in terms of reasonableness. The concept of 'reasonable expectation' is not an exclusive characteristic of the American Constitution; it seems to play an equally important role in several privacy protection rules. For example, in the Code of Practice of the Press Complaints Commission in the UK, the rules on privacy contain a note explaining that private places are considered those (either public or private property) where there is a 'reasonable expectation of privacy'.[97] Expectation of privacy seems to be a starting point for affording protection. Let us, therefore, see how the subjective and objective factors unfold in the on-line environment and affect the nature of on-line privacy.

It is well accepted that people have different expectations of privacy, depending on whether they find themselves in a private or public place. It is important to keep in mind that the distinction between private and public spaces does not coincide with the distinction between private and public property. Private property may well be a public space, like a shopping centre for example; whereas public property usually coincides with a public place. But even then, there is a limited private space often acknowledged to surround an individual, as previously explained (page 17). Is cyberspace a public or a private place?

There are several spheres in cyberspace that seem to resemble private places, like the private network of a company for example. However, the general reaction would be that cyberspace overall has more similarities to a public than a private space. In terms of property, rather than an area belonging to the public, the Internet is better described as an aggregation of privately

[97] Code of Practice, Press Complaints Commission (PCC), November 1997. "3. Privacy : (i) everyone is entitled to respect for his or her private and family life, home, health and correspondence. A publication will be expected to justify intrusions into any individual's private life without concent; (ii) The use of long lens photography to take pictures of people in private places without their concent is unacceptable. Note -- Private places are public or public property where there is a reasonable expectation of privacy." The PCC have indicated that whether the expectation is reasonable or not is not only an objective judgement, but is a decision affected by several factors. In two aparently similar cases it gave different decisions due to a slight difference that had to do with this expectation. Anna Ford and JK Rowling both compalint for the publication of pictures showing them enjoying their vacation. The PCC upheld JK Rowling's complaint, while it rejected that of Anna Ford, due to the fact that the former was appearing at the pictures with her 8 years old daughter. The PCC seems to be more sensitive when the children of famous people are involved in privacy cases. Apparently, the PCC wanted to say that there is no reasonable expectation of privacy in a public beach, but when a child is involved it seems that this expectation becomes wider. See *JK Rowling v OK! Magazine* PCC

owned digital spaces that are open to public access. But this does not make it less of a public space. An Internet store, a newsgroup or a chatroom, for example, are as public as their real-world equivalents of a shopping centre or a coffee shop. We already saw that people expect and are entitled to a degree of privacy even when they move in public spheres. The fact, for example, that a conversation between two friends is taking place in a park or a restaurant does not mean that everyone is entitled to listen to it, that is of course as long as they keep the volume in a low level. People in stores may expect to be noticed and served but they certainly do not expect all their moves or buys to be systematically monitored and kept in a record under their name. Or the fact that a person is using a public telephone does not mean that its conversation is not private.

However, traditional assumptions change as we move to cyberspace; established perceptions of public and private places are significantly blurred. Things in real-world public places may be unnoticed or quickly forgotten, while on-line almost everything can and is frequently being monitored and systematically recorded. But this fact is not equally reflected in the subjective perception of the on-line environment. The Internet has a distinctive nature, very different from real world, that has a considerable effect on the subjective element of privacy expectation. It feels much more like a private sphere, meaning that when a person is in front of a computer it naturally feels alone. It has to visualise prying eyes or data collectors; it does not feel them spontaneously. This change of feeling and its effect on how people perceive their on-line privacy should not be underestimated. When we break the unwritten rules of private and public places in real world, we become targets of notice or disapproval. A person shouting in a square becomes certainly the subject of public attention. Complying with these rules requires that we have a good sense of the nature of the place we are in and the people who are in it. The Internet increases the connections between places and the connections between people distributed in space, and as a result the intuitive sense of physical place and presence that governs our observable behaviour can no longer be relied upon to ensure that we will not be seen, overheard, or recorded.[98] And this is important when testing how much privacy is subjectively expected, because people feel that they have more privacy than they actually enjoy. An average individual, for example, would feel less embarrassed to visit the pornography department of an on-line shop and have a look, whereas he would probably

Report No. 56, 17/08/01 and *Messrs Bindam and Partners, on behalf of Ms Anna Ford and Mr David Scott*, PCC No. 52, 15/09/00.

[98] See V Bellotti, *supra*, note 6, at p.64.

never enter a real world store to browse through the 'adult' merchandise. None the less, the privacy of this individual is probably less exposed when 'having a look' in a real world adult store than in an Internet shop. In the former case, the owner or employees might not even notice him, and far less collect information about him, whereas in the latter, it is very possible that an amount of information, some of it personal, will be gathered about him such as his email address or his browser specifications. To sum up, the nature of cyberspace has an adverse effect for on-line privacy: people in cyberspace feel more private than in the real world public spaces, whereas they enjoy less privacy than they actually feel and subjectively expect.

But how about objective expectation? We already saw that subjective expectation has to correspond with what society is ready to accept in terms of reasonableness in order for a privacy claim to be worthy of protection. Even if the feeling changes, as people tend to experience the Internet as a more intimate environment than the real world, it cannot be denied that a considerable majority are at least aware (if not completely informed) of the dangers they face, or they can become aware with an elementary effort. So it is logical to argue that their reasonable expectation should be tested more according to this knowledge than according to their feeling. Reinforcing this argument, it can also be suggested that, as long as 'participation' in cyberspace is optional in the sense that an individual can decide in what ways and to what extent to use on-line services, the level of reasonably expected privacy should not be affected by the feeling of users. In this way, privacy in cyberspace can be reasonably assumed as limited compared to privacy in the real environment. But is there a real 'choice', or is it rather utopian to believe that people would simply opt for the conventional means once they felt their privacy being too much exposed? According to this author's opinion, it is irrational to expect people not to use Internet facilities when they want to protect their privacy just because there is another option to fulfil their needs, that is by using conventional means. The same actions can be performed so much more easily and effectively on-line that it is like not having a choice, especially when social expectations are being transformed by the existence of the Internet. We must not forget that one of the most decisive factors when people make choices and adopt habits and practices is their convenience. Take for example credit and debit cards and cash-cards. Even though most people are aware of the dangers inherent in using them for their transactions, this knowledge has not prevented them from almost replacing real money. Would it be proper to suggest that their users have no reasonable expectation of privacy or protection from misuses just because

they choose to use them even though they are aware of the dangers? People's habits are transformed more by available commodities than by privacy concerns. Certainly it is utopian to abandon an adopted convenience, unless the imminent danger is of great extent. This element should play an equally important role when deciding how much privacy a person should be entitled to and reasonably expect when on-line, especially if 'legitimate expectation' is to play an important role in deciding in which cases on-line is privacy worthy of protection.

It has to be pointed out, however, that the perception of reasonable expectation changes significantly as time goes by. As Froomkin argues, even though exposure to new technologies will probably give rise to a privacy claim in terms of reasonable expectations, these expectations are notoriously unstable: the more widely a technology is deployed and used, the less reasonable the expectation not to be subjected to it.[99] When intrusive techniques become common you reasonably expect less privacy. Take the example of surveillance cameras (Closed Circuit Television or CCTV). Their use is so ubiquitous nowadays that it is very difficult to accept there is a reasonable expectation, in terms of logical thinking, not to be filmed in certain places (a supermarket or a bank for example). Especially in the UK, who has the global lead in the number of surveillance cameras per person,[100] it is unlikely that any person, either in a rural or an urban environment, can avoid being monitored in his role as a shopper, worker, commuter, resident or even school pupil.[101] For on-line privacy, the possible effect of time is that we may reach a point where no expectation of privacy in cyberspace would be considered as reasonable, due to the ubiquity of intrusive technology or practice. Is this acceptable? I would argue that it is not. Even though there is an admitted difference between the exploitation of CCTV cameras and on-line privacy intrusive techniques, the example of CCTV and the privacy issues that arise as a result of its ubiquitous use is a useful example of a technology that has been hastily adopted (both in people's conscience and governmental mentality) before its effectiveness as a measure diminishing or even deterring crime to be sufficiently proven.

[99] See A M Froomkin, *supra* note 50, p.1510.
[100] See S Graham, J Brookins and D Heery, "Towns on Television: Closed Circuit Television in British Towns and Cities" [1996] 22 *Local Governmental Studies* 3.
[101] See C Norris and G Armstrong, *The Maximum Surveillance Society – The Rise of CCTV*, Berg (Oxford 1999), p. 42.

The example of CCTV in Britain

CCTV cameras in Britain were introduced around 1975 to monitor parts of the London Underground as a means to combat staff assaults and theft. Their expansion was quite quick: in the early eighties they were becoming a common feature in shops and by the end of that decade they were widely used in stadia to combat football hooliganism, shopping malls, city centres and banks.[102] Their wide expansion in the nineties was quite inevitable, since CCTV systems had acquired wide acceptance from the public and were promoted by politicians as a primary solution for urban security. Even though the use of video surveillance was initially heavily promoted by the Conservative government of John Major as a key plank in its law and order strategy, it has been equally supported in practice by the labour governments of Tony Blair (even though it did not appear in the labour parties elections manifesto).[103] In 1999 the Home Secretary announced a £150 million extension of CCTV in England and Wales in order to fight petty crime. The then UK Home Secretary Jack Straw was awarded the 1999 UK Big Brother Award. Now we have reached a point where the existence of CCTV systems in public and private areas in Britain is so ubiquitous that it is irrational for an average person to expect not to be filmed at least several times on a routine day.[104]

Even though it is often said that CCTV enjoys a very large percentage of public support in Britain, this is not anymore the complete truth. It is not meant here that CCTV is no longer welcome by the public, but that the percentage of people who are also seriously concerned about privacy and possible abuse of the system is rapidly growing. According to most of the surveys conducted during the eighties and early nineties, CCTV was presented as being acceptable by, more or less, 90% of the public. However, lately it has been also questioned whether these percentages represent the truth and whether the research methods followed were reliable.[105] It is true that CCTV enjoys a considerable public support, a support notably fuelled by the symbolism of certain images of notorious crimes. In 1993, for example, the images of Thompson and Venables - two ten-year old boys who abducted and killed James

[102] See N Taylor, "Closed Circuit Television: The British Experience", [1999] *Stanford Technology Law Review* 11.
[103] See S G Davies, "CCTV: A new battleground for privacy" in C Norris, J Moran G and Armstrong, (editors) *Surveillance, Closed Circuit Television and Social Control*, Ashgate (Aldershot 1998), p. 244.
[104] See C Norris and G Armstrong, *supra* note 102, chapter 3.
[105] See for example, J Ditton, "Public Support for Town Centre CCTV Schemes: Myth or Reality?", in C Norris, J Moran and G Armstrong, *Surveillance, Closed Circuit Television and Social Control*, Ashgate (Aldershot, 1998).

Bulger, a two-year old - were caught on a shopping arcade camera as they escorted the toddler to the street. These images received great publicity from the media. Even though the killers were not actually identified or apprehended as a result of this footage, in the minds of people the connection was irrevocably made between cameras and crime control.[106] There is no doubt that image has a great effect on people, it is a strong weapon in the hands of those who want to promote CCTV. However, privacy concerns and fears of abuse have also started to rise.[107]

CCTV systems operate in public spaces, where people admittedly enjoy less privacy than in their private sphere. However, as already discussed above (2.2), an amount of privacy is still expected. For example, a person may expect to be filmed shopping in a supermarket corridor, but not to be closely examined by the camera operators for no obvious reason. An extended study conducted by Norris and Armstrong[108] showed that CCTV operators are very much affected by their own character, ideas or sense of humour in the way they do their jobs. Furthermore, the simple fact that a person is suspected of a criminal offence does not mean that he has no claim of privacy. Of course, a criminal would not argue that being filmed while conducting a crime is an offence of his privacy, but he still retains other privacy related rights, as for example the right to ensure that the material gained is not used for unauthorised purposes. The case of *R. v Brentwood Borough Council ex parte Peck*[109] indicates that CCTV systems raise a number of privacy concerns. In August 1995, Peck, who was suffering from depression, tried to commit suicide by cutting his wrist with a kitchen knife in the centre of Brentwood. He was filmed holding the knife by the local CCTV system, installed in Brentwood by the Council for the purpose of preventing crime. The police were alerted and Mr Peck was detained under the Mental Health Act 1983. This incident was later included in a Council press release about the CCTV system, and a copy of the footage was obtained by the local television company for broadcast. Although Mr Peck's face was masked, at the Council's request, many viewers still recognised him, which of course caused him distress.

---

[106] See S G Davies, *supra* note 103.

[107] An important survey commissioned by the Home Office from researchers at the University of Wales (T Honess and E Charman, (1992) *Closed Circuit Television in public places*, Crime Prevention Unit paper no. 35. London: HMSO), showed widespread public support for CCTV but it also showed that a significant proportion were worried about certain aspects of visual surveillance. 72% agreed that these cameras could easily be abused and used by the wrong people; 39% felt that people who are in control of the systems could not be completely trusted to use them only for the public good; 37% felt that in the future, cameras will be used by the government to control people.

[108] See *supra* note 102, chapter 6.

[109] Case *R. v Brentwood Borough Council ex parte Peck* [1998] EMLR 697

An unmasked photograph of the incident later appeared in a local newspaper, and the footage was also shown on BBC, again unmasked (an error for which the BBC apologised). In the Court, the judge concluded that by releasing the video footage the Council had not acted unlawfully, since a verbal assurance that the broadcasters would mask the identity of the individual had been obtained. However, the judge expressed his sympathy for the applicant who had suffered an invasion of his privacy and voiced his concern about the lack of regulations and tight guidelines that would prevent such incidents from happening in the future.

This case indicates how far a technology that has been hastily adopted, without prior consideration of the possible implications, can be harmful for privacy. Undoubtedly, CCTV and on-line privacy intrusive techniques have a number of differences. The former has a comparatively 'acknowledged' role to play in the prevention and detection of crime. Furthermore, the amount of privacy that is exposed due to CCTV cameras is limited compared to the latter and people are pretty much aware of their presence and the way they work. The latter, however, have not such an admitted role to play (at least not for the time being, and certainly not information gathering for commercial purposes) in the prevention of crime. The existence of on-line surveillance techniques or information gathering does not make people feel the world as a safer place. Moreover, the amount of privacy exposed can be far greater due to the fact that people are often unaware of how far their privacy is being compromised, as will be subsequently explained. People in front of the computer feel at home rather than being in a public sphere. To have a direct analogy with surveillance cameras, it would be like placing the cameras inside the user's house, which would be rather unacceptable irrespective of how much time had gone by.

The unobtrusiveness of on-line monitoring

The nature of on-line privacy itself is considerably affected by another factor: the unobtrusiveness of the majority of on-line monitoring. Much of the information that is gathered from a person's on-line experience is collected without its knowledge or consent. A big percentage of this information may never be used, at least not in a way that would be noticed by the subject of the information. Is there still an invasion of privacy? A lot of people would suggest that as long as an individual is not aware of the fact that it is being monitored and it feels no actual intrusion of privacy, then one's privacy is not invaded. But how does this argument work in the real world? Imagine a situation where a person is getting undressed

in front of a window that, although closed, has an unnoticed slot from which this person is monitored. As the person is not aware of the slot, it is also unaware of the fact that it is being monitored. Is its privacy still invaded? Even though there is no objective answer to this question, most people would feel offended if they imagined themselves in a similar situation. In fact, there are two Scottish cases where the court accepted that similar situations were indeed a breach of the peace. The first one, *Raffaelli v. Heatly*,[110] dates back in 1949. In this case, the Court found that the defendant, who was peering in at lighted windows after nightfall, was breaching the peace of the inhabitants. The second case, *McDougall v. Dochree*,[111] is a more recent one (1992). In this case the Court found that the accused, who was peeping through a hole in the toilet wall into the solarium room at naked women using the sunbed, was in breach of their peace. Of course, none of these cases was considered as an issue of privacy, which was any way impossible, given the fact that both English and Scottish law did not recognise (until recently) privacy as a legal right. The value, however, that was considered as worthy of protection is one that would fall under the protection of a privacy right. Privacy, as already analysed, is very much about having the ability to 'control' who has access to a person and there can be no control without knowledge. How can people control the dissemination of their private information if they do not know whether such information is being gathered, when and by whom? A significant element of privacy is the preservation of dignity, a value that can be affected irrespective of whether we know it or not. I would suggest that on-line information gathering does violate privacy, even if the user is and will remain unaware that it ever took place.

Privacy sold on-line?

Another element that needs to be assessed is how far privacy that has been sold, in a sense that it was voluntarily exchanged for a return (like a good or a concession or permission to use a site in full), does in fact deserve protection. In the on-line environment, as already said,[112] people very often knowingly accept compromises on their privacy for a return; they sell, in other words, an amount of privacy for a price that varies according to what each site has to offer, be it a concession in the price of the merchandise or a simple permission to view a site in full. Since this exchange is taking place voluntarily, one could argue that as a waived

[110] *Raffaelli v. Heatly*, The Scots Law Times 1949, p. 284.
[111] *McDougall v. Dochree*, The Scots Law Times 1992, issue 25, p. 624.
[112] See page 38 of the thesis.

right it is not worthy of protection. In the recent case of *Douglas and others v Hello! Ltd*,[113] Lord Justice Sedley[114] considered the fact that the major part of the claimant's privacy had become the subject of a commercial transaction, as a decisive factor for the outcome of the case. The claimants had sold exclusive rights for publication of their wedding photographs to *OK!* magazine for a handsome sum, but they had kept the right of veto over which photographs would be publicised, so as to maintain the kind of image that they preferred. Although the Court accepted that the claimants still had a claim on their privacy (due to this veto), it denied the injunctions sought to forbid publication of some wedding photographs by a rival magazine, *Hello!*. The reason was that, since their privacy had been traded, it fell to be protected as a commodity in the hands of the third claimant, *OK!* magazine. As such, possible damages could be easily calculated in money, had the court decided in the final trial that *Hello!'s* publication did in fact cause damage to it. Even though this case shows a reluctance to recognise full protection for privacy that has been voluntarily sold, things are quite different when it comes to cyberspace. Privacy there is not exchanged as consciously as in the case of the two celebrities. Besides, the price it is sold for does not usually represent its real value for the individual or the value it could acquire once added in a database.[115] In the trade off that takes place in cyberspace, data collectors seem to be in a dominant position as opposed to users, a factor that should be taken into serious account before deciding to deny any kind of protection for sold privacy. So it is not just an issue of consent; giving away one's privacy should be an issue of fair consent, meaning an informed and conscious decision, accompanied by substantial knowledge of the consequences. It is very doubtful whether in cyberspace the average user is exchanging privacy with fair consent.

2.5.4. The distinction between traditional and on-line privacy. Is the nature of on-line privacy different?

It has become clear by now that on-line privacy differs from its off-line counterpart in several ways. Let us sum up the basic changes. First of all, on-line communications (as seen in 2.5.1) are considerably more vulnerable than traditional ones: email messages and digital information that travel in cyberspace are already in a form that machines can utilise and analyse, so mass surveillance becomes easier to conduct. It has become very difficult to know and control who may gain access to electronic communications. Second, (as explained in

[113] *supra* note 54.
[114] ibid., paras 140-144.
[115] See A M Froomkin, *supra* note 73, p. 1502.

2.5.2) the Internet poses new challenges for informational privacy both in terms of quantity and quality: access to numerous databases has become much easier and the amount of information that can be gathered and combined far greater. Apart from that, information technology has allowed the use of gathered information in much more creative ways, through techniques of data mining and on-line profiling. It seems like the zone of privacy is being diminished or jeopardised as people move to cyberspace. Third, traditional perceptions of public and private space are significantly blurred in cyberspace: even though it is a public environment where everything can be monitored or recorded, it feels much more like a private sphere (pages 45-46). People in cyberspace subjectively expect more privacy than they objectively enjoy, whereas in the real world subjective expectations of privacy coincide more with objective ones. Fourth, the invasion of privacy in the on-line environment is to a considerable degree unobtrusive (see page 50), meaning that it takes place without the user knowing when he is being monitored or what information is being gathered. In the real world people are more usually, even though not always, aware of invasions to their privacy. Finally, a considerable amount of on-line privacy is being exchanged for a return (see p. 51). Even though this also happens in the real world, privacy in the on-line environment is not exchanged as consciously as off-line, and usually not under a fair deal.

In effect, the on-line environment seems to have brought a maybe unnoticed but still considerable change to the nature of privacy itself, besides the fact that the on-line environment diminishes our ability to control who has access to our private spheres. Due to existing possibilities for interception of on-line communications and data gathering, a person who moves in cyberspace needs to make greater effort in order to preserve its privacy than is necessary to preserve privacy in the real world. If, for example, we want to make sure that an electronic message will not be read by anyone else than the intended recipient we have to use very strong encryption that is not very easy to obtain or to utilise for an average user. In the real world all we need to do is seal the letter in an envelope. We face, of course, the possibility that the intended recipient will divulge the content of our letter to a third party, but we know that this can not be done without the recipient's consent unless there is a warrant. Actually, the reason why our letter is safe is because there is a norm not to unseal envelopes, whereas there is not a norm (at least not yet) that dictates not to read people's emails. The situation is similar with information gathering. It seems to be happening by default in the on-line environment unless we choose to avoid it, which presupposes substantial effort and, of course, knowledge of the fact that information gathering is taking place, which is not the

default position. As surveys have suggested, a substantial number of websites still fail to inform their visitors whether information is being collected on them and how it might be used, or they fail to do it in a way fairly obvious and clear to the visitor.[116]

As a result, the computerised world changes the perception of privacy as a passive right. Implicit in the notion of privacy as the right to be left alone is the idea that the individual should not need to do much to protect this right, as it ought to be socially accepted and respected. What we may be facing with cyberspace, however, is a considerably different technological and social environment in which privacy is not generally accepted and protected. The individual who wants to achieve and maintain some semblance of personal privacy, therefore, will need to pursue it aggressively and persistently.[117] The choice factor in on-line privacy seems to be switching from opt-in to opt-out. The default is that our private sphere is 'open' on-line, unless we choose it to be intimate. As a result, there is a considerable shift of burden from the privacy intruder to the individual to protect its privacy.

This shift of burden is not a novel phenomenon with regard to technological developments. Advances in many fields of technology and science have facilitated the invasion of our privacy in a way that the necessary steps to preserve one's privacy have notably multiplied. The caller ID recognition in wire and mobile telephony is a good example of how this shift of burden works. Before caller ID, the identity of a caller was revealed to the intended recipient only when the caller identified him/herself or when the recipient recognised a familiar voice. It was easy to make an anonymous call simply by disguising a voice, giving a false identity or not revealing identity at all. It has to be noted here that, although the intuitive or traditional reaction to the idea of an anonymous call would be a negative one, anonymity is not only useful for those who wish to avoid accountability. It is also essential for those who wish to protect their privacy. A person who is calling a help-line for health or psychological support or an abuse hotline, for example, may wish to remain anonymous, and the same goes for a person that is merely asking for sensitive information or wants to contact certain organisations. With ID recognition the caller's identity, the number from which someone is calling, is revealed by default to the receiver's telephone, which means that when the caller

[116] See for example the results of the survey conducted by the Electronic Privacy Information Centre (EPIC) in 1999, "Surfer Beware III: Privacy Policies without Privacy Protection" (available at <http://www.epic.org/reports/surfer-beware3.html>, last visited on 23/04/2002).
[117] See T A Peters, *Computerised monitoring and on-line privacy* (1999), McFarland & Company, Inc., Publishers, at p.127.

wishes to remain anonymous he has to take some necessary steps in order to avoid recognition. Even though it is fairly easy to avoid caller ID recognition by dialling three digits before the telephone number, or simply by using a public telephone, the burden still shifts to the caller to conceal his identity when wishing to do so. The reason why caller ID is not considered to diminish privacy is that this burden is not a considerable one; it is fairly easy to hide one's identity when one chooses to do so. It is interesting to note that American Courts found caller ID not to be in the public interest unless free call blocking (a service that allows a caller to prevent his telephone number from appearing on the device of the person receiving the call by simply calling three digits before the actual number) was also offered.[118]

On-line privacy, in effect, is not a novel right as such but an existing one exposed to a new environment. The special features of this environment have an analogous impact on the dangers faced and the ways one can be protected. Overall, privacy in cyberspace is a right more exposed and less protected than in the real world, a fact that most users are not aware of. However, it would be wrong to assume that its difference with traditional privacy lies basically on the perception users have about on-line privacy. The actual exposure of an individual's privacy on-line, which results from the dangers faced in cyberspace combined with the unawareness of the majority as of these dangers and the spontaneous feeling of being private when in front of a computer, is very much real. Furthermore, as pointed out at the introduction of this chapter, the transnational nature of cyberspace and the complete lack of physical borders create the need for a common perception of on-line privacy, which is undoubtedly very difficult to achieve.

2.6 On-line anonymity

This brings us to the issue of on-line anonymity. Anonymity, in general, is closely connected to privacy, since being anonymous is a way of preserving one's privacy. At a first look, the inclusion of this sub-section may seem a bit irrelevant to the rest of the chapter, since on-line anonymity is a big issue by itself for the on-line environment. However, the reason why this author decided to include it here is because otherwise the discussion on on-line privacy would have been somehow incomplete. What is the nature of on-line anonymity in terms of choice and applicability?

[118] See for example *Barasch v. Bell Telephone* 605 A.2d 1198 (Pa. 1992).

In general terms, anonymity is nowhere recognised as a right or freedom as such.[119] It is rather seen as a value, an element contributing to many freedoms and rights, especially the freedom of expression and the right to privacy. In *MacIntyre v. Ohio Elections Commission,*[120] the US Supreme Court recognised that anonymity is an aspect of the freedom of speech protected by the First Amendment of the American Constitution. That was a case concerning the distribution of anonymous pamphlets by Mrs MacIntyre in a public meeting, expressing her opposition to a proposed school tax levy that was about to be decided by referendum. According to the Ohio Elections law, distributing anonymous/unsigned leaflets is illegal. The idea behind this prohibition is that anonymous pamphlets may mislead the public and be generated by people who act in a surreptitious manner and thus disrupt the election process. The Ohio Supreme Court accepted that Mrs MacIntyre had violated this law and upheld the $100 fine that had been imposed on her by the Ohio Elections Commission. However, the US Supreme Court later vindicated Mrs MacIntyre. That Court recognised anonymity as a right in connection with free speech and voting and accepted that political speech is in the core of the First Amendment protection. Anonymity facilitates participation in the political process of society by promoting the expression of ideas free from the fear of disapproval, while -at the same time- it helps individuals preserve their privacy by concealing their identity whenever they wish to avoid public attention. It can be seen as the cloak of privacy we enjoy in public places (public meaning anything outside our private sphere).

Anonymity in the on-line environment is not less valuable: it is seen by many as an essential, if not the only, tool to protect privacy and avoid interference caused by data gathering or interception of on-line communications. According to an interesting point of view expressed by Karnow,[121] the legal status of users acting on the Internet (electronic persons) can be compared to the legal status afforded to entities (like corporations, associations etc.) in the real world. As the law has accepted that these legal persons have legal standing (they have rights, own property, maintain bank accounts, enter into contracts and express views), it is accepting that electronic persons (who represent physical entities) have analogous rights and legal status. As such, a legal system supporting the use of electronic persons may not differ significantly from that supporting the current panoply of fictitious legal entities. According to

[119] For an analysis on anonymity as a legal right see by anonymous, "The Constitutional Right to Anonymity, Free Speech, Disclosure and the Devil", (1961) 70 *The Yale Law Journal* 1084.
[120] See *MacIntyre v. Ohio Elections Commission* 514 U.S. 334 (1995).
[121] See C E A Karnow, *Future Codes: Essays in Advanced Computer Technology and the Law*, Artech House, Boston 1997 (chapter 10).

Karnow, even though there are mechanisms of identification and recognition both for electronic persons in cyberspace and for legal persons in the real world (like electronic signatures or company records), their status is to an extent 'anonymous' since there is no direct physical recognition of a person. All the more so, in cyberspace electronic persons can by default be more anonymous. As Karnow says,[122] beyond the sight and attention of their progenitor humans, electronic persons can recognise each other, do business, and engage in political activity. Electronic persons may be able to act and express opinions without the fear of retribution, but not without responsibility. This anonymity should not be a problem since there is a strong legal tradition in the US accepting anonymity, as for example the use of anonymity in furtherance of political speech. The key is trusting that the source, even an unknown one, has demonstrated knowledge and intelligence. The same trust needs to be moved in cyberspace in order for electronic persons to operate properly. But let us now turn to the more classical approach: do presumptions of anonymity change as we move on-line? How does on-line anonymity differ from its real world counterpart?

Before addressing these questions, it is essential to point out the two-fold nature of anonymity. Apart from the benefits it entails for free speech and privacy, it can also have some negative consequences. The first and foremost disadvantage of anonymity is its inherent lack of accountability.[123] With the cloak of anonymity a person can engage in unlawful or simply disturbing or socially unacceptable behaviour, without being caught and adjudicated, or merely avoiding undesirable or dissuasive consequences such as disapproval or embarrassment.[124] Anonymity is a great tool for evading detection of illegal and immoral activity, and it poses problems for law enforcement in the investigation and prosecution of crime. It is very difficult to trace back the perpetrator of a crime when there are no clues about his identity, so techniques of anonymity may help criminals to avoid prosecution. Avoidance of accountability, however, is not inherently bad. It is often said that anonymity is useful only for those who have something to hide, but that does not mean that the only thing that a person may wish to hide is its illegal intents. As already said, a person may well wish to keep anonymous when engaged in completely legal activity to avoid embarrassment or

[122] Ibid., p. 132.
[123] See E Dyson, *Release 2.0: A Design for Living in the Digital Age* (1997), Viking/Penguin Group, at p. 239.
[124] See M Froomkin, "Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases", (1996) 15 *U. Pittsburgh Journal of Law and Commerce* 395 (available at

social disapproval, or simply to safeguard one's privacy. The lack of accountability can have the same detrimental or positive effects in the on-line environment, as human activity, legal or illegal, moves in cyberspace. Anonymity has also been accused of facilitating the creation of a society of strangers. This disadvantage is probably exacerbated in the on-line environment, which lacks traditional assumptions that are connected with the physical environment and the physical contact between people. Let us see now how on-line anonymity differs from its real world counterpart.

First of all, when considering cyberspace as an 'environment' in contrast to the physical environment, on-line anonymity seems to be more absolute than off-line, because of the lack of physical contact. Anonymity is not by default absolute when behaving in a physical space. A person may well conceal its name, but the physical appearance usually reveals certain information about its identity, as for example sex, colour of skin, age, social status (from clothing or speech) etc. Even a voice on the telephone may reveal much more than simply the sex of the caller (his origin, for example, connected to a certain accent). On-line anonymity, on the other hand, is more absolute, in a sense that an on-line anonymous person is usually nothing more than an 'individual'. Of course things sometimes may work in reverse: anonymity in a physical environment can be made absolute when a person disguises its appearance or voice and certainly when there is lack of physical contact (as in anonymous publications or letters), and similarly on-line anonymity may become less absolute since there is a good deal of information on the identity of a user that can be inferred from anonymous on-line correspondence or conduct (articulate or intellectual writing or the use of a certain vocabulary may reveal connection of the user with a certain profession).

However, in practical terms there are much more substantial differences between on-line and off-line anonymity than that. The degree of anonymity, meaning how far the real identity of a person is traceable or untraceable, is another important issue. In the on-line environment, one of the most common ways to achieve anonymity of communications is by the use of anonymous remailers. An anonymous remailer is simply a computer that forwards emails or files to other addresses over the Internet, but it strips off the header part of a message, which shows where it came from and who sent it. So, even if the content of a message or file can be

<http://www.law.miami.edu/~froomkin/articles/ocean.htm>, last visited on 23/04/2002).

read, no connection can be established with an individual.[125] This anonymity, however, is easily traceable, because the records kept by the operator of the remailer can reveal the real identity of the sender. So, apart from the fact that anonymity is compromised against the operator, it can be also compromised against a third party who retrieves these records, unless of course such records are destroyed systematically or are kept no more than necessary to forward the messages. Even though traceable, the degree of security offered by this kind of anonymity suffices for many purposes, as for example an innocent posting to a newsgroup. But deciding what degree of anonymity is sufficient is an utterly subjective matter that may differ substantially from individual to individual. In order to achieve untraceable anonymity a person has to follow a much more complicated procedure. First, the content of the message sent should be concealed with the use of encryption for better protection. Then, the message should be routed through a series of anonymous remailers, a technique called 'chained remailing'. Even then, the identity of the sender can be revealed, at least theoretically, if all the remailers keep records of the forwarding messages and they are willing to co-operate and reveal the transactional details of the messages they forward.[126] Even though this is not a very plausible hypothesis, it still makes such anonymity less strong than leaving an unsigned leaflet with no fingerprints on someone's doorstep. Additionally, it makes the degree of anonymity dependent on the trustworthiness of the remailers, a factor that cannot always be easily checked.

Anonymous remailers are certainly not the only way to send an anonymous message over the Internet. It can be easily achieved by following more conventional solutions than using technological tools. Maybe the easiest way to sent an anonymous, or rather pseudonymous, message is by opening an email account with a free server (like hotmail or yahoo) giving false identification information, and use a public Internet access, like an Internet coffee-shop, for example, a library or an airport. Free servers do not ask for verification of the identification information provided by the users, and no one keeps a record of the people using a public Internet access. Even though arguably the most effective, this method is not a convenient or permanent solution for regular Internet users who conduct a considerable number of activities in cyberspace and have a regular access from their home or work. It is

[125] See C Bowden and Y Akdeniz, "Cryptography and Democracy: Dilemmas of Freedom", in *Liberating Cyberspace: Civil Liberties, Human Rights and he Internet* (1999), London: Pluto Press, Liberty Editions.
[126] See M Froomkin, *supra* note 73.

certainly very secure and convenient for those who wish to use anonymity in order to avoid accountability for an illegal action.

But anonymity is not only about anonymous communications, it is about anonymous conduct as well, and conduct on the Internet is not anonymous by default. First of all, in order to use the Internet through an ISP, a person has to reveal its name, let alone other more personal information. Even when access is effected through a public network, such as a company or a university network, each individual user is personified. The identity of the user may not be automatically revealed in any web-page that he visits, but it can be easily retrieved without the user's knowledge or consent. This means that a degree of control over one's anonymity is lost. Apart from that, there are several on-line activities that are impossible or at least very difficult to perform anonymously. It is impossible, for example, to purchase goods or services on-line without revealing at least one's name and credit card details, at least not without the use of digital cash that is not widely available yet.[127] Additionally, as analysed above, many techniques have been developed and are widely used in commercial websites for the collection and processing of clickstream data, that can be said to compromise severely anonymous on-line conduct. A person, for example, who wishes to make an anonymous search for a health problem on the Internet, may later realise that its health condition is not so private after all, as it keeps receiving advertisements for health centres that are specialised in treating the particular illness. Although advertisement is not harmful by default, it might be annoying or unpleasant. Apart from that, the circulation of health information beyond one's control may mean that such information can reach the employer or insurance company of the interested party and have devastating effects for one's personal life, especially when this information is incorrect. This may be a hypothetical scenario but is indicative of how far losing control over one's on-line anonymity can be a negative experience.

Last, but certainly not least, on-line anonymity differs from its real world counterpart in the way it can be controlled and limited by regulation. Even though anonymity is a regular cloak of illegal activity in the real world, no-one has ever suggested banning or eliminating the possibilities of achieving untraceable anonymity because it is extremely difficult, if not

[127] It can be argued that even the use of digital cash is not a sufficient cloak of anonymity, at least not when the goods purchased have to be sent to the buyers address. Apart from that there are, and are still developing, different kinds of digital cash that do not always offer untraceable anonymity for a purchase. But this is a whole different issue whose details are not important for the needs of the present analysis.

impossible, to employ a practical way to do it. On-line anonymity, on the other hand, can be more easily controlled to a certain extent. The unlimited use of strong encryption is still a controversial issue among governments (as will be seen in chapter 5) and there is an on-going discussion on the need to regulate and control anonymous remailers to eliminate their potential of being used for illegal purposes.[128] Even though it is arguably impossible to regulate effectively anonymous remailers unless such regulation is applied in an international level, it is almost certain that even a minimum of control and delimitation would dissuade law-abiding citizens from using them, while it will probably fail to eliminate their use for unlawful purposes. Anonymous on-line conduct, on the other hand, is not something that users enjoy by default if they wish to. It becomes more and more difficult to know, much less control, to whom users' identity is revealed, how much private information is gathered about them and where it is being used. This field, however, is mostly left untouched by regulation that would make sure that a law-abiding citizen could enjoy minimum standards of anonymity.

Even though the issue of on-line anonymity is certainly not exhausted by the preceded analysis, it is fairly clear that anonymity is still more difficult to achieve and control in the on-line environment than in the real world. It is probable that after a few years, when people will be more familiar and comfortable with the potentials of cyberspace, anonymity will enjoy the same or analogous assumptions as it does now in the off-line environment, as for example the legal expectation of being anonymous in a 'public space'. For the time being, however, it remains a critical issue of cyberspace, closely connected with the protection of on-line privacy.

2.7 Assessment

The foregoing discussion has probably raised more questions than it managed to answer. It is obvious by now that on-line privacy is not a simple issue, in the sense that it is not directly analogous to its off-line counterpart. Many things are different in cyberspace, a fact that makes traditional assumptions vanish. To quote the most important, the extended exposure of communications and private information in the on-line environment, the lack of a physical existence and the fact that people experience cyberspace as an environment with their minds

[128] See M M Mostyn, "The Need for Regulating Anonymous Remailers", (2000) *International Review of Law Computers & Technology*, Volume 14, No 1, 79-88.

rather than their senses, are all factors that affect the nature of on-line privacy. However, besides the differences, it would be wrong to assume that on-line privacy is a novel issue altogether. As already said, the majority of on-line activities are not entirely new or different from everyday activities in the physical environment. People communicate, exchange views, read news, buy and sell products, do business, and so on via the Internet. All these are better seen as activities of the real world conducted through a new medium, than as entirely new experiences. That is why the essence of privacy, meaning the values it seeks to protect and the way these values are perceived and cherished by individuals, does not seem to change as we move from real world to cyberspace. I think the most appropriate way to view on-line privacy is not as a right new in its entirety, but as a traditional one that is exposed to a new medium, faces novel threats of abuse, and raises further challenges of protection.

What has become clear from this chapter is that the nature of privacy seems to be affected by the on-line environment for a number of reasons. First, the line between private and public spaces is significantly blurred; users find themselves in the peculiar situation where they feel entirely alone and private in an entirely public environment. The words used here may be somewhat absolute but they facilitate a better understanding of this change. Second, there is arguably, at least for the time being, more exposure but less control over one's on-line communications, personal information and anonymity. Third, any form of control is more burdensome to apply, in a sense that on-line privacy has become much more a commodity that users have to acquire for themselves than a right they enjoy by default. In other words, on-line privacy has become an opt-in rather than an opt-out situation. A user that chooses to preserve his on-line privacy needs to take a number of positive steps in order to achieve it.

The aspiration of this thesis is to identify the limits of governmental interference with on-line privacy, in other words to trace the steps to be followed in order to decide which is the best way for a state to interfere (especially negatively) with this right and to what extent it would be acceptable. This chapter has approached the subject on a much wider context, discussing the issue of on-line privacy as a whole; but it has offered the basis to support this effort. As was also explained at the introduction chapter (page 2), governments are certainly not the only agent threatening on-line privacy. It has become obvious that on-line privacy is threatened by private entities as well, especially when it comes to practices of information gathering that are widespread in cyberspace. Governmental interference then needs to take a positive character in a sense that a state needs to interfere in order to protect privacy instead

of restricting it. Even though this thesis focuses on the limits of negative interference, positive interference is not completely left out. There is an interconnection between the two: by compromising on-line privacy a state may allow the creation of vulnerabilities in cyberspace that can be easily abused by third parties as well. This is an aspect that should always be taken into account when compromising on-line privacy.

On-line privacy can be compromised by governmental interference in many ways. First of all, on-line communications can be intercepted, just as telephone conversations are being intercepted by governments. Personal information and the new possibilities of data matching and profiling can prove a very useful tool in the hands of law enforcement agencies. Clickstream data are becoming a fertile source of information that can be analysed by agents in an effort to track evidence of crime that has been consummated in or facilitated by cyberspace. Anonymity can be compromised to reveal the perpetrators of on-line unlawful conduct. Building such possibilities, however, is a compromise for the privacy of law-abiding users as well as the privacy of those engaging in unlawful activity. Ubiquitous interference would fail to discriminate between lawful and unlawful activity and could grant enormous discretion to executive officials. That is why there should be a carefully drawn balance between the common good that is sought to be protected and on-line privacy concerns.

Achieving this balance is not an easy task, but there are a number of criteria that can be used as a starting point. The Better Regulation Task Force, established in the UK in September 1997, suggested some principles that could be used as a template for judging and improving the quality of regulation. The job of the government, as suggested at the introduction of the 2000 Principles of Good Regulation,[129] is to get the balance right between providing citizens with proper protection and ensuring that the impact on those being regulated is not such as to be counterproductive. The five principles of good regulation are:[130]

a) *Transparency* (the process followed in order to adopt a regulation should be clear and open to the public and its purpose clearly communicated; consultation should take place beforehand and the public should be clearly informed on its new obligations and rights).

[129] Better Regulation Task Force, "Principles of Good Regulation" 2000, (available at <http://www.cabinet-office.gov.uk/regulation/taskforce/2000/PrinciplesLeaflet.pdf>, last visited on 15/07/2003).
[130] *Ibid.*

b) *Accountability* (regulators and enforcers should be accountable to citizens, government, parliaments etc.; there should be a well-publicised, accessible, fair and efficient appeals procedure; enforces should be given the power to be effective but fair).

c) *Proportionality* (any enforcement action should be proportionate to the risk and penalties proportionate to the harm done; alternatives to state regulation should be considered and compliance should be affordable to those regulated).

d) *Consistency* (new regulations should be consistent with old ones and with each other; they should also be consistent with international or European rules).

e) *Targeting* (regulation should aim at the problem and avoid a scattergun approach; it should be effective and able to achieve the goal for which it was initially designed; it should be reviewed from time to time to test whether it is still necessary and effective).

These principles are a good starting point for the needs of this thesis, used as criteria for assessment. Identifying the limits of governmental interference with on-line privacy is a process of striking the balance between good and bad interference. More particularly, there are a number of standards that need to be met according to these principles. Here are some examples: practices that limit on-line privacy should be adopted only if a well-documented and macroscopic threat to the common good is to be combated, and not merely a hypothetical danger;[131] this threat should be a viable reason that law is ready to accept; eliminating privacy should not be the first resort to counter such a threat if other possibilities exist; if interference is considered necessary, it should be made as minimal as possible; practical effectiveness should be taken seriously into account before any measure is applied; the process followed should be open to public and users should be constantly informed of the dangers faced and the possibilities created; finally, regulators should be accountable for their choices and enforces accountable for their actions, a mechanism of redress should always be available. These are issues that will be examined in the following chapters.

We saw earlier in this chapter that traditional privacy is a well-accepted and protected human right that enjoys protection at both national and international level. The existing legal

[131] See A Etzioni, *The Limits of Privacy* (1999), Basic Books - US, p. 12.

framework of privacy protection cannot be ignored, even though it cannot be said with certainty whether it should be equally applied or reinforced in the on-line environment. What is rather incontestable is that the special needs and risks that privacy faces in the on-line environment should be taken into account, as well as the idiosyncratic features of cyberspace as such, since they have a decisive role to play in how far policies followed and measures adopted will achieve the expected result. Finally, it should always be kept in mind that cyberspace is an environment with no physical borders. Traditional perceptions of privacy may differ from place to place, however, when it comes to the Internet, these perceptions necessarily merge in order to formulate a common one, however complicated this process may be.

Chapter 3

Computer-related delinquency: the facts providing a tenable reason for governmental interference with on-line privacy

3.1 Preface

The connection of computer-related criminality with on-line privacy may not be so obvious or direct, but here it will be approached as the major actual base for governmental interference with privacy in the on-line environment. As pointed out at the end of the previous chapter, one of the criteria that can be used as a starting point in reaching the right balance between governmental interference with on-line privacy and adequate protection, is to decide whether there is a well-documented and macroscopic threat to the common good that needs to be combated by practices compromising privacy, and not a mere hypothetical danger. The reason is that when the common good is in danger, the concern overrides the need to protect individual rights and freedoms, though to a certain extent. In the real world, for example, the need to investigate, prosecute and prevent crime is a well-accepted reason justifying interference with individual privacy, carried out by governmental agents through several measures such as surveillance of suspects by wiretapping and other means, search of personal premises or seizure of personal belongings, detention and so on. In order for a government to 'act' in an acceptable way (in a sense of drafting a certain policy and implementing it by enacting new legislation), it needs a factual justification on which to base this action. It is preferable that measures adopted be based on real facts rather than mere speculation, especially when individual freedoms are at stake. Even though governmental action can, and very often should, be based on theoretical grounds (in a sense of adopting pre-emptive measures to avoid a possible mischief), real facts operate as an infallible base of assessment: a successful measure is the one that addresses the real dimensions of a problem.

The purpose of this chapter is to explore and analyse the nature of existing and potential threats against the common good stemming from the on-line environment, to the extent allowed by available data. In this author's point of view, it is the first step to be followed in

order to decide how far on-line privacy can and should be compromised by governmental interference, and assess what kind of measures are more likely to yield the awaited result. It should be mentioned that computer and Internet crimes raise a number of legal issues such as jurisdiction, whether they belong to criminal or civil law, who is the perpetrator and the accomplices etc[1]. All these issues, however interesting and important, are not going to be touched by this analysis; what is sought to be explored here is the nature of on-line criminality and the threat that it poses for our society.

Even though it started as a narrow area, confined to the use of the army and academics, the Internet has now become a ubiquitous medium with multiple potential uses for anybody. As such, however, it has attracted individuals with criminal intentions as well as law-abiding users. The more people are using the Internet for professional or personal activities, the more it is becoming an attractive resource for criminals. As it has been successfully observed,[2] 'the fundamental principle of criminology is that crime follows opportunity, and opportunities for theft (and other forms of crime) abound in the digital age.' Criminal behaviour enhanced by the use of computers, networked or not, seems to operate as the factual justification on which governments around the world tend to base the adoption of policies and legislation of interference with the Internet and the digital world. To quote some examples, the National Criminal Intelligence Service (NCIS) submitted a report to the UK Government in August 2000, proposing, *inter alia*, the retention of communications data by ISPs for up to seven years (a measure severely compromising on-line privacy), in order to enhance the investigation and prosecution of crimes.[3] The Commission of the European Union in a communication paper addressing the issue of creating a safer information society, directly connects computer-related crime with the need to intercept on-line communications and retain traffic data (again measures compromising privacy).[4] The US government has justified

---

[1] See D S Wall, "Policing the Internet: maintaining order and law on the cyberbeat", in Y Akdeniz, C Walker and D Wall (editors), *The Internet Law and Society*, Pearson Education Limited (Harlow 2000), pp. 158-161.

[2] P Grabosky, R S Smith and G Dempsey, *Electronic Theft – Unlawful Acquisition in Cyberspace*, Cambridge University Press 2001.

[3] "NCIS Submission on Communications Data Retention Law", (available at <http://www.cryptome.org/ncis-carnivore.htm>, last visited on 23/04/2002). This report was supposed to be confidential, but it was publicised thanks to an anonymous source.

[4] "*e*Europe 2002", Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*, (available at

the use of Carnivore (software designed to wiretap e-mail traffic from ISPs) on the need to combat computer-related criminality.[5] A major part of the Council of Europe's Cybercrime Convention[6] (whose final draft was approved by the European Ministers, on 9 November 2001), is dedicated to the adoption of measures considered necessary for the investigation and prosecution of on-line criminality. One of the side effects of such governmental activity is the compromise of individual privacy. How far this compromise should go depends heavily on the threat posed by computer-related crime. It is, therefore, essential to consider and analyse the nature and potential of such criminal behaviour, before identifying the ideal targets and limits of governmental action. This chapter will explore on-line delinquency in two separate groups: the first contains computer-related crimes, whereas the second encompasses certain concerns of a distinctive nature and the way they have been affected by the use of computers and the Internet.

3.2 Computer-related crime: a major concern

Information technology does not originate from a neutral background; it is the outcome of scientific research that was initially carried out in order to serve military and defence purposes. The first computer was created in the UK during the World War II in an effort to break the secret communication codes used by the Germans, and the Internet begun in 1969 as an experimental project of the US Advanced Research Project Agency (ARPA). First called ARPANET, the network linked computers and computer networks owned by the military, and university laboratories conducting defence-related research.[7] Computers, however, are inherently neither good nor bad; they can be either used for moral and legitimate purposes, or manipulated by criminals to pursue their immoral and illegitimate ambitions. As their number expands globally, there will be a concomitant rise in both the rightful and malicious purposes for which they are put in use.[8]

<http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeCommEN.html> last visited on 23/04/2002).

[5] See M Figueroa, "Carnivore - Diagnostic Tool or Invasion of privacy?", (available at <http://www.sans.org/infosecFAQ/legal/carnivore.htm>, last visited on 23/04/2002).

[6] The final draft of the Convention on Cybercrime is available at <http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm>, last visited on 23/04/2002.

[7] See N Gringras, *The Laws of the Internet* (1997), Butterworths London / Edinburgh / Dublin, chapter 2.

[8] M D Goodman, "Why the Police Don't Care About Computer Crime", (1997) 10 *Harvard Journal of Law and Technology* 465 (available at <http://jolt.law.harvard.edu/articles/10hjolt465.html>, last visited on 23/04/2002).

Governments, especially in the Western world, are becoming more and more concerned about the malicious use of computers since society has come to depend to a considerable extent upon the digital infrastructure. Recent changes in technology arising from the convergence of communications and computing have already had a significant impact on many aspects of life, in both the public and private sector.[9] Vital factors of public life such as air, road and railway traffic control, the dissemination of energy like electricity or gas, telecommunication systems like wire and mobile telephony, systems controlling vital sectors such as national defence and several public services, are now controlled through the use of computers and networked systems. In the private sector computers and the Internet are highly involved in the way we work, communicate, buy or sell products, run businesses, control or invest money, educate or entertain ourselves. Banks, stock markets, and other monetary institutions that handle vast amounts of money base their operation entirely on computer systems. We are moving rapidly to the point where everything will depend on software.[10] Society, as a result, is being exposed to a new form of criminal behaviour, usually referred to as computer crime.

3.2.1 Defining computer crime

As with every new phenomenon, there is still an ambiguity as to which term better describes it and what exactly it encompasses. A considerable number of terms are used for this new kind of criminal conduct, with 'computer crime' being only one of them. Terms such as computer-related crime, information technology crime, cybercrime, information age crime, digital crime, Internet crime or high-tech crime are also in use.[11] Although each one of them seems to emphasise a separate aspect of the phenomenon, they all have a common feature: a computer is somehow involved. It may well be argued that some of these terms describe different things. For example, cybercrime or Internet crime is a term used to describe harmful behaviours in cyberspace,[12] and many commentators choose to approach the subject from this

[9] See P Grabosky, "Computer Crime: A Criminological Overview" (A Paper prepared for presentation at the workshop on Crimes related to the Computer Network, Tenth United Nations Congress on the prevention of Crime and the Treatment of Offenders, Vienna, 15 April 2000, available at <http://www.aic.gov.au/conferences/other/compcrime/>, last visited on 23/04/2002).

[10] P N Grabosky and R Smith, *Crime in the Digital Age (Controlling telecommunications and cyberspace illegalities)* (1998), Transaction Publishers - The Federation Press, at p.3.

[11] The terms 'computer misuse' and 'computer abuse' are also frequently used but they are more obviously connected with a much more certain form of criminal behaviour, especially after having been used in certain laws enacted in the UK and US. See for example the Computer Fraud and Abuse Act 1986 in the US and the Computer Misuse Act 1990 in the UK.

[12] See D S Wall, *Crime and the Internet: Cybercrimes and Cyberfears*, London: Routledge 2001.

perspective. According to this author's point of view, the interconnectivity of computers and the Internet underlines the need for all computer related criminality to be considered in a uniform basis.[13] An all-encompassing approach would be certainly more realistic, since nowadays it has become almost impossible to consider computers without an Internet connection. So, computer crime is used here as a general term to comprise all computer – related delinquency.

Defining computer crime is not an easy task. Suggesting that it encompasses any crime or unlawful conduct where a computer has been somehow involved is a very simplistic approach that provides no help for a substantive analysis. Even after several years there is still no internationally recognised definition of the term;[14] it covers such a wide range of offences that unanimity is very difficult to achieve.[15] For example, if a commercial burglary takes place and a computer is stolen, does this constitute a computer crime, or is it merely another burglary? Does copying software without authorisation constitute a computer crime? What about sending obscene pictures over the Internet? And to make things even worse, the answer to all these questions may depend upon the jurisdiction in which one finds oneself. However, a widely accepted approach is lately being developed, that tends to cover all the cases where a computer has been somehow involved in a crime.

This approach divides computer crimes into three general categories, using as a criterion the role a computer (or computer network) has played in a criminal case.[16] The first includes crimes where a computer is the target of an offence, the second crimes where a computer has been used as a tool for committing a crime, and the third crimes where a computer is incidental to an offence or has been used as a storage medium and, as such, has evidential

[13] Even telecommunications crime (the fraudulent use of any telephone, microwave, satellite or other telecommunications system), which clearly encompasses certain behaviour, is usually considered a computer crime. This is due to the fact that telecommunications systems today are so heavily dependent on computer infrastructure that a crime against them will no doubt involve a computer.

[14] See the "United Nations Manual on the Prevention and Control of Computer-Related Crime", (available at <http://www.hinduja.org/cj.htm>, last visited on 23/04/2002).

[15] See P A Collier and B J Spaul, "Problems in Policing Computer Crime", (1992) 2 *Policing & Society* 307.

[16] D Carter, "Computer Crime Categories: How Techno-Criminals Operate", (1995) 64 *FBI Law Enforcement Bulletin*, at 21. This categorisation has also more recently been recognised, see for example J K Robinson, "Internet as the Scene of Crime - Remarks presented at the International Computer Crime Conference", Oslo - Norway, 29-31 May 2000, (available at <http://www.cybercrime.gov/roboslo.htm>, last visited on 23/04/2002).

value.[17] The distinction between these categories is very often blurred, since each of the roles can be and often are present in a single criminal case. Care should also be taken to avoid confusion between unlawful and immoral or merely annoying behaviour that often takes place in cyberspace.[18]

A number of divergent legal issues arise in the context of computer-related crime, such as what exactly constitutes a computer crime for criminal law purposes, who is the perpetrator, where and when exactly the crime has occurred, who has jurisdiction over it and so on. However, these issues are not the main focus of the present analysis. As already said at the preface of this chapter, the basic target is to explore the nature of the risk imposed upon society and the difficulties in combating it.

3.2.2 Computer as the 'target' of a crime

The most obvious way in which a computer may be involved in a criminal case is when it constitutes the target of an offence. This may occur when the conduct is designed to access, without authorisation, a computer or computer network in order to collect information or cause damage to it, or even steal a computer or a vital component with stored information. The target of such attacks is usually the confidentiality, integrity or availability of a computer or a system. The most common crime belonging to this category is hacking, the unauthorised access of a system or network with the intention to intimidate or steal information or even damage useful resources or information.[19] Other examples include the creation and dissemination of computer 'infections' such as viruses, Trojan horses, worms or mail bombings, the denial of service (DoS) attack (the rendering of a system temporarily

[17] See P Cullen QC, "Computer Crime", in L Edwards and C Waelde (editors) *Law and the Internet: Regulating Cyberspace* (1997), Hart Publishing / Oxford.

[18] This is not the only categorisation of computer related crime; many commentators have used other characteristics in the effort to describe this type of criminal behaviour. For example, focusing on the Internet. The Internet has engendered criminal behaviours in three broad ways: it has provided the vehicle for the further facilitation of existing harmful activities (i.e. e-mail as communications means for criminals), it has generated new opportunities for harmful activities that are currently recognised by existing law (i.e. fraud, theft etc.), and has engendered entirely new forms of harmful activities (i.e. hacking, viruses, etc.). See Wall, D., *supra* note 1, p. 156.

[19] The term hacker was initially used to characterise a person who was largely involved with exploring, testing and analysing computer systems. These were the predecessors of the new age hackers. Even today, the community of hackers argues that the term should not be used to describe those who break into systems and networks with malicious intentions (these should be called crackers instead), because the real hacker is not a person who tries to cause harm but a person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to

unavailable to potential users, using several techniques[20]), spoofing (the act of disguising one computer to 'look' electronically like another, in order to gain access to a system that would normally be restricted), extortion based on threats to release information stolen from a computer system, trespass, vandalism or sabotage.

This category of offences is seen by many as the 'pure' form of computer crime, mainly because it comprises types of offensive conduct that are inconceivable out of the context of computers and did not exist before the advance of information technology. However, it would be very simplistic to view it as the sole form of computer crime; such an approach would fail to take into account the vital role that a computer can play in a criminal case, however traditional its result may be. Offences of this category are often the first step for the commission of traditional crimes, so the distinction between them and offences of the next category (computer as a tool of a crime) is often blurred. To quote some examples, computer spoofing may be used as a way to steal a trade secret or money, or a 'hacker' may unauthorisingly access a system and commit a fraud.

Computers and system networks can be valuable resources for both individuals and organisations. This value has various dimensions, so the damage caused by such offences can be assessed in several dimensions as well.[21] First of all, when computers, chips or other components are stolen or damaged by an intruder, these components themselves have a value in terms of replacement costs. Secondly, the information on the computers has a value of its own; it may have been collected over a long period of time and be unique and vital for the function of an organisation or business. Or it might be confidential, private or personal to an individual who would wish to keep it secret and secure. Even worse it may be vital for either national or individual security, for example information held by a national defence system or confidential data held by a hospital. Thirdly, the continued availability of the computer resource might be of separate value, especially when a system is attacked. A company, like an on-line shop or bank, may be highly dependent on the continued access to the attacked resource or to its computer system as a whole. As a result, unlawful conduct targeting computers can indeed be very intimidating.

---

most simple users who prefer to learn only the minimum necessary. See S Furnell, *Cybercrime – Vandalizing the Information Society*, Addison – Wesley (Boston 2002), pp. 41-42.

[20] See J B Richards, Written Testimony before the US Senate Committee on Appropriations Subcommittee on Commerce, Justice, State and Judiciary *Hearing on Cybercrime*, 16 February 2000, at <http://www.internetalliance.org/policy/000216_testimony.html>.

[21] N Barrett, *Digital Crime - Policing the Cybernation* (1997), Kogan Page editions, at p.64.

It is not easy to assess the nature and extent of the threat posed by computer crimes of this category. Let us take hacking, the most well-known offence of this group. There seem to be two kinds of hackers: those with a criminal intent (the 'crackers', as explained in footnote 19) and those without. The former intrude on computer networks and systems in order to commit a certain damage, steal information or destroy the resources, whereas the latter do it for the mere excitement of intrusion, or simply to annoy their victims and prove how far they can go, some times without causing any severe damage.[22] Both forms are dangerous, however, since they both entail a big repair cost to compensate for systems whose security is compromised,[23] if not damaged, and they both constitute an offence recognised by criminal law at least in the most up to date legal systems.

It is true that in order to analyse in depth the phenomenon of hackers we would need a whole chapter. The origins of hacking, in the sense of technological exploration[1] and tampering, can be traced back to the phone 'phreakers' of the 1960s and 1970s. These were technologically capable persons who had a passion with the telephone system, and tried to learn how to explore, manipulate and control it.[24] The fascination lay in the fact that it was a globally connected network, enabling you to communicate with virtually any other place on the planet, a similar attraction to that which many modern hackers find with the Internet and computer networks. Hacking is a phenomenon of our age; the stereotype of a hacker is a 15-25 year-old male, lacking in social skill and fascinated or even obsessed with technology.[25] However, as the hacker community claims, the motivation for many is simply the fun and challenge that playing with the system can bring. Still, there is no doubt that many hackers are causing serious damage by their intrusions (calculated even in terms of repair cost); accessing a system without authorisation is illegal in most jurisdictions. Anyway the hacker mentality may not be that of a typical criminal, but still it demonstrates a degree of anti-social

---

[22] See M Rogers, "Modern-day Robin Hood or Moral Disengagement: Understanding the Justification for Criminal Computer Activity", 1 July 2000, (available at <http://www.infowar.com/articles/00/article_010700a_j.shtml>, last visited on 23/04/2002).

[23] According to a survey conducted in July 2000, viruses and other destructive actions by computer hackers are estimated to cost businesses around the world $1,6 trillion this year alone. See Internet Nua Surveys at <http://www.nua.ie/surveys/index.cgi?f=VS&art_id-905355901&rel=true>.

[24] For a detailed account of the phreaking scene see B Clough and P Mungo, "Phreaking for fun, " in *Approaching Zero: Data Crime and Computer Underworld*, Faber and Faber (London 1992), chapter 1.

[25] See S Furnell, "Hackers – anti-heroes of the computer revolution?," chapter 3 in *Cybercrime – Vandalizing the Information Society*, Addison-Wesley (Boston 2002).

behaviour.[26] Still, there are many people with great hacking skills that have a clear malicious intention to cause damage and disruption in cyberspace. An in depth exploration of the hacker community and mentality indicates that hacking should not be seen as a typical aspect of criminal conduct. Action against it is certainly needed, but not in the wrong direction. It should not be forgotten that hacking is highlighting the deficiencies of systems and indicates that security should be increased.

The vast majority of intrusions reported up to present have caused nuisance and economic loss rather than severe material or human damage, as would have been the case if a vital network had been manipulated, such as an air traffic control or a military defence system. Economic loss is undoubtedly very devastating for an organisation, but is a value of a lesser legal merit compared to other values protected by law, like life, individual physical integrity or even privacy, and it has less emotional impact on the victims. It is also interesting to note that various data have shown that the majority of system manipulations are perpetrated by insiders, or people who had or somehow attained insider knowledge,[27] which gives a distinctive dimension to the problem as to what kind of measures are more likely to succeed in preventing it. A survey conducted in 2000 showed that the concern about such offences often exceeds the precautions taken by companies and individuals to protect themselves,[28] which means that a considerable number could have been avoided if further protection had been put in place.

Another important crime belonging to this category is computer malicious software or 'malware' (viruses, worms, Trojan horses, software bombs). A computer virus – the most

[26] According to the *Hacker Ethic,* that is widely reproduced on the web, the principles of the hacker community are in summary: access to computers should be limited and total; all information should be free; mistrust authority – promote decentralization; hackers should be judged by their hacking, not bogus criteria such as degrees, age, race or position; you can create art and beauty on a computer; computers can change your life for the better. See a detailed description of the *Ethic* by Steven Levy in S Levy, *Hackers: Heroes of the Computer Revolution*, Anchor Press – Doubleday 1984, pp. 26-36.

[27] According to a number of studies employees represent the largest threat. One study estimated that 90 per cent of economic computer crimes were committed by employees of the victimised companies. A recent survey in North America and Europe indicated that 73 per cent of the risk to computer security was attributable to internal sources and only 23 per cent to external criminal activity. See "United Nations Manual on the Prevention and Control of Computer-Related Crime", *supra* note 14.

[28] Consumers and tech professionals are plenty concerned about being victimised by cybercrime, but only a fraction of them use firewalls on their personal computers, according to a survey by on-line security provider Symantec Corp. See D Kelsey, "Survey - Cybercrime Concern Outweighs Precautions", news article, *Newsbytes*, 29 June 2000 (available at <http://www.infowar.com/survey/00/survey_062900a_j.shtml>, last visited on 23/05/2002).

popular type of malware – has been defined as 'a non-autonomous set of routines that is capable of modifying programs or systems so that they contain executable copies of itself'.[29] Viruses can be very destructive and cause great damage in terms of economic loss and forfeiture of important data and stored information. Two of the most famous incidents were the Melissa virus in 1999 that caused damages in excess of $80 million, and the "I love you" virus in 2000, whose worldwide effect were estimated to have caused at least $7 billion in damage (mostly in terms of lost work time). The perpetrators of these incidents were caught and successfully prosecuted in Court.[30] Computer malware can cause considerable harm and in the majority of cases is generated by skilful persons with malicious intention. It is interesting to note, however, that the best way to combat these incidents is by increasing security and informing people how to be cautious against such attacks.

According to this author's point of view, the main priority in combating this category of offences, before attempting to trace and prosecute perpetrators, is to improve and reinforce the security of computer systems and networks, even though their invulnerability can never be absolutely guaranteed.

3.2.3 Computer as a 'tool' of a crime

The second category (also referred to as crime supported or aided by computers) includes crimes where a computer has been used as a tool to commit an offence. This category is probably the biggest one, as it comprises all the various cases where a computer has been used as a tool, either as such or as a remote access medium through the use of the Internet. The majority of crimes falling within this category are traditional offences committed by the use of a new medium, or simply 'on-line'. Some examples are child or adult pornography, paedophilia, economic fraud, forgery, theft[31] or violation of trade secrets and intellectual property, the sale of illegal substances or goods on-line, stalking, credit card abuses, tax evasion, gambling and money laundering. All these are crimes of the physical world that existed long before the expanded use of computers. Information technology has offered new

---

[29] K Brunnstein, S Fischer-Hübner and M Swimmer, "Classification of Computer Anomalies," Proceedings of the 13th National Computer Security Conference, Washington D.C., 1-4 October 1990, 374-84.

[30] For a detailed description of these cases see S Furnell, *supra* note 25, chapter 5.

[31] For an extended analysis of theft through computers and the Internet see P N Grabosky, R G Smith and G Dempsey, *Electronic Theft – Unlawful Acquisition in Cyberspace*, Cambridge University Press 2001.

potential for their perpetration, and cyberspace itself has become a new area for criminal activity through the use of the Internet.

A wide variety of criminal offences can be perpetrated using or involving computer technology; even murder or manslaughter, by interfering, for example, with a safety-critical system such as an air traffic control system or a hospital computer monitoring the treatment of patients[32] (although this scenario is still only a speculation). It would be wrong to approach these crimes as an entirely new phenomenon, since the values they offend remain the same, and they are usually covered by existing legislation. Money loss, for example, will have the same impact on its possessor irrespective of the means by which it was stolen. What is important to speculate with regard to this category is whether there is an increase of delinquency due to the use of information technology or whether committing certain crimes has become so easy as to raise novel concerns; also, whether the use of information technology hinders their investigation or prosecution.

It is certainly true that information technology can be an extremely helpful tool for perpetrating a number of offences. Computers, for example, can assist the creation of counterfeit currency or official documents using scanners and graphic programs, enhancing this way the traditional crime of forgery. Intellectual property can be violated much more easily, due to the fact that counterfeit digital products, as for example software or compact discs, are of the same quality as the originals and are often difficult to recognise. Computers can also enhance criminality in another way. We saw in the previous chapter that the instinctive feeling of being in cyberspace (in front of a computer) is very different from that of being in the physical world. In that sense, from a psychological point of view, stealing money from a bank by intruding and manipulating its computer network can be much easier and more attractive than walking into the bank with a shotgun. Maybe that is one of the reasons why economic fraud is one of the most frequent computer crimes. The Internet as a medium can facilitate many forms of criminal activity such as the illegal sale of prescription drugs, controlled substances or guns, money laundering, fraud or gambling.[33]

An important example is adult or child pornography and paedophilia; the traditional barriers

[32] See D Bainbridge, *Introduction to Computer Law* (2000), 4th edition, Longman, p.353.
[33] A report of the US President Working Group on Unlawful Conduct on the Internet, "The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet", February 2000 p.12 (available at <http://www.politechbot.com/docs/unlawfulconduct.txt>, last visited on 23/04/2002).

which may deter people from obtaining pornography, such as the embarrassment factor or the price of the material or the difficulty of making contacts, are a much lesser concern with the freedom of access and the facility to make appropriate contacts provided by the Internet.[34] Actually, the source of most public concern over the use of the Internet derives from its potential as a site for child pornography. The very flexibility of the network seems to provide a veritable Pandora's box for controlling the illegal activities of paedophiles intent upon accessing images of children in indecent poses.[35] However, it is also interesting to note that their Internet activity has also opened the way for many paedophiles to be tracked down and prosecuted by law enforcement.

For the time being there are no statistical data showing the actual increase, or not, of traditional delinquency due to the use of computer technology and the Internet. What surveys seem to suggest (as will be later analysed in further detail) is that there is a gradual increase in annual economic losses due to computer crime, resulting mainly from economic frauds and intellectual property theft and violation.[36] However, there is no clear indication as to whether criminality has been so seriously enhanced by new technologies as to demand extended governmental intervention. Stronger security for both individuals and organisations becomes again one of the major priorities. This does not mean that no particular attention should be given by governments to this category of crimes. New needs have been created in terms of investigation and prosecution that demand adequate regulation by governments. For example, international co-operation is very often needed in the investigation of an Internet related crime. The terms of such co-operation need to be regulated. ISPs hold personal and traffic data that are usually extremely valuable for an investigation on an Internet related crime. How long these data should be kept and how can they be retrieved by law enforcement? These are also issues that demand regulation. It is in these regulations that governments are called to respect on-line privacy, by making sure that the possibilities created will not be more intrusive than necessary for the amount of threat posed by computer-related criminality.

The present situation shows that, objectively, only speculations can be made about the

[34] See P Cullen QC, *supra* note 17, p.215.
[35] D Thomas and B D Loader, *Cybercrime –Law Enforcement, Security and Surveillance in the Information Age,* London: Routledge 2000, p. 5.
[36] See M Savage, "Surveys Shows Growing Losses from Cybercrime", news article on the annual survey conducted by the CSI (Computer Security Institution), *TechWeb News*, 5 August 2000 (available at <http://www.techweb.com/wire/story/TWB20000323S0010>, last visited on 23/04/2002).

potential and the threat posed by this new criminal behaviour. It would be mistaken to assume that criminals would be dissuaded from offensive behaviour as a whole, if adequate governmental intervention in computer technology would make their prosecution certain. It is more probable that they would be induced to use other means of communication or tools for their offensive actions. So we should be very careful in assessing the extent of the threat posed by such criminal behaviour and, especially, what are the best measures to deal with it.

3.2.4 Crimes where a computer is 'incidental'

This category comprises all those cases where a computer is incidental, in a sense that it is not by itself required for the commission of unlawful conduct, but has been used in some way connected to the criminal activity. It includes all the cases where a computer has been used as a passive storage medium or, generally, constitutes a valuable resource of evidence for the investigation and prosecution of a crime. A computer, for example, may be important for a drug trafficking case, when drug dealers have used it to store information regarding their sales and customers. Another example is a computer used to store stolen password lists or credit card numbers, irrespective of the way they have been stolen. The Internet can also play an incidental role in a criminal case when, for example, criminals have used it to communicate and organise their plan of action, or a bomb recipe has been taken from a web site, or even when a threatening letter is sent by electronic mail. As Casey observed,[37] computers can contain evidence related to any crime, even homicide and rape. Of course this does not render them pure computer crimes it simply shows that it is no longer sufficient to have a few experts familiar with evidence stored on and transmitted using computers. Any investigation can involve computers or networks and everyone involved in a criminal investigation or prosecution can benefit from knowledge of the underlying technology and its technical and legal parameters. Obviously, this category of crimes seems to overlap with the two previously mentioned, due to the fact that a computer is always of evidential value for criminal cases where computers or systems constitute the target of the offence or have been used as tools. It has a separate value, however, because it has been created to include all these cases where a computer or the Internet has not played such a vital role for the cases to be classified in the other two groups, but it is nevertheless essential for the investigation and prosecution of the crime.

[37] See E Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet,* Academic Press (San Diego, 2000).

As with the previous groups, it is not easy to estimate whether delinquency has been particularly enhanced by the incidental use of computers by criminals. Advances in technology have, no doubt, always been used by criminals to further their ends. Cryptography, for example, is by many said to provide an unprecedented potential for criminals to hide illegal activities, store valuable data, communicate secretly and so on. Cryptography constitutes a popular target for regulation (many governments, especially the US, have tried to eliminate the circulation of strong encryption, as will be later seen in chapter 5). It is interesting to note, however, that the majority of investigations are not actually stopped by encryption. Denning and Baugh[38] report that in most of the investigations they heard about in their research, authorities obtained the key by consent, found it on disk, or cracked the system in some way, for example, by guessing a password or exploiting a system in the overall system. There does not seem to be any evidence that computer technology and the Internet offer such an unprecedented potential for criminal behaviour that there is a need for extreme action by governments to diminish the danger. This is not to say that no special attention should be given to the use of information technology by criminals, but simply that any action should be the outcome of serious consideration on what measures are necessary and whether they can provide the desired result. Technology is in the hands of criminals as much as it is in the hands of law enforcement agencies; it is reasonable to assume that it enhances criminal behaviour as much (if not less) as it enhances the prosecution of criminals by law enforcement. Criminals do not seem to be more sophisticated than governments or law enforcement agencies.

3.2.5 Analysis of available statistics

The title of this subsection may be misleading, as one might think that there are indeed dependable statistics revealing the real dimension of computer-related crime. The truth is far from that for a variety of reasons. First of all, since a commonly accepted, all-encompassing definition of the term is yet to be agreed on, it is still unclear whether certain criminal activity should be included or excluded from these statistics. Each one seems to focus on individual aspects of computer-related criminality (such as system intrusions, Internet fraud, or intellectual property theft), so no concentrated information is available. Furthermore, computer crime is often difficult to detect due to a lack of highly developed detection tools

[38] See D E Denning and W E Baugh, Jr, "Hiding crimes in cyberspace" in D Thomas and B Loader (editors) *Cybercrime – Law Enforcement, Security and Surveillance in the Information Age*, London:

and well-trained personnel, so a large number of incidents (especially system intrusions) remains in obscurity. Roughly speaking, it is estimated that less than one in ten successful computer intrusions is detected. In addition, a large number of computer-related crimes are usually not reported, mainly due to reputation concerns; a system's vulnerability could be devastating for a business once exposed. The same stands for public interest networks: system weaknesses may cause public distrust, so a serious number remains under cover. It is estimated that the percentage of intrusions that are reported to law enforcement agencies is somewhere between 11% and 17% of the actual incidents. Finally, there is no systematic assessment of the threat in a uniform way and over the course of several years so as to have comparative information. But even so, let us see what can be inferred from several samples of available data.

Surveys conducted in both sides of the Atlantic have reached a variety of conclusions, but they all seem to have certain points that they agree on. The National Criminal Intelligence Service (NCIS) of the UK, in its 2001 'UK Threat Assessment of Serious and Organised Crime', dedicated a small part to analysis of the threat posed by high-tech crime (primarily Net crime).[39] The report suggested that this type of crime (without further defining it) is a recent phenomenon compared to other areas of criminality and its current scope and scale are not fully understood. However, it is rather clear that the number of attacks (meaning attacks against networks and systems) is growing, even though greater awareness may be partly responsible for an increase in reporting. In the US, the Computer Security Institute (CSI) released in March 2001 the results of its "2001 Computer Crime and Security Survey", conducted with the co-operation of the FBI.[40] The results of this survey are quite interesting because, although they reveal an increase in the financial losses due to computer-related crime, the actual number of computer security breaches of both government and private-sector systems seems to have dropped. In the 2000 survey, 90% of the respondents reported they had detected a security breach in the last twelve months, whereas in 2001 their number fell to 85%. As for reporting, 36% of the respondents reported the intrusions to law enforcement agencies, a significant increase from 2000 when only 25% said they had reported them. In the US, there are a big number of surveys conducted independently by

---

Routledge, 2000, p. 113.

[39] NCIS "UK Threat Assessment of Serious and Organised Crime", released in July 2001, available at <http://www.ncis.co.uk/threat_assessment.html>, (last visited on 23/04/2002).

[40] CSI/FBI, "2001 Computer Crime and Security Survey", available at <http://www.gocsi.com/prelea/000321.html>, (last visited on 23/04/2002).

private parties; needless to say that it is impossible to quote all of them. It is worth noting, however, that one interesting point they seem to agree on is that the majority of computer intrusions or misuses is perpetrated by 'insiders', i.e. disgruntled employees who have easier access to the system and are perhaps more aware of its weak points than outside hackers. For example the '2001 Industry survey' conducted by the InfoSecurity magazine[41] concluded that insider threats are much more serious than outside attacks. Another private survey conducted by a New York-based firm in 2001[42] concluded that, of all the theft of proprietary information through computer systems, 35% was due to malicious employees and 28% due to hackers. In the international scale now, the latest web statistics of the InterGOV International (an intergovernmental organisation formed to serve, inform and protect all citizens of the Internet community), reveal interesting results.[43] The crime rate is reported to have increased to 41.3% for 2001, but there is a considerable rise in the number of complaints that are reported (even though the majority are invalid). 80% of computer crime is reported to have been committed by 'insiders'. Hackers committed an estimated 5,700,000 intrusions during 2001 alone, but most caused no harm; only 12% of hacker attacks do cause damage.

We could go on and on citing results of surveys conducted around the world, but the picture would still not be much clearer. One thing is for sure; computer-related criminality is an existing problem that seems to be growing in parallel to the proliferation of computer and Internet users. There is no survey assessing computer-related crime in its entirety, encompassing all the three cases where a computer has been somehow involved in a criminal case, referred to in this chapter. Most surveys seem to suggest that computer crime is on the rise (either in terms of reported cases or economic losses) but there are several points that deserve closer attention. First of all, there appears to be a significant rise in the number of reported or admitted cases, so we cannot say with certainty how far the actual number has indeed risen. People have become much more aware of the dangers they face in cyberspace,

---

[41] "2001 Industry Survey", Information Security Magazine - October 2001, available at <http://www.infosecuritymag.com/articles/october01/images/survey.pdf>, (last visited on 23/04/2002).

[42] Computer Crime Survey conducted by Michael G. Kessler & Associates Ltd., see news article at <http://www.ethailand.com/IT/Columns/Siamrelay/computer_crime.html>, (visited on 01/11/200, not available anymore).

[43] InterGOV: Latest Web Statistics (2001), available at <http://www.intergov.org/public_information/general_information/latest_web_stats.html>, (last visited on 23/04/2002).

although that does not necessarily mean that they take adequate measures to protect themselves from them. Second, when contemplating these statistics the rise in the number of Internet users internationally should also be taken into account. That number is around 500 million for 2001, having risen almost 200 million compared to 2000, and estimated to rise 200 million more in 2002.[44] The more people are added to the cyberspace community, the more criminal behaviour related to computers will increase. According to this author's point of view it would be wrong to view computer-related criminality as an exceptional phenomenon of criminal behaviour, a notion that should be mirrored in any decision-making regarding measures to counter on-line delinquency. This does not mean that no special measures are required, but rather that there is no need to compromise individual freedoms and rights more than we do in the real world. Last, computer-related crime should be closely observed if measures are to be adopted that could really reduce it. For example, one of the most interesting pieces of information that we get from the surveys is that the majority of system intrusions is perpetrated by insiders; interpreted correctly, this information suggests that perhaps more effort should be made to build internal and external security for companies than to build surveillance capabilities through local servers. But the necessity and effectiveness of measures will be approached in greater detail later in this thesis.

3.3 Other computer-related concerns

Apart from computer crime as presented above, there is a second group of concerns, regarding the impact of information technology on several other criminal activities, that are increasingly troubling governments around the world (with the US in a leading position[45]). These concerns include the use of information technology for organised crime and paedophilia, terrorism and economic espionage; all three are by many seen as a growing threat for our societies, especially in the Western world, and, as such, a plausible cause for governmental reaction. The need to combat and control these threats is turning into an ever more important base to justify governmental interference with the digital world.

---

[44] The number of Internet users for 2001 worldwide is 513.41 million (377.65 million in 2000) according to Nua Surveys (available at <http://www.nua.ie/surveys/how_many_online/index.html>, last visited on 23/04/2002) and 574 million (322 million in 2000 and 741 million estimated in 2002) according to InterGOV, *supra* note 43.

[45] See M Maher, "International Protection of US Law Enforcement Interests in Cryptography", (1999) 5 *Richmond Journal of Law and Technology* 13, (available at <http://www.richmond.edu/jolt/v5i3/maher.html>, last visited on 23/04/2002).

Undoubtedly, it could be argued that there is an overlap between computer crime and the above-mentioned forms of unlawful conduct, and for that reason they should not be seen as a separate base of governmental concern. This argument is not absolutely incorrect since the conduct of organised criminals or terrorists is objectively a mere aggregation of typical crimes. For example, one of the main fields where organised criminals act is drug trafficking, a crime that may anyway be covered by the foregoing analysis of computer crimes, if it is performed by using information technology as a tool. However, the presentation of organised crime and terrorism as a separate concern is based on the fact that they always receive a distinctive treatment in criminal investigations. The threat that they pose to a country has several dimensions, distinct from the threats posed by other crimes. Terrorism, for example, constitutes a phenomenon whose political dimensions are much more severe than its criminal aspects. One of the major targets of terrorist activity is to inflict fear in people and coerce governmental decision-making, a dimension not existing in other forms of criminal behaviour. Paedophilia has acquired a distinctive value in cyberspace; the Internet has enhanced the interconnection between paedophiles and has allowed it to take a form of organised activity (that is why it is tackled together with organised crime). Such special characteristics dictate the need to evaluate these concerns in a separate section.

3.3.1 Organised crime and paedophilia

Organised crime is distinguishable from other kinds of crime by a number of special features. According to the UK Home Affairs Committee 1994-95 Report on Organised Crime,[46] these can be characterised in a number of ways, but would generally be taken to include the following elements: it is a group activity; undertaken for profit; involving long-term criminal activity; frequently international in nature; of a large scale; frequently combining both licit and illicit operations; and involving some form of internal discipline amongst the group, including use of violence and intimidation. Of course these criteria are not exclusive; organised crime groups have several other, equally noteworthy, characteristics. They usually have a hierarchical organisational structure, a restrictive membership with specialisation of activities, and willingness to use or threaten to use force, and they tend to maintain a code of secrecy.[47] However, what is important is not to have a watertight definition of the term but a

[46] See Home Affairs Committee, Third Report, Organised Crime (1994-95 HC 978).
[47] See B Sullivan, "International Organised Crime: A Growing National Security Threat", (1996) 74 *Strategic Forum* 2.

common understanding of the essential features of organised crime.

Organised crime groups profit from criminal activity, which involves a wide range of crimes. Their most common field is drug production and trafficking (that is also the most readily obvious internationally organised criminal activity[48]), arms and munitions smuggling, human trafficking (either for facilitating illegal immigration or for profiting from sexual exploitation of women and children), money laundering, counterfeiting and forgery. Furthermore, they usually provide their criminal services, such as kidnapping, murdering or stealing, for large amounts of money. Well-known examples of organised criminal groups are the Mafia and the drug trafficking cartels of South America. An interesting dimension of organised crime, (according to the UK Home Affairs 1994-95 Report[49]) and a common view of law enforcement authorities in Europe, is that organised crime should not be seen as the activity of a series of discretely operated groups of criminal gang members. Rather, it involves networks of people many of who might hardly be involved in any direct criminal activity at all, but whose role is to facilitate the criminal enterprise, perhaps by some professional service such as accountancy or legal advice. This indicates that organised crime is a complex phenomenon with intricate dimensions that needs special attention in terms of research and investigation in order to be encountered.

Organised crime constitutes a distinct concern for governments because it seems to have a more severe impact and a greater potential of harm than isolated instances of criminal activity. Many social concerns such as the use of narcotic substances or human trafficking have a direct connection with organised crime, that is considered responsible for providing society with the main supplies in drugs and people. Dealing with this kind of crime is much more difficult and complicated for law enforcement agencies, since most of such groups are highly organised especially to avoid detection and prosecution. Furthermore, there seems to be a link between organised crime and terrorism. For example, a recent UK Report of the Northern Ireland Select Committee on the financing of terrorism in Northern Ireland[50] indicates that there is a link between organised crime and terrorism in that area. In fact, organised crime has been clearly demonstrated to be feeding and facilitating Northern Ireland

[48] See Home Affairs Committee Report, *supra* note 46, p. xiii.
[49] Ibid., p.xi.
[50] See House of Commons, Northern Ireland Affairs Committee, "The Financing of Terrorism in Northern Ireland", Fourth Report of Session 2001-2, HC 978-1.

Terrorism.[51] The preferred activities for fund raising seem to be money laundering, tobacco and fuel smuggling, business and social security fraud, intellectual property theft (counterfeiting). These are operationally complex and potentially very lucrative crimes, but were appealing to terrorists because they attract relatively low penalties compared to the penalties for traditional terrorist crimes.[52] This link between organised crime and terrorism is an important dimension because increased access to money enables organisations to increase the sophistication and impact of their activities,[53] a fact also illustrated by the events of 11 September 2001. One of the main efforts of the US governments in its 'war against terrorism' has been to prevent fund raising for terrorist groups.

There is no reason to believe that organised crime groups would not be interested in taking advantage of information technology, especially those with an international dimension (that is, when either their actions or connections extend beyond national borders) or extended membership are very much likely to use computers or the Internet. These groups are usually powerful in terms of money and people, so they have the potential to take full advantage of available technology to further their ends in numerous ways. The Internet, for example, can be used to strengthen their influence internationally or to communicate in better terms. Computers can be precious storage media where information about clients, connections and members can be kept securely with the use of strong encryption.[54] But, most importantly, the Internet seems to facilitate money laundering and transfer of illegal funds; in effect, it has become easier to use and circulate money that was acquired by illegal means. The UK Home Affairs 1994-95 Report on Organised Crime[55] states that the technical facility which now exists to transfer enormous sums of money along the electronic highway to banks and other financial institutions in other countries and in such a great speed, has some very serious consequences. It has become more difficult to trace the money and therefore the identity of the criminal, smaller countries have become more susceptible to infiltration and need to have very effective monitoring systems in place and, finally, the sums of money that might be moved are so enormous that a great potential of abuse is being created.

---

[51] Ibid., p. 18.
[52] Ibid., p. 13.
[53] J Adams, *The financing of terror*, New English Library 1986, pp. 237-238, 245.
[54] See for example, "Threat from International Organised Crime and Terrorism Before the House of Commons, on International Relations", 105th Cong. 94 (1997) available in 1997 WL 615544 (F.D.C.H.).
[55] *Supra*, note 46, p. xix.

The issue, however, is how far information technology has actually been used by such criminal groups, and whether organised criminality has been promoted in a considerable degree so as to justify vesting governmental authorities with extensive investigatory powers in cyberspace. As in all cases of computer crime, this is very difficult to discover. Available reports, as for example the 2000 NCIS report on organised crime in the UK,[56] have shown no direct evidence that information technology has seriously enhanced organised crime. The Internet, as already said, is a facility area offering unprecedented ability to connect people from around the world with minimum cost and expenditure of time, and as such is also a new area for criminal activity. It certainly assists money laundering, one of the most common activities for organised criminals, but it is doubtful how far it will be used for organised criminal intercourse, given the fact that the whole structure of such groups - especially in their traditional version - is usually based on a closed and secretive mechanism. It can certainly be used to establish connection with remote collaborators or clients, but not as the only means of communication or an area to advertise their 'services'. As for the threat to manipulate critical information infrastructure, it does not seem to be particularly extended for several reasons. It is speculated, although it has not been definitely proved by numbers, that the majority of organised criminals are not of a high intellectual level so as to be able to perpetrate digital crimes of a high level, such as hacking. That is because the nature of the most common crimes conducted by such groups (gun and drugs smuggling, human trafficking, etc) attracts mostly people of lower intellectual classes. Of course this is not absolute. A counter-argument would be that their economic potential would allow them to hire people with the necessary knowledge, but anyway vital information infrastructure is not a usual target for organised crime groups. Their main focus is activities offering a fast and direct profit, such as smuggling of any kind. It is interesting to site the NCIS 2002 Report on Serious and Organised Crime;[57] this report says that it is unclear what proportion of hi-tech crime is attributable to organised criminals but realises that, as banks, businesses and individuals become more reliant on information technology and on-line transactions, the more organised crime groups will be attracted by on-line targets. It goes on to suggest that the ability of such criminals to exploit hi-tech crime will be limited by their level of

[56] NCIS (National Criminal Intelligence Service) 2000 Report on Serious and Organised Crime in the UK. The unclassified version of this report is available at <http://www.ncis.co.uk/PDFS/SmallThreatPages1-14.pdf > (15-39.pdf) (40-52.pdf). (last visited on 23/04/2002)

[57] See "The UK Threat Assessment 2002", The Threat from Serious and Organised Crime, National Criminal Intelligence Service 2002.

technological competence, but admits that criminals are becoming increasingly technologically competent and organised criminals have demonstrated in other areas that they are willing to buy in skills and expertise, or subcontract to specialists, where there is a need or advantage in doing so.[58]

The most obvious way that a computer can be useful for organised crime is as a storage medium, where names, telephone numbers, addresses or appointments can be kept for reference. However, law enforcement agencies are usually led to such evidence after investigation has proceeded to a certain extent; a catalogue with names and telephones hardly constitutes an incriminatory element on its own. Organised crime can of course be enhanced by the use of information technology (especially when it comes to money laundering), but it is still uncertain whether it has done so to a degree dictating drastic measures. Money laundering is a more general problem of criminal activity in cyberspace, not entirely connected with organised crime. The UK Home Affairs 1994-95 Report on Organised Crime recognised that intelligence gathering has a vital role to play in the fight against organised crime but the situation does not call for substantial inroads to be made into ordinary citizen's freedom from intrusion by the state.[59]

However, this subsection would be incomplete without special reference to a certain type of criminal activity that has in fact acquired 'organised' dimension due to the interconnectivity offered by the Internet: that is paedophile crime, on-line child abuse and child pornography. Paedophilia is not an organised crime in its strict sense. Most identified paedophiles operate alone. Organised groups are rare in the UK, as the NCIS reports, but there is an extended networking between individuals for the exchange of material, pornography and fantasies.[60] Advances in information technology and especially the Internet have changed the nature and extend of paedophile networking; before, they would meet mostly by chance or through being imprisoned with other paedophiles. The Internet has made it easier to network on a wider scale and with less risk, where extended security measures are taken. There are paedophile bulletin boards and chat rooms where paedophile and pornographic material is being exchanged. The Internet is also used for establishing contact with victims and for grooming. In effect, the Internet has made networking possible and paedophiles are now considered as

[58] Ibid., pp. 58-59.
[59] *Supra*, note 46 p.v.
[60] *Supra* note 57, p. 62.

organised criminals, although the nature of the crime is completely different from traditional drugs or guns smuggling.

More particularly, computer technology and the Internet allow paedophiles to do things that were not possible in the past. They allow, *inter alia,* instant access to other predators worldwide, open discussion of their sexual desires, shared ideas about ways to lure victims, mutual support of their adult-child sex philosophies, instant access to potential child victims worldwide, disguised identities for approaching children (even to the point of presenting as a member of teen groups), ready access to "teen chat rooms" to find out how and who to target as potential victims, means to identify and track down home contact information, ability to build a long-term "Internet" relationship with a potential victim, prior to attempting to engage the child in physical contact.[61] Inevitably, one would suggest that information technology have enhanced the crime of paedophilia, which is not far from the truth. However, there is another aspect that should be taken into account: information technology has also allowed the investigation and prosecution of many paedophile cases. By the use of information technology paedophile activity is leaving more traces behind than before; large amounts of pornographic material are stored in computers and exchanged through the Internet, all these can be retrieved by law enforcement agencies in the investigation of a paedophile case. In fact, there has been a rise both in the number of paedophile cases that are being tracked down and turn out to see the light of publicity.[62] However, child abuse and pornography is a sensitive matter with many aspects for the society and as such demands special attention, which of course does not mean that any compromise of rights would be acceptable.

3.3.2 Terrorism and cyberterrorism

Terrorism has become one of the most vital concerns for many societies of the Western world, especially after the attacks of September 11 2001 in New York and Washington. Even though the bulk of the research for this part of the thesis was conducted before the events of September 2001, things do not seem to have changed dramatically as to how far this concern affects decision-making in terms of governmental interference with privacy. The fear of terrorism already constituted one of the most popular reasons justifying the application of

[61] See D Mahoney and Dr N Faulkner, "A Brief Overview of Paedophiles on the Web", submitted to the Child Advocacy Task Force on *The Internet On-line Summit: Focus on Children*, Washington DC December 1997.
[62] *Supra* note 57, p.64.

measures restricting freedoms in the on-line world (as for example the effort of the US Government during the last decade to limit the free circulation of unbreakable encryption, as will be further analysed in chapter 4). This fear has now become more concrete and imperative, and reaction more drastic and acute (several laws enhancing surveillance powers were passed in both sides of the Atlantic, soon after the attacks[63]). But let us begin with a more general analysis before turning to the specific impact of the recent events.

Conventional Terrorism

Even though terrorism is a phenomenon with long history,[64] there is still a controversy on the exact definition of the term.[65] It can be roughly described as an act or aggregation of acts involving criminal violence, usually with the intention to intimidate a civilian population and coerce governmental or military decision-making or, generally, express disagreement with governmental policies and actions. One of the most essential characteristics of terrorism, the one that differentiates it from other forms of criminal activity, is its strong dependence on ideology; the motivation for terrorist activities is usually strong political or religious beliefs. This implies, among others, that membership in terrorist groups can be independent of social or economic status and irrelevant to educational or intellectual background and potential. As a consequence, it is very likely that terrorist groups have the potential to make increasing use of information technology, as usually some of their members are well-educated individuals comfortable with the use of technology.

Terrorism provokes such intense concerns that there is temptation to be careless in choosing the weapons to fight it. The fear that it inflicts can be, and has in the past been manipulated by politicians to pass questionable legislation that otherwise would not stand a chance of

[63] In the US, for example, the USA Act was passed, a law greatly enhancing investigatory powers of the police in both real world and cyberspace. (See "Farewell web freedom?", The Guardian 22 October 2001, available at <http://media.guardian.co.uk/mediaguardian/story/0,7558,578204,00.html>, last visited on 23/04/2002). The EU has also reacted, although in a more moderate way. See Statewatch for an analysis of the proposals for legislative reaction, at <http://www.statewatch.org/news>, last visited on 23/04/2002.

[64] The term was initially used after the French Revolution in 1789, although with a different meaning: it used to describe a certain way of governance. Terrorism has taken many forms through history, it has evolved to its present form after World War II, and especially after the 60's. See B Hoffman, *Inside Terrorism* (1999), London: Indigo.

[65] See J R White, *Terrorism: An Introduction* (1998), 2nd ed., Belmont, CA; London: West / Wadsworth, at p.5.

being accepted by public opinion.[66] More government secrecy, more police powers to detain people at will, less governmental accountability, less freedom and less privacy are not novel responses to terrorism.[67] That is why, even after the attacks of September 11, we should be very careful in assessing the real threat posed by terrorist groups using information technology. Governmental action against it could easily go beyond acceptable limits.

Terrorism and Information Technology

Roughly speaking, information technology can be useful for terrorists in two basic ways: first as a tool to enhance traditional action, and second as a target against which to launch attacks. There is speculation that information infrastructure could be a very attractive target, since well-organised attacks against vital networks can cause incalculable damage to public or private organisations[68] and entail serious injury or harm and inflict fear, depending on how crucial is the system. However, it is still unclear whether the results of a determined and deliberate infrastructure attack can be predicted or controlled.[69] But these are two separate threats with different dimensions as to their effect and the measures necessary to deal with them.

Let us first examine the use of information technology as a tool. There are various ways in which computers and the Internet can and are known to be used by terrorists.[70] First of all as a communication medium: electronic mail is one of the quickest, cheapest and most effective ways of communicating and exchanging information, since it can be effectively used to exchange information on possible targets or co-ordinate an action without needing to cross national borders. The Internet can be a useful resource on its own; there is much scattered information on potential targets or weapons (as, for example, instructions on how to manufacture a bomb). It can also be used to recruit supporters or even raise funds; there are

---

[66] See Testimony of David B. Kopel, "Hearings on Wiretapping and other Terrorism Proposals", Cato Institute - Committee on the Judiciary US Senate, 24 May 1995, (available at <http://www.cato.org/testimony/ct5-24-5.html>, last visited on 23/04/2002).

[67] In UK for example the Prevention of Terrorism Act, giving unprecedented investigative and prosecuting power to law enforcement, has caused serious harm to human rights and has hardly immunised Britain from terrorism. See Testimony of D B Kopel (ibid.).

[68] For a detailed account of potential threats see D Denning, *Information Warfare and Security*, ACM Press, Addison-Wesley (New York 1999).

[69] See P Newman, *Computer Related Risks* (Reading: Addison Wesley 1994).

[70] For an interesting analysis of terrorists' web-strategies see K Damphouse and B Smith, "The Internet: A Terrorism Medium for the 21st Century" in H Kushner (editor) *The Future of Terrorism: Violence in the New Millennium* (London: Sage Publication 1998), pp. 208-224.

many known groups that maintain web-pages to advertise their ideology and reach the public in a wide scale.[71] The World Wide Web has become a very effective propaganda instrument since it allows terrorist organisations to spread their message globally by providing background and updated information about their struggle.[72]

Computers, in general, can be as useful for terrorists as they are for law-abiding citizens (as storage media, for example), by becoming part of their every-day activity. Reporters who visited Osama bin Laden's headquarters some time ago, discovered that the group possesses computers, communications equipment and a large number of disks for data storage; it is also speculated that some groups are using strong encryption.[73] It is clear that this use of information technology does not constitute terrorism as such. It remains, however, a severe concern since it presents new dimensions in the investigation and prosecution of terrorist activities. Furthermore, it is important to determine whether such use of information technology is responsible for boosting terrorism activity in general.

Turning against information infrastructure and use it as a target for terrorist attacks is a different issue altogether. Cyberterrorism, a new term describing the convergence of terrorism and cyberspace that has lately become quite popular, is very different from using the Internet for conventional purposes. It is generally understood to mean attacks and threat of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or people in furtherance of political or social objectives.[74] However, it is one thing to penetrate a system in order to extract information or disrupt its users, and another to access remotely a vital system (like an air or road traffic control system)

---

[71] See T Regan, "When Terrorists Turn to the Internet", 07/04/1999 Infowar.com (available at <http://www.infowar.com/class_3/99/class3_070499a_j.shtml>, last visited on 23/04/2002). Some groups that are known to use the Internet for fund-raising are the Mexico's Zapatista Rebels, Peru's Shining Path and Tupac Amaru groups, the Revolutionary forces of Colombia, and also the Hezbollah, Hamas and Hizb ut-Tahrir in the Middle East. See "Cyberterrorism: Overview of the Problem" (available at <http://www.mvhsmun.org/com/terrorism/internet.html>, visited on 15/02/2001, not available anymore).

[72] H Cleaver, Jr, "The Zapatista Effect: The Internet and the Rise of an Alternative Political Fabric", [Spring 1998] *Journal of International Affairs* 51/2, pp. 20-39.

[73] See I O Lesser, B Hoffman, J Arquilla, D F Ronfeldt, M Zanini, B M Jenkins, "Countering the New Terrorism", Rand Report 1999, chapter 3, available at <http://www.rand.org/publications/MR/MR989/MR989.pdf/>, last visited on 23/04/2002.

[74] See D E Denning, "Cyberterrorism" - Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, US House of Representatives, 23 May 2000, (available at <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>, last visited on 23/04/2002).

in order to cause an accident resulting in serious material damage and loss of life. Even though there is still no uniform definition of the term, it is widely accepted that in order to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that disrupt nonessential services or are mainly a costly nuisance would not. There is a tendency to include in cyberterrorism several instances of hacking attacks aiming to disseminate propaganda and express disagreement or political opinions, but this is a phenomenon of a separate value.[75] The first such reported incident occurred in 1998, when ethnic Tamil guerrillas swamped Sri-Lankan embassies with e-mail bombing. The US intelligence authorities rushed to describe the incident as the first cyberterrorist attack, even though it did not result in any big damage. Since then, such techniques have been used during the Kossovo conflict in 1999, and they are a usual incident between parties in many conflicts around the world, such as Israel and Palestine, China and Taiwan or India and Pakistan.[76] Such incidents, however, although usually perpetrated by small groups that could be characterised as terrorists, are more a phenomenon of infowar than cyberterrorism. Terrorists may resort to such actions to publish propaganda or reach public opinion, but it is doubtful whether such activity could be characterised either as terrorism or cyberterrorism. According to the author's point of view it should not, since the effect of such attacks is very different in nature from the effect of a pure act of terrorist violence. It would be more accurate to classify these attacks in the previous category, as use of information technology as a tool for general terrorist activity, rather than as pure forms of cyberterrorism.

However, whatever this author's opinion may be, whether such on-line actions constitute terrorist activities or not is not a simple question to answer. There is an on-going debate around the world on whether several groups that are fighting for political or ideological purposes (like liberation armies for example) are in fact terrorists or not. As the famous saying goes "one man's terrorist is another's freedom fighter". The most recent example in the UK was the debates about section 1 of the Terrorism Act 2000. Much of the legal argument surrounding the passage of the Bill focused on the definition of terrorism. Section 1

[75] See D E Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a tool for influencing foreign policy", Internet and International Systems: Information Technology and American Foreign Policy Decision-making Workshop, (available at <http://www.nautilus.org/info-policy/workshop/papers/denning.html>, visited on 18/09/2000). Not available, na vallw to vivlio

[76] See T Haershman, "Israel's Seminar on Cyberwar", 10/01/2001 InfoSec News, available at <http://www.wired.com/news/politics/0,1283,41048,00.html>, last visited on 23/04/2002.

of the Act elaborates the meaning of terrorism over 5 subsections. Terrorism can mean the threat of, as well as the use of, an action that can occur anywhere within or outside the UK. The persons, property or government affected by the threat or action itself can be anywhere in the world. The purpose of this action must be to influence government "or to intimidate the public or a section of the public" for any "political, religious or ideological cause" (Section 1, (1) b and c). The types of action are defined in Section 1(2) and include "serious violence against a person", "serious damage to property", endangering a person's life, creating a "serious risk to the health and safety of the public", and seriously interfering or disrupting an electronic system. "Terrorism" is also defined by the weaponry involved, whether or not it is designed to influence government or the public. Firearms and explosives deployed in any of the actions in S1(2) means that terrorism is involved. Admittedly this is a very wide definition of terrorism. In the Second Reading of the Bill in the House of Commons,[77] many members of the Parliament raised concerns on whether this definition would include groups and organisations, some of them operating in the UK, that fight for political change in their country. As such groups were mentioned, the Kurds fighting Saddam Hussein in north Iraq, the Kosovo Liberation army combating the Serbs in Kosovo, those fighting for a political change in Saudi Arabia, Iran, Iraq or India, the Ogoni in Nigeria who resist to the theft and pollution of their lands, the Amazon Indians who resist to the destruction of their rain forests, even the animal-liberation campaigners who some times use violent methods to promote their ideology and many more. A Committee was set to discuss on the issue further but Section 1 of the Act was finally passed, accompanied by a big list of "terrorist groups" that operate around the world in Schedule 2. Even though the Government offered strong reassurances that it would apply this definition strictly, there are no absolute safeguards that this will be also the case for all future governments.

There is a number of incidents that have taken place in the past and resulted in major general disruption and economic loss in cyberspace, like the dissemination of the 'I love you' virus in February 2000 that brought down powerful servers such as Yahoo! and AOL. Such incidents are still happening and they will probably continue to do so in the foreseeable future; they are often characterised as cyberterrorism. However, this author is not in agreement with those who adopt such a characterisation, without underestimating the disruption and damage caused by such incidents. The reason is that the effect of such incidents and the intention of

[77] See House of Commons, Second Reading of Terrorism Act 2000, 14 December 1999, Hansard Reference Vol 341, Cols 152-234.

those perpetrating them are very different from cyberterrorism as described above. They lack the underlying extreme ideology and the intention to create fear or disseminate propaganda. Of course what is and what is not cyberterrorism is not to be decided by one person (and certainly not this author), but if there is an agreement to describe such attacks as cyberterrorism, then it would be preferable to find a different name for cyber-attacks that result in serious injury or damage, so as to avoid confusing two substantially different phenomena. Apart from that, it is important to keep in mind that 'terrorism' in common parlance is traditionally connected with acts of a very different nature and impact than the spreading of computer viruses.

In effect, cyberterrorism is not even a 'phenomenon'[78] yet, no pure cyberterrorist attack has taken place up to the present (2002); the attacks that can be attributed to terrorist groups were launched merely to annoy or intimidate their targets, no great damage has occurred and no lives have been lost. So again we can only resort to speculation. There are reasons to believe that cyberterrorism could be very attractive for terrorists. First of all, it can be conducted remotely, anonymously and fairly cheaply, without requiring the handling of explosives or a suicide mission. Computer networking will greatly reduce the personal danger of injury or death or getting caught, for the terrorist.[79] Dependence on information infrastructure gives an opportunity for terrorists to aim at targets that would otherwise be difficult to handle, like air traffic control systems or energy distribution. There is vulnerability even in the most crucial systems, like defence and military networks, which makes them attractive for terrorists.[80] Furthermore, a successful attack could gain extended media coverage, a factor that seems to be a major priority in planning an attack. Information technology, in general, can work as a force multiplier since it allows even a limited number of people to target vital systems and cause serious damage. Valeri and Knights[81] argued that there are three possible criteria indicating which terrorist groups are most likely to incorporate operations of offensive information warfare (OIW): the lack of an established and successful operational style, the ability to foster an offensive OIW capability and an enemy that is highly dependent on information systems. In particular, such groups can be the US militia groups, eclectic

[78] The word phenomenon is used to refer to a fact or occurrence.
[79] R E Stephens, "Cyber – Biotech Terrorism Going High Tech in the 21st Century", in Kushner, H. W., *The Future of Terrorism: Violence in the New Millennium*, Sage 1998, p. 198.
[80] In 1997, a survey conducted by the National Security Agency (NSA), revealed the vulnerabilities of military operational systems in the US.
[81] See L Valeri and M Knights, "Affecting Trust: Terrorism, Internet and Offensive Information Warfare", [2000] 12(1) *Terrorism and Political Violence* 15, pp.20-21.

religious groups, narcissistic individuals and single-issue pressure groups.

However, there are also drawbacks for terrorists in exploiting information technology. Even though vulnerable, systems are usually complex; so it might be difficult to control an attack and achieve a desirable level of harm or damage. Targeting critical infrastructure or causing casualties using information-based attacks may not be as simple as many cyberterrorism scenarios imply.[82] Unless people are injured, there is less emotional appeal and an attack is less successful. It is also probable that terrorists will be disinclined to try new methods and use new tools, unless they consider their old ones inadequate. Our knowledge of terrorism suggests that they tend to use weapons they feel comfortable with or suitable for their activity. Cyber-attacks entail remote handling that gives a feeling of insecurity and a difficulty in checking the actual result. Although radical in their politics, the vast majority of organisations appear to be conservative in their operations. For example, while terrorist groups were more active and considerably more lethal during the 1980's compared to the 1970's, the weapons they chose and the tactics they employed remained remarkably consistent.[83] In general terms, it is difficult to assess potential harm because we do not know how vital systems would react and we cannot foresee all possible forms of attack.[84] Even though we should not underestimate the human factor (there is still adequate control in most of the systems), whatever the measures taken, a risk still remains. Terrorists tend to be a little ahead of the counter-terrorism technology curve, because their efficiency depends on spotting vulnerabilities and launching their attacks against them.[85]

As for the use of technology as a helpful tool by terrorists, the situation is not much different than with the use of other forms of technology. It is utopian to believe that terrorists or any criminals will not use the technology available, but it is hasty to assume that information technology will render them more lethal. A report conducted in the US during 2000,[86] detailing the changing threat of international terrorism, concluded that although the terrorist's

---

[82] See J M Post, K G Ruby and E D Shaw, "From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism", [2000] 12(2) *Terrorism and Political Violence* 97.
[83] See P Wilkinson (editor), *Technology and Terrorism* (1993), London: Frank Class.
[84] See D Denning, *supra*, note 68.
[85] See M Devost, B K Houghton and N A Pollard, "Information Terrorism: Can you trust your toaster?", (available at <http://www.terrorism.com/documents/suntzu.pdf>, last visited on 23/04/2002).
[86] See "Countering the Changing Threat of International Terrorism", a Report of the National Commission on Terrorism, pursuant to Public Law 277, 105th Congress, (available at <http://www.fas.org/irp/threat/commission.html>, last visited on 07/04/2003).

toolbox has changed with the advent of the information age, the objectives of the world's terrorist organisations remain the same. It stated that terrorists are adopting information technology as a command-and-control tool, but there is still no indication as to whether information infrastructures will constitute their new target. Actually, the events of September 11 2001 came as a proof of that. Even though we still know very little about what exactly happened, the events themselves have shown that conventional targets remain the most attractive option. The means used to conduct the attacks were indeed remarkably conventional: no high-tech tools seem to have been involved. Actually, the same sort of attack could have easily happened even thirty years ago, but it seems that no one had ever thought about it or, even less, tried it. As for the use of the Internet as a communication medium, even though at the beginning there was a wide speculation that strong encryption or steganography had been used by the plotters to co-ordinate the attacks, the FBI later admitted that the conspirators had indeed used the Internet to communicate but not in a sophisticated way. They must have used public accesses, such as libraries or Internet cafés, and conventional language codes; the e-mails could be openly read once found but nobody would understand their true meaning.[87]

Certainly the course of the events cannot be taken to indicate that there is no need for special measures to allow on-line investigation. The above mentioned inhibiting factors are likely to change over time; as information systems increasingly become the base of modern society terrorist attacks that target this infrastructure will become more prevalent.[88] There is no doubt that law enforcement agencies need to have the ability to investigate and research the Internet resources in order to combat terrorism and crime. But any measures chosen should be effective and adequate, without imposing a disproportionate burden on law-abiding individuals. For example, the fact that terrorists can use encryption to communicate is not a reason to abolish private communications *per se*. Apart from that, the priority of society must be to counter the routes of terrorism, focusing on the motives that create terrorism. The quest for attention of every oppressed, starving or fighting group of people is such a motive. To those who look for simple acknowledgement that they exist and are part of the society, it has become clear by now that terrorism makes a statement and 'it gets centre stage.' [89]

---

[87] See D Campbell, "How the plotters slipped US net", The Guardian / September 27, 2001, available at <http://www.guardian.co.uk/Archive/Article/0,4273,4264719,00.html>, last visited on 23/04/2002.
[88] See J M Post, K G Ruby and E D Shaw, *supra* note 82, p. 119.
[89] See R E Stephens, *supra* note 79, p. 207.

3.3.3 Economic espionage

The last and possibly least concern belonging to this group is economic espionage. This term signifies the theft or misappropriation of business trade secrets or confidential communications, which provide a negotiating advantage and, as such, constitute an extremely useful tool to prevail over competitors. This technique has proved to be very helpful in pursuing advantageous trade deals; knowing the rival's strengths and weaknesses helps a negotiator pursue his interests more effectively. Of course this concern is less strong than organised crime or terrorism, since it has solely monetary consequences and, as such, has less emotional impact upon the public. But it is still very important because it has a political dimension as well. Big companies are the most usual targets of economic espionage, which is perpetrated either by competitors or by foreign intelligence agents. Companies are also often victims of 'insider' espionage, conducted by their employees who have easier access to the targeted system. With the gradual expansion of telecommuting,[90] the threat becomes even bigger, due to the fact that a business becomes more and more dependent on the information infrastructure. The continuous growth of importance of intellectual property rights is also strongly related to the proliferation of economic espionage.[91]

As businesses enter the information age, the value of trade secrets will continue to grow. However, the same conditions that enhance this value increase a criminal's ability to steal them. The amount of information that can be stored in digital form and travel over a network eliminates much of the constraint associated with having to steal physical documents. Furthermore, the ability to copy data quickly, accurately and securely makes identification of trade secret theft difficult to detect.[92] Finally, a large amount of business communications is done through the Internet, an area where the exact interception potential of private or public actors is still unknown.

The economic well-being of a country, which depends heavily on its industry and businesses

---

[90] Which means moving the work to workers instead of moving the workers to work, by the use of information technology. See J C Dombrow, "Electronic Communications and the Law: Help or Hindrance to Telecommuting?", (available at <http://www.law.indiana.edu/fclj/pubs/v50/no3/dombrow.html>, last visited on 23/04/2002).

[91] See S Perry, "Economic Espionage - The corporate threat", September 1995, at <http://www.the-south.com/USInternational/econ.html>, visited on 18/08/2000, not available anymore).

[92] See M Maher, *supra* note 45, at p.18.

especially in a capitalistic system, constitutes a major concern for a government seeking to ensure a secure environment for economic growth. As a result economic espionage is seen in the Western world as a threat to stability and as such tends to be used as an actual base to justify measures interfering with on-line privacy (such as the use of escrowed encryption, as will be seen in chapter 4). However, the limited available data seem to suggest that the vast majority of economic espionage is not perpetrated by individuals with criminal intention but by governmental intelligence agencies, which seem to have changed their targets after the end of the Cold War.[93] This means that economic espionage concerns have become more a diplomatic issue between governments than a governmental battle against criminals, and as such should have a limited effect on decisions pertaining to limit on-line privacy. However, this does not mean that security should not be a priority, maybe even higher than crime prevention.

3.4 Assessment

Responding successfully to the above-mentioned concerns is not an easy task for governments. Unlawful conduct using the advantage of information technology is different from conventional forms of criminal behaviour in many ways. It is very difficult to assess the real threat placed, because truly reliable estimates of computer-related crime are difficult to obtain and available surveys can be deceptive. Whatever the real estimates, computer-enhanced delinquency is an existing problem that poses a number of different challenges for governments and law enforcement agencies, both of a legal and technical nature.

Computer crime is geographically complex due to the ability offered by the Internet to cross international boundaries without detection. This means that there is a jurisdictional complexity; it usually takes the involvement and co-operation of more than one national authority to trace the perpetrator, a difficult task by default. There may also be a disagreement on substantive law; whether or not the activity in question is criminal at all, who has committed it, when and where, who has in fact been victimised or who should adjudicate and punish it. Furthermore, real time investigation (meaning investigation while the crime is committed) is often needed, which is impossible without the co-operation of several national

[93] See B Livesey, "Trolling for Secrets - Economic Espionage is the new niche for government spies", 28 February 1998, (available at <http://www.infowar.com/class_3/class3_030698a_s.html-ssi>, last visited on 23/04/2002).

authorities, given the fact that a transmission may pass several jurisdictions, even before ending up next door. In fact, one of the most important characteristics of cybercrime is its transnational dimension. Since the Internet has no natural borders, criminal activity in cyberspace has no natural borders as well. This transnational nature calls for a transnational response to the arising problems, unilateral actions would be insufficient.[94] G8 (the group of the 8 most economically powerful countries on earth) have adopted principles and an action plan to fight cybercrime, but definitive steps are still to be made.[95] The most important initiative is the one taken by the Council of Europe that has recently approved the final draft of its long awaited Convention on Cybercrime.[96] The main objective of this Convention (the first international treaty on crime committed via the Internet and other networks) is to pursue a common criminal policy aimed at the protection of society against cybercrime.[97] It is divided in to three sections: the first dealing with substantive criminal law, the second with procedural law and the third with jurisdiction. Even though not fully implemented yet, it has already faced severe criticism; even though it contains a lot of surveillance provisions, it fails to provide specific privacy protection.[98] That is probably because, although drafted by experts, it was not preceded by a thorough investigation about the nature and extent of computer-related crime and the special features of on-line privacy.

The development of information technology offers new techniques to investigate and combat digital criminal behaviour. It is not only criminal action that is enhanced; law enforcement and prosecution are also strengthened. Unlike traditional means of communications, the Internet is an area where technically there is the possibility to intercept on-line

---

[94] See A D Soafer and S E Goodman, "Cyber Crime and Security: The Transnational Dimension" in A D Soafer and S E Goodman (editors), *The Transnational Dimension of Cyber Crime and Terrorism,* Hoover Institution Press (Stanford, 2001).

[95] See Remarks of Kevin DiGregory, "Fighting Cybercrime - What are the challenges facing Europe?" (Meeting before the European Parliament), 19 September 2000, (available at <http://www.cybercrime.gov/EUremarks.htm>, last visited on 23/04/2002).

[96] The final draft of the Convention on Cybercrime was approved by the European ministers on 8 November 2001 and signed in Budapest by the participating states. But it will only become enforceable when five of the 43 signatory states ratify it by incorporating it into their legislation. The final draft is available at <http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm>, (last visited on 23/04/2002).

[97] See the preamble of the Convention.

[98] See Centre for Democracy and Technology (CDT), "Comments of the CDT on the Council of Europe Draft Convention on Cybercrime", available at <http://www.cdt.org/international/cybercrime/010206cdt.shtml>, (last visited on 23/04/2002).

communications,[99] to apply mass surveillance, to access stored data or to track an individual's on-line 'steps'. But the present law in countries around the world is still unable to give a solution, by defining computer crime and drawing the line between acceptable and unacceptable ways of combating it. It is indeed a very difficult task to identify the boundaries of acceptable governmental intervention, because the technological capabilities available compromise a considerable amount of privacy in the Information Age. There is a legitimate need to use existing capabilities to combat crime but there is also a legitimate expectation for privacy for every individual. Even though difficult to estimate, computer-related criminality is a serious problem for society, but it does not appear to be much more serious than expected under the normal course of development in society. As society moves forward, it takes along the problems that emanate from human nature. As Furnell observed,[100] it would be unrealistic to expect a complete removal of the criminal element from the information society; there will always be elements that are unethical or disruptive within any society. As technology itself becomes more pervasive, cyberspace will become a natural environment for criminal opportunities. Widespread acceptance of this fact and good information of users can be the first step in ensuring that information society is a safe place to be. According to this author's point of view, action (either legal or practical) against computer-related crime should not exceed the absolute necessary in terms of compromising on-line privacy, it should not go further than it has done in the real world.

[99] C Bowden and Y Akdeniz, "Cryptography and Democracy: Dilemmas of Freedom", in Liberty eds., *Liberating Cyberspace: Civil Liberties, Human Rights and the Internet* (1999), Pluto Press, p.82.
[100] *Supra*, note 25, at p. 283.

Chapter 4

From facts to theory: the legal justifications for governmental interference with on-line privacy

4.1 Preface

Whereas the previous chapter was dedicated to the presentation of the facts that seem to constitute the most popular justifications for governmental interference with on-line privacy, this chapter will focus on the examination of the legal justifications that can validate interference with individual privacy in the real world in an effort to examine how these factors could similarly operate in the on-line environment. The first part is an approach on a theoretical basis; an effort to explore the most popular reasons that are usually used in laws allowing interference with otherwise protected rights. These reasons are national security, public safety and the economic well-being of a country, a choice of the most popular and all-encompassing justifications that are usually met in legislations. This chapter will try to analyse their content and the drawbacks and difficulties met in their application. For example, the complete lack of a uniform definition has allowed for a rather wide margin of interpretation, used by governments so as to cover even trivial circumstances. The same reasons will probably constitute the basis of legal justification allowing interference with privacy in the on-line environment; so the lessons learned from their up to now application will prove useful, perhaps in order to avoid making the same mistakes.

However, the most interesting part of this chapter is the second one, which is an analysis on how governmental interference with privacy works in the context of the European Convention of Human Rights. As already referred to in chapter 2, Article 8 of the Convention recognises privacy as one of the human rights deserving protection, and lays down the conditions under which interference by governmental authorities may be allowed. The reason why this author chose to examine privacy protection in the context of this treaty is twofold: first, because it is one of the few legal forums that afford a complete protection for privacy, and second, because the existence of an independent Court to deal with the implementation of this convention has allowed for the creation of a uniform and substantive interpretation of

how this Article should be applied. The case law of the European Court of Human Rights is a very interesting field of discussion in the effort to see how legal justifications of interference with privacy work in practice. Perhaps it could be used as a ground on which future legislation concerning interference with privacy on the Internet may be based. The ECHR is the most important and influential Human Rights document in the wider European context and it will inevitably play a prominent role in any future development of law.

4.2 General overview

The idea of safety has always played a significant role in the process of decision-making in any society and in any given time. The feeling of safety and security is an indispensable factor for the well-being and further development of any individual or nation as a collective entity. To understand how important this feeling is let us quote the most recent example signifying it: the events of September 11 2001. One of the most profound effects of these events is the shaking of the feeling of safety in the entire Western world. We have witnessed a number of things being affected by this loss of safety, with law being only one of them. A number of laws have been adopted in both sides of the Atlantic in an effort to combat terrorism and restore the feeling of safety in our society.

The preservation of this feeling of safety and security seems to be one of the primary causes of action for a state. We could say that it is inherent in some of the most popular and general reasons that are being presented as legal justifications for governmental activity that may transgress the limits of individual rights. We are going to proceed with an initial analysis of the most general and perhaps popular such reasons: the national security, public safety and economic well-being of a country. These are of course not the only existing justifications, but rather, according to this author's point of view, the most representative and comprehensive ones.

4.2.1 The case of national security and public safety

The need to protect national security and public safety seems to be the most widely used and accepted legitimate reason for governmental action or interference with individual rights. The importance of these two values has been traditionally recognised in an international level. One of the major tasks of any given government is to serve the public interest by preserving public safety and national security, even when that entails the unavoidable compromise of

individual rights. It is interesting to note that even oppressive regimes tend to govern their states under the pretence of preserving national security and public safety, although their interpretation of the terms is rather not in agreement with the democratic approach.[1] However, what is clearly demonstrated by this fact is the difficulty and risk inherent in analysing and interpreting national security and public safety without transgressing acceptable limits. Governments have to find and implement the right balance between private and public interest, a very difficult task indeed. An attempted definition of the terms would be certainly useful before proceeding to a further analysis.

In a multinational level, there is no widely accepted definition of the terms national security and public safety, even though they have been used in many multinational documents (treaties, agreements etc.)[2] The literal meaning of these terms is well known and understood, but there is no uniformly accepted delimitation of the cases that should fall under these categories. States individually may have adopted some kind of a definition for national security and public safety in internal legislation, although this is not usually a detailed one but rather one that leaves a wide margin of interpretation (as the example of the UK will subsequently show, in 4.3). In theory, an initial approach would suggest that public safety basically refers to the internal situation of a country,[3] whereas national security has to do with external threats. The former tends to cover threats and risks stemming from the interior of a state, whereas the latter risks stemming from external factors and international relationships. However, this is not an absolute distinction since a lot of cases (if not all) tend to lie somewhere between these terms. Especially when it comes to national security, there are numerous internal situations that are considered as issues of this kind. National security clearly covers all military issues, either when it comes to internal military affairs or external threats. The army, defence and intelligence services are the most important factors in preserving national security, so when it comes to them almost any issue could and usually is regarded as one of national security. Besides that, there is a great flexibility in what exactly can be considered as an issue of national security. Dealing with terrorism, for example, - either of internal or external origin - is usually perceived as such. Traditional crimes on the

[1] For example, all the dictatorships of South America and many other countries in the 60's 70's and 80's were exercising their powers under the pretence of safeguarding national security or public safety, "protecting" their states from the threat of communism.

[2] This point, the advantages and disadvantages of a lack of a definition, will be further analysed in 4.3 of this chapter.

[3] See for a relevant reference S Aftergood, "Intelligence versus the Rule of Law", (2000) 84 *Secrecy & Government Bulletin.*

other hand, like drug trafficking or smuggling, are considered as threats to public safety, even though their origin is not of an absolute internal nature. These examples of course are not an exhaustive enumeration, only indicative as to what could be included in the otherwise long catalogue of possible threats. The basic idea behind these justifications is security; the maintenance of internal and external security is, as already said, one of the primary duties of a state, being the prerequisite for the protection of other important values and interests, both in the public and private sphere. The potential risk stemming is that a government could cross the line between acceptable and unacceptable interference with privacy, justifying its intrusive and sometimes arbitrary actions under the auspices of combating terrorism, crime, child pornography, etc.

The position of national security and public safety as important safeguards in a legal system varies according to the nature of each system. For example, in states with a written constitution (e.g. Continental law), both are usually explicitly referred to as cases where the compromise of basic civil, political or human rights is legally accepted. In the absence of a written constitution, national security and public safety can be well-based principles of legal tradition (e.g. Common law). Surprising though it may be, it is very difficult to find in either case well-defined principles of how to implement them in interfering with an otherwise protected right. Of course this does not mean that when it comes to public safety and national security there are no limits in compromising a right. The right balance has to be found in each case so as to achieve adequate protection without compromising liberties and rights more than absolutely necessary. A so-called test of proportionality is supposed to apply, at least in theoretical terms, according to which a compromising measure taken by a government should be proportional to the imminent risk, necessary for its prevention and adequate in nature to achieve the awaited result (see for example Article 8 of the ECHR). However, as will be discussed in further detail later in this chapter, it is rather questionable whether this test can be effectively applied in every case.

4.2.2 The economic well-being of a country

The economic well-being of a country as an indispensable value for its overall prosperity is not a new principle, but its importance has been increased since the end of the Cold War in 1990. Before that, the strength of a country and its ability to influence decision-making at the international level was more or less dependent on its military power and political friends. In the aftermath of the Cold War, this value has become increasingly important as much of

international politics has moved to the economic sphere. Economic power nowadays is equivalent to what military power was during the Cold War. Now the strength of a country depends almost entirely on the value of its currency and its overall wealth, which heavily affects international relationships. A typical example, before the end of the Cold War and the collapse of the Eastern bloc, the balance of power between the two major rivals, the USA and the USSR, was not bending in favour of one of them, even though the USA was admittedly more powerful in terms of economic strength and stability. At the present day, the USA has evolved to an unequalled super power, with its strength resting basically on its enormous economic force.

Of course, this should not be taken to mean that economic evolution is or should be the sole factor in assessing the prosperity of a country; it is just indicative of the importance that it has come to gain nowadays in the game of international politics. The preservation of the economic well-being of a country is gradually becoming a widely accepted legal justification for governmental intervention to citizens' rights and liberties. The idea behind it is that it is a 'collective' right belonging to all citizens, an indispensable factor for both the individual and collective well-being of a nation. A person can better enjoy personal security within the framework of life in a nation that can maintain a number of preconditions, such as a certain standard of living and other social institutions such as health and basic welfare, apart of course from safety and liberty. This idea is not new. General economic prosperity has always been considered a precondition for individual well-being. For most jurisdictions it was until recently an issue of national interest that could justify intervention with individual rights only when interpreted as to form a reason of public safety or national security.[4] Now it has evolved to an independent principle and has been given, as a result, more weight than previously. It has to be mentioned, however, that it constituted one of the legitimate reasons allowing interference with privacy in the context of the ECHR since its very beginning (1950). The acceptable compromise of rights and liberties is again not without limits: the usual tests of proportionality, necessity and adequacy also apply, in a way analogous to the significance of each case.

It is rather difficult to collect in an exhaustive list the range of cases that could fall under this justification. The meaning of the term economic well-being is quite clear, although deciding

[4] For example, in none of the documents of the OECD forum is there any reference to the economic well-being of a country.

what level of economic prosperity is essential or satisfactory is a rather subjective issue. For a country in the Developing world, its economic well-being may well be satisfied by securing a minimum standard of living for its citizens. For a developed and powerful country, like the USA or a Western European state, the standards of satisfying its economic well-being are certainly higher. What is important to make clear, according to the author's opinion, is that the term does not cover only issues of a public nature; it tends to expand to the private sphere of individuals as well. This is almost self-explanatory, at least in the Western society, as the overall economic strength of a modern state is absolutely dependent on the prosperity of private industries and enterprises. However, when the need to combat a threat against economic interests of an apparently private nature comes in conflict with individual rights, these interests have to be of a comparatively wide range before they can be considered to affect the economic well-being of a whole country. When it comes to deciding the right balance between delimiting a right in order to allow for the economic prosperity of a private entity, the criteria as to how far compromising an otherwise protected right is necessary and proportionate to the aim pursued should be stricter than those applying when compromising a right for the sake of the public interest. Inherent in the private interest seeking protection should be an either short or long-term impact in the public good as well.

The emphasis that is given nowadays to the economic well-being of a country as a collective value seeking protection is a usual target of criticism. Much of this criticism suggests that, although it is not wrong for a government to regard economic prosperity as an important national interest, there should be certain limits to the methods, and more broadly to the atmosphere or spirit in which such efforts are conducted. In other words, actions undertaken in pursuit of an economic advantage must never be permitted to curtail democratic freedoms.[5] Undoubtedly, assigning appropriate importance to economic prosperity is particularly useful in finding the right balance of preserving it in expense of individual rights.

4.2.3 Applying the justifications to the on-line environment

After this initial presentation of the most general and popular reasons for governmental interference with individual rights, the first question that comes to mind in the context of the present research is whether the actual situation of computer-related criminality, as analysed

[5] See L Lustgarten and I Leigh, *In from the Cold: National Security and Parliamentary Democracy* (1994), Clarendon Press - Oxford, at p.28.

in the previous chapter, would justify governmental interference with on-line privacy and to what extent. It is not difficult to engage in an initial and rather speculative assessment, although a thorough and substantiated analysis would definitely be more demanding.

Traditional crime has always constituted a serious threat to public safety. Computer crime, in whatever form, causes no less harm than traditional crime. At least when it comes to conventional crimes committed with the help of information technology or through the use of the Internet, there is no doubt about that. The same goes for ordinary crimes that are simply committed on-line. Child pornography or forgery for example, constitute a serious threat to public safety irrespective of the way in which they have been committed. As for the new forms of crime, developed due to recent advances in information technology and the increasing use of the Internet, like unlawful intrusions in vital systems and networks or the dissemination of catastrophic viruses, they can undoubtedly threaten public safety depending on the severity and extent of the damage caused. National security can also be at stake, especially when it comes to unauthorised access of military networks, interception of important correspondence or theft of important military information or secrets.[6] Terrorists can also use technology either as a tool or as a target for their attacks. Either way such actions are usually considered as threats to national security. Finally, electronic surveillance is increasingly promoting economic espionage, which can be very harmful to the economic well-being of a country. The expanded use of computers and the Internet by big corporations increases their vulnerability to the theft of trade secrets or intellectual property. Interception of the correspondence and communications of a company can reveal useful information to its rivals, either of an internal or external origin.

Obviously, an initial approach to the issue would end up with this conclusion: the threats posed to a community from unlawful conduct enhanced by the use of computers, networked or not, could justify governmental interference based on public safety, national security and concerns for the economic well-being of a country. However, the situation is not that simple; this is merely a theoretical approach. Applying the particular justifications as reasons where interference with an individual right, such as privacy, by the government is acceptable is a

[6] See M G Devost, "The Digital Threat: United States National Security and Computers", (Paper prepared for presentation at the 1994 Annual meeting of the New England Political Science Association, April 1994), available at <http://www.oss.net/Proceedings/ossaaa/aaa3/aaa3ae.htm> (last visited on 23/04/2002).

much more complicated procedure. What can be inferred with certainty is that computer-related criminality, in whichever of the forms analysed in the previous chapter, is a plausible reason for interference with individual rights and liberties. The major difficulty in applying that is that the nature and wide use of computers and the Internet has created new expectations for users, mainly concerning their privacy and freedom of on-line action. Given the fact that the Internet started as a free un-regulated area, that was supposed to develop in a self-regulatory manner,[7] it is very difficult for governments to find how far such intervention should or could go.

4.3 The difficulties and drawbacks met in approaching the terms national security, public safety and economic well-being of a country

The first and major difficulty encountered in the effort to approach the terms national security, public safety and economic well-being of a country (as reasons justifying interference with otherwise protected rights) is the lack of a widely accepted definition. Few, if any, of the laws referring to them (either of a supreme character such as a constitution or treaty, or of an ordinary nature such as a national law) offer a contentious definition, by delimiting the cases that should fall under each category.

Especially when it comes to 'national security', there is an admitted reluctance in proceeding to a further detail or definition than just referring to the term. This is partially understandable since few concepts are more complex, vague and of such a practical importance for the exercise of political power than national security.[8] An additional problem is that the operative meaning of the term is utterly subjective, varying correspondingly for each state and each time. The consequent disadvantage is that national security can be very easily confused or rather conflated with national interests. This is rather hazardous due to the fact that giving to the term so wide-ranging a meaning is potentially very oppressive, for it erodes the distinction between the civil and military spheres of social life, or at any rate between a liberal and an authoritarian society.[9] Moreover, unlike other governmental authorisations to limit human rights, powers granted to governments in this area are often wholly discretionary

[7] See A J Campbell, "Self-Regulation and the Media", available at <http://www.law.indiana.edu/fclj/pubs/v51/no3/CAMMAC15.PDF> (last visited on 23/04/2002).
[8] See L Lustgarden and I Leigh, *supra* note 5, at p.3.
[9] ibid., p. 27.

and non justiciable. The lack of statutory definitions of what is meant by the term leaves a wide margin of appreciation for governments to decide themselves what is and what is not an issue of national security. This margin of appreciation can be easily abused by governments.[10] Another impact of this lack of definition is that it is very difficult for the judiciary, when it is given the chance, to rule that an exercise of power by the government falls outwith the scope of national security. Courts may moreover lack the procedural competence, for example jurisdictional obstacles, or the political will to intervene.[11]

Let us see in a little more detail the situation in the UK. National security (such as public safety and the economic well-being) appears to a considerable number of statutes of internal legislation as a legitimate reason for acceptable governmental interference with individual rights. Some of the more characteristic laws that permit considerable interference with individual privacy are the Security Service Act 1989[12] (later completed by the Security Services Act 1996), the Intelligence Services Act 1994[13] (enacted to regulate the function of the MI5, MI6 and the GCHQ), the Official Secrets Act 1989, the Interception of Communications Act 1985 (IOCA), and the most recent Regulation of Investigatory Powers Act 2000 (RIPA) (that has integrated and replaced IOCA). In most of these statutes the term national security is not accompanied with a further definition or an indicative list of cases that would fall under this category. Section 1(2) of the Security Service Act 1989 is one of the exceptions; it states that the function of the Security Service is the "protection of national security, and in particular its protection against espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means". As the Security Service Commissioner has mentioned in many of his annual reports[14] the concept of national security is not defined in the Act, but includes, though is not confined to, these specific cases. This means that the list is not exhaustive, and in effect this is not a definition of the term but an indication of the cases that will necessarily be covered. A margin of appreciation is left open for other cases to be considered as matters of national security. The Official Secrets Act 1989

[10] See H Barnett (editor), *Constitutional and Administrative Law* (1998), Cavendish Publishing Ltd, London-Sydney, at p.17.
[11] See I Cameron, *National Security and the European Convention of Human Rights* (2000), Kluwer Law International, at p.68.
[12] See I Leigh and L Lustgarten, "The Security Services Act 1989", (1989) 52 *Modern Law Review* 801.
[13] See J Wadham, "The Intelligence Services Act 1994", (1994) 57 *Modern Law Review* 916.
[14] See for example "The Annual Report of the Security Service Commissioner for 1999".

also provides some indicative definitions of the terms used, but not such a clear one. For example in Section 1(9) it says that security or intelligence means "the work of, or in support of, the security and intelligence services or any part of them, and references to information relating to security or intelligence include references to information held or transmitted by those services or by persons in support of, or any part of, them". This may be a definition, but it is such a wide one that would cover almost anything that the secret services decide to tackle. The rest of these Acts simply refer to national security as one of the reasons justifying activity (interception, surveillance etc), without further analysing the term or the cases that should fall under it.

It is interesting to note that the definition of terms such as national security, public safety and the economic-well being of the country have many times been discussed in the Parliament, during debates about the passage of these Acts. Concerns have many times been raised on the unlimited width of these terms and the possibility to cover many cases. In the most recent passage of RIPA through Parliament, concerns on the definition of these terms were raised and discussed by several Parliamentarians, but these discussions have not led to an inclusion of exact definitions in the Act.[15] It is very characteristic that in 1988, during the debate on the Security Service Act 1989 in the Parliament, the then Prime Minister, in answer to a Parliamentary question from an MP regarding the definition of the term, stated that: "*National Security is generally understood to refer to the safeguarding of the state and the community against threats to their survival or well-being. I am not aware that any previous administration has thought it appropriate to adopt a specific definition of the term*".[16] This statement is indicative of the reluctance on the part of the political authorities to determine the exact boundaries of what can be covered by the term, so national security can mean whatever any given government chooses it to mean. The situation has not changed in more recent legislative efforts. There is no further definition of the term national security, or the rest of the reasons allowing governmental activity, in the recent Regulation of Investigatory Powers Act 2000, where national security is one of the primary legitimate justifications of interference with privacy. There are of course, in all the above-mentioned laws, provisions regulating safeguard procedures in case an individual considers interference with his rights to

[15] See for example the Second Reading of the Regulation of Investigatory Powers Bill 2000 in the HC Dbs, Voll 345 Col 767-838 (6 March 2000).
[16] See HC Debs, Vol126, col.7 (25 January) 1988.

be unlawful; however the adequacy and efficiency of these procedures is rather debatable.[17]

The lack of definition on the part of the legislature makes the Courts, when and if given the chance, reluctant to proceed to a definition of their own. They tend not to question the issues presented by the government as ones of national security, focusing their approach to the cases on less sensitive matters, such as applying the test of proportionality and necessity on the measures in question.[18] Striking examples of this practice are a number of cases that had to do with the Intelligence Services: the Spycatcher cases,[19] the case of Richard Tomlinson[20], the case of Blake[21] and the most recent case of David Shayler.[22] All these cases considered ex-employees of the Intelligence Services, who decided to reveal and publish information that came to their knowledge while they were working for the UK government. Although these cases were touching issues of national security (since the information revealed could expose the work of the Intelligence Services), the Court focused in their confidentiality aspects and decided them on confidentiality grounds, being a safer and more clearly legal way of approaching them. National security was certainly at stake, but the Court accepted that as a fact, without regarding it necessary to engage in a detailed discussion on how far national security was endangered or not by these publications.

In the latter of these cases, *R v Shayler*, the Court came very close to discussing the meaning of national security, but preferred to focus on the principle of proportionality. David Shayler, a former member of the Security Service, had been charged with unlawful disclosure of documents and information contrary to the Official Secrets Act 1989 (sections 1 and 4). Under this Act it is illegal for a member or former member of the Security Services to disclose information that came to his knowledge under duty. There is no public interest

[17] Even though a further analysis would nor be so relevant to the subject, it is worth noticing that none of these Acts allows for an individual to get a case into a Court other than the special Tribunals created for these specific cases. This issue will be discussed in detail in chapter 6, with regard to RIPA.

[18] See for example the UK Case *Balfour v Foreign and Commonwealth Office*, [1994] 2 All ER 588, where the Courts refused to accept a role in providing an independent check on claims of public interest immunity certificates issued on the grounds of national security.

[19] *Attorney-General v. Guardian Newspapers Ltd.* [1987] 1 W.L.R. 1248, *Attorney-General v. Guardian Newspapers Ltd. (No. 2)* [1988] 2 W.L.R. 805, *Attorney-General v. Newspapers Publishing Plc.* [1987] 3 W.L.R. 942. For an analysis of the cases see P M Dane, "The Spycatcher Cases", (1989) 50 *Ohio State Law Journal* 405.

[20] See A S Reid & N Ryder, "The Case of Richard Tomlinson: The Spy who E-mailed Me", (2000) 9 *Information & Communications Technology Law* 61.

[21] *Attorney-General v Blake and Jonathan Cape Ltd*, [2000] 4 All ER 385.

[22] *R v Shayler* [2002] UKHL 11.

defence to justify disclosure and the question was whether this lack of defence was compatible with article 10 of the ECHR that regulates freedom of expression. Both the Court of Appeal and the House of Lords accepted that this lack of defence is compatible with the ECHR, given that the Act offers the possibility of applying for a permission of disclosure and Mr Shayler had not used this procedure. It is interesting to note that although the Court went into much detail in analysing the conditions under which freedom of expression can be restricted under the ECHR, it focused on the issue of proportionality expressing no doubt whether issues of the Secret Services were issues of national security. There was no direct reference to the content of the information disclosed by Mr Shayler, in order to decide which one was heavier: national security protected by these information or the public interest served by their disclosure. It is interesting to note that Mr Shayler had revealed details of a plot to assassinate Muammar Gadafy, claiming that the Secret Services had paid Al Qaeda £100,000 to assassinate the Libyan leader. Given the events of 9/11 2001, there is no wonder why the Court avoided discussion on the merits of the case. It would mean taking a decision of a political nuance, which is something the Courts have always been avoiding to do.

It is a well-known judicial view in the UK that matters concerned with national security are generally non-justiciable,[23] in the sense that the Courts do not tend to argue whether the issue at stake is indeed one of national security. This is understandable, given the fact that the Courts are trying to respect the principle of the separation of powers. It is indeed a job for the legislature to delimit these terms and the Courts will probably continue to leave those issues untouched without a lead from Parliament.[24] The resulting disadvantage is that it will be easier for any government to be less prudent and more arbitrary when considering a matter as one of national security. Apart from that, secrecy usually accompanies national security policy-making and operations, which unavoidably entails a high potential for abuse of power.[25]

The disadvantages stemming from the lack of definition are also apparent when it comes to public safety or the economic well-being of a country.[26] However, the potential effect is much

[23] See A Tomkins, "Public Interest Immunity after Matrix Churchill", (1993) *Public Law* 650.
[24] See J Wadham, *supra*, note 13, at p.920.
[25] See I Cameron, *supra*, note 11, p.67.
[26] The economic well-being of the country has been an issue of Parliamentary Debates many times during the passage of laws through the House of Commons. Most recently, this term was discussed during the Second Reading of RIPA (*supra* note 15), where concerns were raised on the unnecessary width of the term.

less harmful in these cases, since national security is considered a much more sensitive issue compared to safety or economic well-being. It is certainly easier to doubt whether there is a threat to public safety than to argue on a case of national security. There is, nevertheless, a new trend in approaching public safety issues which is proving rather problematic. It seems that the line is being blurred when it comes to issues of crime and public order regarded as something for the ordinary police, and crime regarded as mandate of the security police, or the internal security agency (which is traditionally vested with extended discretion and more secrecy). For example, in UK the Security Service Act 1996 was enacted to complete the 1989 Act by adding to the function of the Security Service the prevention and detection of "serious crime" (section 1(4)). The prevention and detection of serious crime is also a reason justifying severe intervention with privacy through interception of communications in RIPA (Section 5(3)(b)). A general international development can be discerned whereby the security police and Intelligence Services are given a role to play in combating major drug trafficking, organised illegal immigration, smuggling of weapons, corruption of public institutions and organised crime more generally.[27] Of course there is a reason for that: there seems to be an inter-connection between such crimes and terrorism. Terrorist groups tend to engage in other forms of criminal activity (like weapon smuggling or money laundering) in order to secure funds for their ulterior purposes (see chapter 3, page 83). Of course this is a viable explanation and justification for transferring powers to the Intelligence Services to deal with such crimes. But as more and more issues are being transferred to the authority of the Security Services, the discretion in interfering with individual rights becomes bigger and the potential of abuse higher.

Even though the disadvantages and difficulties stemming from the lack of an official definition of the terms, aiming to specify and delimit the cases falling under these categories, are rather serious, it is admittedly not simple to come up with an all-encompassing and yet moderate definition. The task would become even more difficult if we were to decide on a multilateral treaty. The way that a state perceives national security or public safety has a lot to do with internal circumstances, international relationships and economic stability, issues that are highly variable and easily changeable for every state. Especially when it comes to information technology, the rapid steps of progress and the different level of modernisation in each country make it even more problematic to achieve a satisfactory and technology neutral

[27] ibid., p.69.

definition. For example, the number of Internet users and the level of dependence on information infrastructure, utterly determinant factors when it comes to deciding whether certain abuses can constitute a threat to public safety or national security, varies considerably from country to country.[28] Internet users are not disseminated around the globe in an analogy to how world population is disseminated. The same factors will also be crucial in deciding how far the economic well-being of a country is endangered by abuses of information technology resources.

The next question is how to achieve the right balance of governmental interference with individual rights, especially privacy, when it comes to the Internet and information technology more generally. The first step of course would be a meticulous and unambiguous definition of the facts constituting a legitimate reason for interference with on-line privacy. But as this is rather utopian, it becomes very useful to focus on the rest of the conditions applying when a government decides to interfere with an individual's rights. The next part of this chapter will concentrate on the European level. The European Convention of Human Rights becomes relevant when it comes to deciding acceptable interference with privacy, since it is the base on which most European legislation on human rights is being developed. An examination of the case law relevant on the subject may prove to be very useful for an all-embracing approach.

4.4 Governmental Interference with privacy under the European Convention of Human Rights

Privacy constitutes one of the basic human rights recognised and protected by the ECHR. As already said in the first chapter, the ECHR is the most important document in the sphere of human rights protection in the European level, due to its great number of contracting states and its binding nature. An independent judicial system has been created by the treaty to safeguard its effective implementation. When a person or a state considers that there has been a violation of a treaty right by a contracting state, they both have the right to file a complaint against that state to the European Court of Human Rights.[29] The Court will then decide whether there is indeed a case of violation of the treaty that deserves adjudication, before a decision on the merits is made. A further analysis of this system is not necessary for the

[28] See *supra*, note 7 of chapter 2.
[29] Henceforth also referred to as the Court.

present study: it suffices to say that the mere existence of case law on the interpretation and implementation of the ECHR is very useful, as it indicates how certain issues would or should be approached. Furthermore, the case law of the court has become even more relevant for the UK, because it has recently incorporated the ECHR as an internal law by the Human Rights Act 1998.[30] Since October 2000, the ECHR is fully implemented throughout the UK. There is certainly much to say about the Convention in general, and privacy in particular. But the main focus of the following analysis will be the way the legally acceptable justifications for interference with privacy are being implemented.

4.4.1 Privacy protection in the ECHR and the limits of governmental interference

As stated above, privacy is one of the basic rights that the contracting states are bound to protect under the ECHR. According to Article 8 of the Convention:

> *"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 in accordance with the law and is necessary in a democratic society in the interest of national security, public safety or the economic well-being of a 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".*

The first paragraph of Art. 8 recognises the right to privacy as deserving protection under the Convention. The interpretation of this paragraph has been discussed in a large number of cases, in an effort to identify the meaning of the terms 'private' and 'family life', 'home' and 'correspondence', and decide the sphere of implementation. Doing that was considered necessary because none of the terms used in this paragraph to specify the meaning of privacy is self-explanatory. In general terms, the Commission (when it still existed) and the Court have both adopted a rather wide interpretation, avoiding laying down general understanding of what exactly is covered by each of the terms and preferring to utilise the co-terminacy of them so as to cover a broad range of cases.[31] Admittedly, this lack of precision has allowed them to develop a case-law that is open to take into account social and technical

[30] See J Wadham and H Mountfield, *Blackstone's Guide to the Human Rights Act 1998* (2000), Blackstone Press Ltd.
[31] See D J Harris, M O'Boyle and C Warbrick, *Law of the European Convention of Human Rrights* (1995), Butterworths – London, at p.303.

developments.[32] By this interpretation the Court has managed to cover all the different 'types' of privacy, as they were described in chapter 2 (page 13).

For example, there are a number of cases where the Court was faced with an issue of interception of communications, secret monitoring and surveillance. In *Khan v. UK*[33] the Court accepted that the use of equipment in police surveillance operation (listening devices on the premises of the applicant) was indeed an infringement of privacy (whether it was justified or not is a different issue altogether). In *Valenzuela Contreras v Spain*[34], it was not disputed whether interception of communications/ monitoring of a telephone line was an issue of privacy, and the same happened in *Kruslin v France*[35], *Huvig v. France*[36] and *Malone v UK*[37]. Secret surveillance and monitoring of communications entails both physical and mental access to a person's territory or activities, without his knowledge or consent. In effect, these cases cover the type of accessibility privacy, that is controlling who has physical or intellectual access to a person.

The Court has also recognised informational privacy, a person's ability to control the dissemination of information relating to it. In *Leander v Sweden*[38] the applicant was refused permanent employment as museum technician on account of secret information. It was uncontested that an interference with privacy under Art. 8 had occurred through information being held in a secret police register about him, combined with the refusal to allow the applicant an opportunity to refute the information. In *Gaskin v UK*[39] the applicant was denied access to personal files and records, which contained information concerning highly personal aspects of his childhood, development and history. The Court had no difficulty accepting that a privacy issue was at stake.

Last, the Court has recognised expressive privacy as well. This type of privacy has to do with freedom from coercion and discrimination when making personal decisions; a key feature of expressive privacy concerns the free development of one's identity. In *Niemietz v Germany*[40],

[32] See *Rees v UK* A 106 (17/10/1986) and *Marckx v Belgium* A 31 (13/6/1979).
[33] *Khan v.UK* (2000) 31 EHRR 45.
[34] *Valenzuela Conntreras v.Spain* (1999) 28 EHRR 483.
[35] *Kruslin v.France* (1990) 12 EHRR 547.
[36] *Huvig v.France* (1990) 12 EHRR 528.
[37] *Malone v.UK* (1985) 7 EHRR 14.
[38] *Leander v.Sweden* (1987) 9 EHRR 433.
[39] *Gaskin v. UK* (1989) 12 EHRR 36.
[40] *Niemietz v.Germany* (1992) 16 EHRR 97.

a case concerning the search of the law office of a lawyer, the German Government disputed whether there was an issue of privacy since the search considered the professional life of an individual. The Court held that:

> "it would be too restrictive to limit the notion of privacy to an 'inner circle' in which the individual may live his personal life as he chooses and to exclude therefrom entirely the outside world not encompassed in that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. There appears to be no reason of principle why this understanding of the notion of privacy should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant opportunity of developing relationships with the outside world".

Similar cases were *Kopp v Switzerland*[41] and *Amann v Switzerland*[42] where it was held that professional life is part of private life, since it is an area where people develop their personality. Expressive privacy has also been recognised in a number of cases that had to do with homosexuals being dismissed from the army due to their sexual preferences.[43] The Court recognised that the sexual preferences of a person are an integral part of his character and a vital aspect of its private life.

Although the Court has not yet been given the chance to rule on how far privacy protection applies when it comes to information technology developments, such as the Internet, the approach that has been adopted in a way suggests that they will be ready to accept it as a new sphere of implementation for Article 8. Of course, it is dangerous to make a hasty generalisation since the majority of cases do not tell us much beyond their own facts. As a result, the only conclusion that can be drawn with relevant certainty is that the Court is open to accept new spheres of implementation. It is difficult, if not impossible, to decide which are the exact cases that will fall under the protection of Article 8.

However, what is of greater relevance for the present analysis is paragraph 2 of Article 8, which lays down the conditions under which governmental interference can be legally accepted under the Convention. According to this paragraph such interference is acceptable when it is 'in accordance with law' and 'necessary in a democratic society', and it is aiming to protect 'interests of national security, public safety or the economic well-being of a

[41] *Kopp v.Switzerland* (1998) 27 EHRR 91.
[42] *Amann v.Switzerland* (2000) 30 EHRR 843.
[43] *Lustig-Prean and Becket v.UK* (1999) 29 EHRR 548, *Smith and Grady v.UK* (1999) 29 EHRR 493, *Buckley v.UK* (1997) 23 EHRR 101.

country', or when it is designed to help the 'prevention of disorder or crime', or, finally, for the 'protection of health or morals and the rights and freedoms of others'. The reasons presented above are the legal justifications under which a government is allowed to compromise privacy. The importance of the case-law of the Court interpreting and applying this paragraph lays on the fact that it is indicative of how such interference should be implemented in areas not yet covered by a case-law of their own. It is very interesting to see how the Court tends to react in cases of interference, how it tends to interpret and approach legal justifications and how much weight it lays on each one of the conditions.

Paragraph 2 of Article 8 contains an exhaustive catalogue of the reasons for which governmental interference can be allowed. National security, public safety and the economic well-being of a country are the first and more general ones mentioned in this catalogue. The other reasons referred to are certainly more specific and arguably less problematic than the former ones, in a sense that it is a lot easier to identify the cases falling under them. One could also argue that these more specific reasons are in a sense contained in the meaning of the more general ones. The prevention of disorder or crime can be regarded as a case of public safety, and the same goes for the protection of health or morals. There is no indication, however, that these more specific reasons work as a definition of the general ones, nor has the Court ever adopted such an approach. It is more probable that the original drafters of the Convention wanted to make sure that these more specific reasons would be, one way or another, regarded as legal justifications for interference, leaving in any case a large margin for discretion for governments to interpret national security, public safety and the economic well-being of a country, as there is a complete lack of further definition or clarification of the terms.

An acceptable reason is not the only condition for justified interference. It should be, in addition, in accordance with the law and necessary in a democratic society. These additional conditions are aiming to prevent abuse and misinterpretation from the part of the government. They play an important role in the process of identifying the limits of governmental interference with individual privacy, in order to find the right balance. The way the Court has approached these conditions could work as a guideline of how interference in new areas of privacy should be planned.

4.4.2 The case-law of the European Court of Human Rights interpreting the conditions for governmental interference with privacy

The Court has been given the chance to apply Article 8 of the Convention many times, it is impossible to refer to all of them in the present study. The examination will focus on the ones considered most interesting in terms of interpretation of paragraph 2, and correlation with potential cases of governmental interference with computers and the Internet. Reference will also be made to certain cases dealing with the interpretation of Article 10 of the ECHR, regulating freedom of expression. Although freedom of expression is not the focus of the present study, case law on Article 10 becomes relevant so far as the conditions laid down by the Convention for acceptable restrictions of the right are similar to the conditions laid down in paragraph 2 of Article 8.[44]

The case-law on telephone tapping and secret surveillance

The Court has several times been given the chance to rule on cases of governmental interference with privacy, in the form of telephone tapping and secret surveillance. One of the main ways in which on-line privacy can be compromised by governmental interference, as seen in the first chapter, is through surveillance of on-line behaviour or communications. The nature of such interference with on-line privacy is very similar to the interference examined in cases of this group, which is why they are of great interest for the present study.[45]

One of the first cases in this area was *Klass v. FRG*,[46] where the Court was asked to decide whether a German law permitting state authorities to open and inspect mail and listen to telephone conversations under certain circumstances, was compatible with the ECHR. The

---

[44] Aricle 10, paragraph 2 of the ECHR reads as follows : *"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 interest of national security, territorial integrity or public safety, for the prevention or disorder of crime, for the protection of health or morals, for the protection of the reputation the rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."*

[45] The Cases studied in this group are (in chronological order) : *Klass and Others v.Federal Republic of Germany* (1979-80) 2 EHRR 214, *Malone v.UK* (1985) 7 EHRR 14, *Huvig v.France* (1990) 12 EHRR 528, *Kruslin v.France* (1990) 12 EHRR 547, *Niemietz v.Germany* (1992) 16 EHRR 97, *Kopp v.Switzerland* (1998) 27 EHRR 91, *Valenzuela Conntreras v.Spain* (1999) 28 EHRR 483, *Amann v.Switzerland* (2000) 30 EHRR 843, *Khan v.UK* (2000) 31 EHRR 45.

[46] *Klass and Others v.Federal Republic Germany* (1979-80) 2 EHRR 214.

applicants were five German lawyers who, although they had not themselves been subject to such measures, considered themselves as potential victims, since there was no absolute requirement in this law to notify the persons after the surveillance was finished; consequently there was no way to get informed that such an activity, which would have violated their privacy, had taken place. The Court accepted the application of the lawyers, considering them indeed as possible victims, but ruled that the measures of the law did not violate the right to privacy since they were necessary in a democratic society and in the interests of national security, within the terms of paragraph 2 of Article 8. Irrespective of the result, it is interesting to note that the Court insisted that paragraph 2 of Article 8 should be interpreted narrowly, since it provides for an exception to a right guaranteed by the Convention.[47] However, this is rather a general remark and not an imperative principle with much practical implication; the rest of the cases do not seem to be strictly decided under this assumption. The Court seems to focus much more on other issues.

In most of the cases studied (eight out of nine[48]) the Court found that there had been a violation of Article 8, because the interference could not be justified under paragraph 2. The Court has always followed a consistent practice when applying Article 8: it first examines whether there is an interference with a protected right and then in goes on to check whether this interference is justified, by examining whether (a) it is in accordance with law, (b) pursues a legitimate aim and (c) is necessary in a democratic society to achieve this aim. In most of these cases the Court decided that the interference was not justified because it was not 'in accordance with law'. As this is the first of the three conditions to be tested, the Court did not go on to examine compliance with the other conditions as well. Consequently, less can be inferred on how the Court has tested the legitimacy of the aims pursued and the necessity of the measures taken. Let us take these conditions in reverse, starting with the legitimacy of the aims pursued.

1. Does the interference pursue a legitimate aim?

It is obvious, at least from the cases where the Court went on to examine all the conditions of Article 8 par. 2, that it has generally been reluctant to go in too much detail when assessing whether the government was indeed in pursuance of a legitimate aim. It does not seem to

[47] *Klass and Others v.Federal Republic Germany*, ibid., par. 42.
[48] Only in *Klass and Others v.FRG,* ibid., did the Court find that there was no violation of Article 8.

have followed a narrow interpretation of this condition. In both *Klass v.FRG* and *Niemietz v.Germany* (in which a German lawyer complained that the search of his office by governmental authorities had given rise to a violation of Article 8) the Court did not discuss this point beyond merely accepting that the aims presented by the Government were indeed legitimate (national security in the first case, and the prevention of crime and protection of the rights of others in the second).[49] The Court tends to follow this practice of unquestioned acceptance of the reasons presented in the bulk of its case law, and not only in this group of cases. One reason is that a state can rely on a long list of broad purposes, so when the Court reaches the explanation given by a government to justify interference, it is easily convinced that the state was acting for a proper purpose, even where this issue has been disputed by the applicant.[50] Furthermore, assessing the legality of the aims pursued would mean that the Court would have to adopt a highly political and theoretical attitude, criticising and scrutinising political views and decisions, which is a difficult task to perform in legal terms. This is not an unexpected attitude since it is a common judicial practice for courts to focus on purely legalistic approaches, avoiding criticism of governmental policies in theoretical terms. Therefore, few assumptions can be made as to how the Court will approach analogous reasons for interference with on-line privacy, whether it will recognise flaws in the legitimacy of the aims pursued or the particular cases where interference will probably be accepted. It is rather expected that it will generally accept the aims proposed by governments with little difficulty.

2. Is the interference in accordance with law?

Now let us turn to the first condition applied, whether governmental interference is 'in accordance with law'. There is greater clarity on how this condition is applied, since the Court has followed a consistent practice interpreting it. Unlike the issue of the legitimacy of the aims pursued, it has entered upon this point in much more detail, to a considerable extent due to the fact that it feels more comfortable with purely legalistic approaches. *Malone v.UK*[51] is one of the most characteristic cases where this condition was interpreted. Mr Malone was a UK national who, after being charged with a number of offences and acquitted by the Courts, filled a complained against the UK state for interfering with his privacy by

[49] *Klass and Others v.Federal Republic of Germany*, ibid., par. 46 and *Niemietz v.Germany* (1992) 16 EHRR 97, par. 36.
[50] Eg *Andersson (M and R) v.Sweden* (1992) 14 EHRR 615.
[51] *Malone v.UK* (1985) 7 EHRR 14, paras. 66-68.

intercepting his telephone calls and his correspondence. Before this case, there was no legislation in the UK regulating the interception of communications, although it was a standard practice for the police and Security Services. The Court ruled that the interception at stake was not in accordance with law since such a law did not exist. It is interesting to note that as a result of this decision the UK introduced laws regulating the interception of communications, the Interception of Communications Act 1985. Starting from this case, the Court has consistently held that interference with privacy by surveillance measures, as with any other interference, must have some base in domestic law, which must itself be compatible with the rule of law, in a sense that it should be '*adequately accessible*' and '*reasonably foreseeable*' for the citizens. That is because the phrase '*in accordance with law*' does not merely refer back to domestic law but also relates to the '*quality of law*'. As the Court said in *Sunday Times v.UK* ,[52] a citizen must have an indication of the legal rules applicable to a given case and must be able to control his conduct in the sense that the consequences which a given action may entail must be foreseeable, to a degree that is reasonable in the circumstances. In *Kopp v.Switzerland* and *Valenzuela Contreras v.Spain*, where the Court was asked to rule on the legality of monitoring of telephone lines in connections with criminal proceedings, it said that, especially when it comes to interception (that constitutes a serious interference with private life and correspondence), it has to be based on a law that is particularly precise, as the technology available for use is continually becoming more sophisticated.[53] This notice is becoming all the more important in the context of the Internet, where the technology of on-line surveillance is becoming very complicated indeed; making a law comprehensible for citizens will be a great challenge. Furthermore, the Court has come to accept that quality of law also implies that there must be, in the domestic law in question, a measure of legal protection against arbitrary interference by public authorities with privacy. Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident (as seen in *Amann v.Switzerland* [54]) and safeguards against abuse should exist. These safeguards include a definition of the categories of people liable to be subjects of surveillance by judicial order, the nature of the offences which may give rise to such an order, a limit on the duration of surveillance, detailed provisions of how data attained should be handled and destroyed, particularly where the accused has been discharged by an

[52] *Sunday Times v.UK* (1979-80) 2 EHRR 245.
[53] *Kopp v.Switzerland* (1998) 27 EHRR 91, *Valenzuela Contreras v.Spain* (1999) 28 EHRR 483.
[54] *Amann v.Switzerland* (2000) 30 EHRR 843, *Khan v.UK* (2000) 31 EHRR 45.

investigative judge or acquitted by a court.[55]

In *Huvig v.France* and *Kruslin v.France*[56] the court was given the chance to explain another point of what is meant by the term law as used in Article 8. Both cases concerned French nationals who complained against their government after having been subjects of telephone tapping and surveillance. Although there was a French law regulating surveillance, the Court found in both cases that there was a violation of Article 8, because this law was inadequate. The Court said that the term 'law' ought to be understood in its substantive sense and not in its formal one, in a sense that it does not include only traditional forms of law, but also both enactments of a rank lower than statute and unwritten law, provided of course that they meet the other criteria. This is indicative of the fact that the essence and content of a law in question are much more important than formalities. As a result, even though there was a law in these cases, it was considered inadequate due *inter alia* to the lack of adequate safeguards against various abuses, failure to define the conditions under which telephone tapping could be ordered, and lack of an obligation on the part of the judge to set a limit on the duration of the telephone tapping. As a general remark it can be said that in this series of cases, the Court has come to develop a quite clear image of how a government should apply surveillance in a way acceptable under the Convention.

3. Is the interference necessary in a democratic society?

When assessing the last condition, whether the measure in question is necessary in a democratic society to achieve the aim pursued, the Court applies a test of proportionality. *Leander v.Sweden*[57] was a case in which the applicant had been refused permanent employment as museum technician with the Naval Museum on account of certain secret information that allegedly made him a security risk. This case did not deal directly with surveillance; it rather sought to assess the legality of secret gathering of information by the government and refusal to disclose them in terms of national security. The court found no violation of Article 8, accepting that the interference was in accordance with law and sought to protect the legitimate aim of national security. It also accepted that it was necessary in a democratic society, which is a point it analysed further. The Court held that the notion of

[55] *Huvig v.France* (1990) 12 EHRR 528, par. 34, *Kruslin v.France* (1990) 12 EHRR 547, par. 35, *Valenzuela Conntreras v.Spain*, (1999) 28 EHRR 483, par. 46.
[56] *Huvig v.France*, ibid., par. 28, *Kruslin v.France*, ibid., par. 29.
[57] *Leander v.Sweden* (1987) 9 EHRR 433, paras. 58-60.

necessity implies that the interference corresponds to a '*pressing social need*' and, in particular, that it is '*proportionate to the aim pursued*'. The Court recognises that national authorities enjoy a '*margin of appreciation*' which varies according to the particular aim pursued and the nature of the measure in question. It also accepts that, when national security is at stake, this margin of appreciation is a wide one. Nevertheless, in view of the risk that a system of secret surveillance considerably undermines democracy on the grounds of defending it, the Court must be satisfied that there exist adequate and effective guarantees against abuse. In *Klass v.Germany*, when assessing the same condition, the Court stressed that states do not enjoy an unlimited discretion to subject persons to secret surveillance just because it is done for a legitimate reason. The condition of necessity implies that states may not adopt whatever measure they deem appropriate, and whatever measure is adopted, adequate and effective guarantees against abuse should exist. Assessment of the adequacy and effectiveness of the guarantees offered depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided for by national law.[58] The existence of a remedy is a very important factor. It is in principle desirable to entrust supervisory control to a judge, since judicial control offers the best guarantee of independence, impartiality and a proper procedure; however, other safeguards might also suffice, if they ensure independence and are vested with sufficient powers to exercise an effective and continuous control.[59]

The fact that the Court recognises that there should be a pressing social need indicates that a government should not base its actions on mere assumptions. There is no doubt, of course, that it would not be difficult for a government to persuade the Court that the social need pursued is indeed pressing, but the fact that the Court proceeds to such an assessment may make a government more cautious. Furthermore, the Court seems to consider the existence of adequate and effective safeguards against abuse a major priority when it comes to secret surveillance and other cases where a government enjoys a wide margin of appreciation, since it considers it necessary for both the conditions of quality of law and necessity in a democratic society to be justified.

[58] *Klass and Others v.FRG* (1979-80) 2 EHRR 214, par. 50.
[59] ibid., paras. 55-56.

Case-law on the interpretation of Article 8, par.2, and Article 10, par. 2

The first remark that can be made from the way the Court has applied Article 8, par.2 in the rest of the cases studied (meaning those not dealing with telephone tapping and secret surveillance) is that the reluctance of the Court to go into considerable detail when assessing whether a government has a legitimate reason to interfere with privacy is a general phenomenon. As already noted in the context of the previous group of cases, the Court does not seem to be eager to challenge governmental policies by questioning with persistence whether they were planned to serve a legitimate aim. It easily accepted, for example, without much discussion in *Lustig-Prean and Becket v.UK* and *Smith and Grady v.UK*, [60] that eliminating homosexuals from the army was indeed planned for the protection of national security. Preventing a gypsy from living in caravans on her own land, as was the case in *Buckley v.UK*,[61] was a measure taken for the preservation of public safety and the economic well-being of the country. The Court clearly prefers to focus its attention on applying the principle of necessity and proportionality. It is not accidental that the vast majority of the cases where violation of Article 8 was found were decided either on grounds of disproportionality or inadequacy of the existing law.

It is not suggested here that this reluctance of the Court is questionable or incorrect. Anyway, governments tend to present plausible reasons, as it would be naive to base their actions, at least expressly, on reasons of doubtful validity. It is, however, probable that had the Court been eager to criticise in further depth the legitimacy of the reasons presented, governments would have been more prudent when deciding whether there is a reason to interfere with privacy. There is no particular indication from the case-law of the Court as to how the terms national security, public safety or the economic well-being of a country could be defined. It can only be deduced that the terms comprise a wide range of cases and it would not be particularly difficult for a government to convince the Court that it had such a legitimate reason to interfere with on-line privacy.

The Court seems to counterbalance this tolerant attitude by being more demanding and strict when deciding whether the measure in question is necessary in a democratic society. It has

[60] *Lustig-Prean and Becket v.UK* (1999) 29 EHRR 548, *Smith and Grady v.UK* (1999) 29 EHRR 493.
[61] *Buckley v.UK* (1997) 23 EHRR 101.

formulated a consistent approach based on a considerable number of cases.[62] First of all, in *The Sunday Times v.UK*,[63] it ruled that the adjective 'necessary' is not synonymous with 'indispensable' or as flexible as 'reasonable' or 'desirable', but rather implies the existence of a *pressing social need*. In this case the publisher and editor of the *Sunday Times* complained about the interlocutory injunctions imposed by the English courts on the publication of details of the book *Spycatcher* and information obtained from its author. This was a book written by an ex-employee of the British Intelligence Services that revealed information concerning the operation of the Services. The UK government had sought to stop the publication of the book, both home and abroad, but it had failed to do so abroad. As a result the book was already in the public domain and, although not circulating in the UK market, could be easily obtained on-line or by a person travelling abroad. The Court failed to see a *pressing social need* to prevent the British public reading about something that was already in the public domain, concerned a matter of major interest to it and which the rest of the world was free to read by then. Perhaps what the Court really meant by this decision was that stopping people from reading something that was already in the public domain was not really a matter of national security (and in fact it was not), but it chose to avoid this route and take the safer one of saying that it did not serve a pressing social need, basing in this way its decision to a reasoning with a lesser political flavour. The Court seems to have developed this attitude as a practice: it generally avoids taking a political role by criticising on the reasoning presented by the governments as such, but in effect it is doing it through its judgement on necessity.

In *Barthold v.Germany*,[64] it said that the notion of necessity implies that the interference of which complaint is made corresponds to this pressing social need, in a sense that it is proportionate to the legitimate aim pursued and that the reasons given by the national authority to justify it are relevant and sufficient. Furthermore, the compromising measure taken should be efficient in that it indeed yields the awaited result. The Court recognises that it is for the national authorities to make the initial assessment of necessity, but the final evaluation as to whether the reasons cited are indeed relevant and sufficient is one for the

[62] See for example *Lustig-Prean and Becket v.UK*, (1999) 29 EHRR 548, *Smith and Grady v.UK* (1999) 29 EHRR 493, *Buckley v.UK*, ibid., *Berrehab v.The* Netherlands (1988) 11 EHRR 322, and cases on Article 10 *The Sunday Times v.UK* (1991) 14 EHRR 229, *Rekvényi v.Hungary* (Appl. no 25390/94) 20/05/1999, *Şener v.Turkey* (Appl. no 26680/95) 18/07/2000.
[63] *The Sunday Times v.UK* (1991) 14 EHRR 229, par. 67.
[64] *Barthold v.Germany* (1985) 7 EHRR 383, par. 55.

Court. A margin of appreciation is left open to contracting states in the context of this assessment, which is not identical in each case but varies according to the nature of the activities restricted and of the aims pursued. This margin of appreciation is wide when it comes to national security, as already mentioned before, but it also depends heavily on the degree of privacy that is at stake. For example, in cases where the restrictions in question concern 'a most intimate part of an individual's private life', like his sexual orientation (*Dudgeon v.UK, Lustig-Prean and Becket v.UK, Smith and Grady v.UK*) ,[65] the Court said that there must exist 'particular serious reasons' before such interference can satisfy the requirements of Article 8 par.2. The more privacy is at stake, the stricter the Court becomes in accepting interference. In *Vereinigung Demokratischer Soldaten Osterreichs and Gubi v.Austria*[66] it underlined that there is a link between the notions of 'necessity' and 'democratic society', the hallmarks of the latter including pluralism, tolerance and broadmindedness. In this case the Court had to decide whether the decision of the Federal Minister of Defence of Austria not to distribute in the barracks the first claimant's periodical and the second claimant's letter, in order to preserve order in the armed forces, was an infringement on their freedom of expression. The Court said that freedom of expression is also applicable to information or ideas that offend, shock or disturb the State or any section of the population. Having that in mind it ruled that the publications in question could scarcely be seen as a serious threat to military discipline, so the measure in question was disproportionate to the aim pursued and infringed Article 10.

The systematic approach and application of this condition dispels the impression formed at the beginning that a government could easily pass as acceptable an interference with privacy, under the pretence of pursuing one of the wide range of legitimate aims, given of course that it is in accordance with law. The Court may be unwilling to scrutinise the legitimacy of the aims pursued, but it is certainly not unwilling to apply the tests of necessity and proportionality effectively enough to combat abuse. As a result, a government may have a wide margin of discretion when deciding whether there is a need to interfere with privacy, but it has to be more cautious when deciding the degree of interference and the way it should be applied in each case. There is no plausible reason to believe that, were the Court to

[65] In *Dudgeon v.UK* (1981) 4 EHRR 149, par. 52, *Lustig-Prean and Becket v.UK*, (1999) 29 EHRR 548, par. 82 and *Smith and Grady v.UK*, (1999) 29 EHRR 493, par. 89.
[66] See *Vereinigung Demokratischer Soldaten Osterreichs and Gubi v.Austria* (1995) 20 EHRR 56, par. 36, *Dudgeon v.UK*, (1981) 4 EHRR 149, par. 41.

adjudicate on interference with on-line privacy, it would follow a different approach. This attitude indicates that the secret of finding the right balance does not lie on the decision to interfere or not, but on the exact measures that will be chosen to implement this interference.

4.5 Assessment

This chapter was an effort to explore the legal justifications on which governmental interference with on-line privacy can be based. The most usual reasons presented by governments to compromise otherwise protected rights and liberties are national security, public safety and the economic well-being of a country. Irrespective of the difficulties and disadvantages stemming from the lack of an operative definition of the terms, these reasons will probably be brought into play to allow interference with on-line privacy as dictated by the risks stemming from several forms of computer related criminality and the extended use of the Internet. Practical application of these justifications is not simple. Governmental interference is not accepted without limits just because there is a legitimate reason to justify it. At least in the European level the European Convention of Human Rights becomes relevant. On-line privacy is not of a lesser value than traditional privacy, so Article 8 will have to apply when deciding whether governmental interference can be accepted in each case. Therefore, the case-law of the European Court of Human Rights interpreting the conditions laid down by the Convention for acceptable compromise of privacy becomes of great utility.

In brief, if the ECHR model is to be followed, apart from being based on a legitimate reason, interference with on-line privacy will probably be accepted only when it is provided for in an adequately accurate, accessible and foreseeable law that provides effective safeguards against abuse. It should be dictated by a pressing social need and be necessary and sufficient to achieve the awaited result. A remedy against abuse should also exist which, if not judicial, should at least provide all the guarantees of independence and impartiality that are inherent in a judicial system of supervision and control. It is worth noting at this point that this test will be used later in the thesis (chapter 6) to assess the compatibility of the Regulation of Investigatory Powers Act 2000 with the ECHR.

Chapter 5

Regulating Cryptography: Encryption policies and their effect on on-line privacy

5.1 Preface

Cryptography and its use in the on-line environment is one of the most widely deliberated issues in contemporary discussions about cyberspace regulation. Even though encryption is an art with long-standing history, dating back to ancient Greece and Egypt,[1] it is becoming all the more important nowadays due to its unprecedented value as a unique tool for preserving security and privacy in the digital environment. Cryptography enjoys a special relationship with on-line privacy, being one of the few available technological tools that can enhance its effective protection. Encryption enhances the confidentiality, integrity and authenticity of messages and data transmitted through the Internet. Its basic effect is that data and communications stored or transmitted can be read only by their intended recipient or user (confidentiality), unless of course encryption is compromised by either breaking the code or giving away the secret key. It can also be used to make sure that private communications will remain unaltered during transmission (integrity). And last, it is used to provide security that the message originated from the alleged sender (authentication).

It has to be made clear at the beginning of the chapter that cryptography nowadays functions in three different levels: the military, the commercial (being a tool that enables e-commerce), and the one relating to the protection of individual on-line privacy. Although cryptography has a much wider use in the military environment than in the other two levels, its use for the protection of privacy is the most important for this thesis, although reference to the other two is unavoidable due to the interconnection between them. For the needs of the present study, cryptography becomes relevant for two basic reasons. First, since it enjoys a special relation with on-line privacy, any governmental effort to control its use and circulation would have a direct effect on the ability to protect on-line privacy; in other words regulating it is a form of

[1] See S Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, 1999 Fourth Estate - London.

interfering with privacy. Second, being a field where regulatory efforts have already been launched, it is proffered for discussing governmental interference with on-line privacy in a more pragmatic base.

5.2 Cryptography in the digital environment - uses and abuses

5.2.1 What is cryptography

The term cryptography comes from the Greek words *kryptos* which means 'hidden', and *graphia* which means 'writing'. It is the art of concealing data or communications by transforming them into an unreadable form before storage or transmission.[2] Cryptography is not about hiding the existence of a message itself (this is 'steganography', see further page 217); it is about scrambling its content in a way that can only be read by the intended recipient. This is achieved by using a code or - as it is otherwise called - a 'key' to encrypt and decrypt the message. Unless the code used is given away or broken, the encrypted message can be put into a readable form only by the intended recipient. In old-fashioned cryptography, codes had the form of a pre-agreed transformation technique; it was not necessary to have special knowledge in order to invent or break a code.[3] In the digital age codes have the form of binary numbers that undergo complicated mathematical operations in order to scramble and unscramble information. This qualitative difference underlines an important factor often neglected in contemporary discussions: cryptography is not a popular science any more, but involves the application of pure mathematics. One has to be a competent theoretical mathematician in order to study encryption and decryption in the digital environment, and even that is some times not enough.[4] This is an important element to keep in mind when discussing cryptography regulation; it would be wrong to assume that technical details are not important. Adequate appreciation of the scientific background is essential when trying to regulate its everyday use by less knowledgeable people. The fact that cryptography is not a product that can be easily developed and manufactured for mass

---

[2] See B Schneider, *Applied Cryptography*, edited by John Wiley, 1996.

[3] It is not suggested here that cryptology (cryptography and cryptanalysis) was not a respectable 'science' of its own. It certainly required special mental capabilities in order for a person to be a competent cryptographer. The utility of this comment is to underline the contrast between old-fashioned cryptography with the modern one that relies entirely on theoretical mathematics.

[4] See for example W Tuchman, "A Brief History of the Data Encryption Standard", in D E Denning and P J Denning *Internet Besieged - Countering Cyberspace Scofflaws*, ACM Press 1998, at pp. 289-291.

consumption should play a distinctive role in the process of adopting balanced rules for its use and circulation.

It is also worth mentioning that cryptography is not value-neutral. The science of information secrecy has been a field dominated throughout history by the military and intelligence communities; cryptography has been traditionally treated as munitions. This characterisation has overall been a successful one, since the ability to exchange diplomatic and military information securely or to decrypt the opponents' communications has proved a considerable advantage in the diplomatic and military affairs. During the Cold War, and especially during the 1950's and 1960's that spying was at its peak, the cryptographic and cryptanalytic potential of a country was one of the most important munitions in its artillery. This explains the secrecy by which the field of cryptography was covered until the 1970's. There has been a general desire to discourage public research, and although much research has been conducted by academics and others since the 1970's, previously very little appeared in the public domain.[5] Although the situation has considerably changed at present, this background gives an explanation for the attitude of governments towards cryptography and several policy choices in contemporary efforts to regulate its everyday use.

The 1970's were the time when the rapid development of the Internet commenced. Even though it was not until the 1990's that it broke through the narrow limits of the academic circles and became a popular medium (accessible to anyone with a computer and a modem), it quickly became apparent that the Internet was a field where cryptography would find new applications and play an important role. Nowadays, the exclusive character of cryptography as munitions belongs to the past; encryption technologies are increasingly integrated into commercial systems and popular applications.[6] As already said, it enjoys a special relationship with privacy as well.

However, cryptography should not be seen as a panacea to all on-line privacy related problems. Encryption, for example, may be used to make sure that the information you send to a merchant will not be intercepted on its way, but it can do nothing to prevent the

---

[5] See C Mitchell, "Cryptography: Key Distribution, TTPs and Warranted Interception", (An Occasional Paper published by the Global Transformation Research Group) 1999 Series, 2 / Jan. 1999, at p.7.

[6] See Y Akdeniz, "No Chance for Key Recovery: Encryption and International Principles of Human and Political Rights", 1998, available at <http://webjcli.ncl.ac.uk/1998/issue1/akdeniz1.html> (last visited on 23/04/2002).

merchant from misusing it himself.[7] Further, it can do nothing to prevent on-line monitoring of a person's activity on the Internet meaning the web-sites visited, the information downloaded etc. (web browsers with encryption features usually conceal the data you exchange through the Internet, i.e. a credit card number, but not Internet activity as such). It can, however, enhance the element of control on an individual's on-line privacy, basically when used as a tool to make sure that the content of communications or data travelling through the Internet or stored in digital form will remain unreadable by unintended eavesdroppers.

5.2.2 Symmetric and asymmetric, strong and weak encryption

Cryptography has many applications in the digital environment, especially since the Internet has transformed from an open academic network to a medium with commercial applications. It would not be an exaggeration to say that it has empowered electronic commerce since it permits secure transactions between companies and their clients. There are two kinds of cryptography currently in use: symmetric and asymmetric.

Symmetric-key cryptography, the first to be used and developed, uses a single key both for encrypting and decrypting a message. Even though it is quick in application and very secure when the key used is adequately big,[8] it has one major drawback: the secure dissemination of a secret key through an insecure medium. In other words, before using symmetric encryption for a digital communication, the parties have to use a different route to exchange the key (i.e. by the post or meeting in person), which is not always possible and diminishes the convenience of the Internet as a medium. This problem was solved by asymmetric or otherwise so-called public-key cryptography, a technique that uses two different keys in order to encrypt and decrypt a message. The basic theory is that the two keys are interactive in a way that the one can decrypt what was encrypted by the other and *vice versa*, but are also independent of each other in a way that the one can not be calculated from the other. One of the keys is kept secret (the 'private key'), and the other is published (the 'public key'). So

[7] See S A Brands, *Rethinking Public Key Infrastructures and Digital Certificates*, The MIT Press 2000.

[8] The strength of a cryptographic key depends on its length, the greater the number of bits the more difficult to break it. The strength of a key is measured by the time is needed for a computer to crack it by brute force attack, that is by trying all possible combinations. As computers become more quick and powerful, the number of bits that are needed to make sure that a key cannot be cracked in reasonable time becomes bigger. Keys that were considered secure 10 years ago, 56-bit for example can now be cracked fairly easily using powerful computers.

whenever A wants to send a secure message to B he encrypts it with B's public key, knowing that only B can read it by decrypting it with his (B's) private key. In that way, the problem of secure dissemination is solved. And for authenticity purposes, A can encrypt his signature with his own private key, so when B receives the message he can decrypt the signature using A's public key, knowing this way that it was A who sent the message.

Public-key cryptography was considered a breakthrough for the digital environment. It was initially proposed by Diffie and Hellman[9] as a theoretical concept to address the problem of key distribution. Its practical application, meaning the concrete algorithm that would implement this theoretical concept, was the work of three other scientists, Rivest, Shamir and Adleman. It is interesting to note that even though the above-mentioned people take all the credit for inventing public-key cryptography,[10] it had indeed been earlier invented by some mathematicians working for the British Intelligence Services, but it was kept secret as being extremely valuable for military applications. It was not until 1997, when public-key cryptography was well out in public, that this information was officially confirmed.[11]

Public-key cryptography has many applications, one of the most important being that of digital or electronic signatures, an extremely valuable authentication technique for commercial on-line transactions. Each person has a pair of signature keys, one secret and one public. When A sends a message to B, he uses his private key to encrypt his signature (that has the form of identification details for the needs of the digital environment). When B receives the message, he uses A's public key to decrypt the signature and put it in an intelligible form, making sure in that way that the message was originated by A, the sole possessor of the matching private key. The same technique is also used to check the integrity of a message, that is to make sure that its content was not altered during transmission. The major disadvantage of public-key systems is that they are slow in operation, much slower than symmetric encryption because they use larger keys, which makes them unsuitable for encrypting big amounts of data. This problem has already been solved; several systems have been developed that use a combination of symmetric and asymmetric cryptography to produce the best possible result. Asymmetric cryptography is used simply to exchange

[9] The Paper of W Diffie and M E Hellman that introduced the notion of public-key cryptography, "New directions in cryptography", IEEE Transactions on Information Theory IT-22 (1976), 644-655.
[10] And there is no doubt that they reached this result independent of any previous knowledge.
[11] For more details on the story of public-key cryptography invention see S Singh, *supra* note 1, pp. 252-297.

securely the symmetric key, which is the one used to encrypt the data or the message itself. This technique is known as the digital envelope, a well-known example being Pretty Good Privacy (PGP) developed by Philip Zimmermann.[12]

Apart from this technical distinction between symmetric and asymmetric, encryption is also divided into strong and weak. Strong encryption is the one that cannot be broken, in the sense that the time needed for a computer to find the matching key by a 'brute-force' search (by trying every possible key combination until one obtains a readable text) is so long that it makes it practically impossible. Weak encryption is the one that can be broken, meaning that the key can be found by a brute force attack within a reasonable amount of time. The strength of the encryption depends on the amount of digits making up the encryption algorithm: the more the digits, the less rapidly it can be decrypted and the stronger the encryption. For a sufficiently large key, a brute force search on even the most powerful super-computer could take longer than the life of the universe.[13] For the time being, 56-bit for symmetric and 512-bit for asymmetric encryption is the threshold between strong and weak encryption. It is important to keep in mind that this threshold is not permanent but changes according to the computer potential. The more powerful computers become, the quicker they perform mathematical operations, and the amount of time needed to decrypt a message by brute force attack diminishes. Until recently, a 56-bit symmetric encryption algorithm was considered strong, but now it can be broken within a reasonable amount of time.

The distinction between strong and weak encryption is very important; they both offer protection but on a different level. Weak encryption can provide sufficient protection against people or organisations that do not have the potential to break it, whereas strong encryption provides protection against everyone. A person using weak encryption, for example, can be almost certain that his communications and data will not be read by a simple competitor or by a system administrator or by a colleague using the same system. He cannot be certain, however, that his data will not be read by a governmental agency, either of his own or a foreign country, if it happens to attract any attention (i.e. if considered useful for a criminal investigation or for intelligence purposes). Governmental attitude against strong and weak encryption is therefore very different, especially in the US. It is obvious that weak encryption

[12] See W Diffie and S Landau, *Privacy on the Line - The Politics of Wiretapping and Encryption*, The MIT Press 1999, pp. 205-6.
[13] See Committee to study National Cyptography Policy, National Research Council (NRC), "Cryptography's role in securing the Information Society 96-97" (1996), at p. 63.

is harmless compared to strong, since it does not render information totally unintelligible. The attitude against weak encryption is much more liberal than it is against strong encryption. As will be later discussed, the use of weak encryption is not restricted at present in most of the countries, whereas several restrictions remain in force when it comes to strong encryption. Strong encryption is vital for military purposes and that is one of the major reasons why governments persist in controlling its dissemination.

5.2.3 Encryption uses and abuses

In the electronic environment the need for privacy-enhancing technologies is apparent and cryptography is certainly one of them. First of all, cryptography enhances or rather enables electronic commerce since it allows the secure exchange of transactional information and money through an insecure medium. Apart from that, it is also important for the integrity of electronic correspondence and the protection of personal communications. Cryptography can also provide anonymity as well as confidentiality, and allows human rights monitors to communicate without fear of persecution or reprisal. It also offers unprecedented security for the tremendous amounts of personal or confidential data stored nowadays in digital form. It is undoubtedly the phenomenal rise in the use of cryptography for commercial reasons that have prompted the need for a consideration of the legal regulation of cryptography and electronic signatures.[14] That is because, as the use of strong cryptography is becoming popular, it is almost certain that it will be used for illegal as well as legal purposes.

Cryptography can be a very useful tool in the hands of criminals who act in the digital environment. It can be used to conceal illegal operations (such as money laundering, tax evasion and child pornography) and it enables secure communications and exchange of information between criminals or terrorists, enabling them to evade law enforcement.[15] Additionally, being a technology with valuable military and intelligence applications, its unlimited use and distribution in public is seen by governments as a threat to national security and stability. It should be made clear that digital signatures and the use of cryptography for authentication purposes are not only a problem for law enforcement. On the contrary, they may prove helpful as an 'architecture' of identification in the anonymous by

[14] See M Hogg, "Secrecy and Signatures - Turning the Legal Spotlight on Encryption and Electronic Signatures", in L Edwards and C Waelde (editors) *Law & the Internet - A Framework for electronic commerce*, 2nd edition, Hart Publishing 2000, at p. 37.
[15] See D E Denning, "The Future of Cryptography", in B Loader (editor) *The Governance of Cyberspace*, Routledge London and New York 1997, pp. 176-7.

nature Internet environment.[16] The use of cryptography for confidentiality purposes is what makes law enforcement agencies uneasy, as it complicates investigation and prosecution of crimes.[17]

Regulating cryptography is apparently a question of finding the right balance between enabling valuable uses and eliminating possible abuses. Governments tend to focus on the latter, but the on-line privacy landscape may dictate a more complete approach. Let us see now the most significant cryptography policies and how they have affected or are likely to affect on-line privacy.

5.3 Regulatory efforts and their effect on on-line privacy

The regulatory efforts launched in order to control the use and dissemination of cryptography in the digital environment can be divided in two broad categories: export controls of cryptographic products (either hardware or software), and control of domestic use (mainly in the form of key-escrow schemes). Apart from having an entirely different history, these two categories have an equally different effect on on-line privacy, and as a consequence they will be viewed separately.

5.3.1 Export controls of cryptographic products: theory and practice

The first and certainly most successful category of measures adopted to restrain the development and wide use of encryption products is export controls, a measure targeting the availability of strong encryption by limiting its proliferation from the source of manufacture. Undoubtedly, it is weird to claim that export controls have been the 'most successful' measure in restraining the use of encryption, given the international proliferation on the use of encryption either by individual users or in the context of e-commerce and on-line transactions. However, this is not far from the truth since export controls are in effect the only measure that the states managed to adopt in order to delimit strong encryption. As will be subsequently analysed, efforts to adopt other measures, such as key-escrow, have failed in both sides of the Atlantic. The effectiveness and actual impact of these measures will be

[16] See L Lessig, *Code, and other laws of cyberspace*, Basic Books, 1999, pp. 34-5.
[17] See K W Grewlich, *Governance in Cyberspace - Access and Public Interest in Global Communications*, Kluwer Law International, 1999, at p. 173.

discussed at the end of this subsection, it is however worth noticing from the beginning that export controls have had and continue to have a not indifferent effect in the use of strong encryption by ordinary and law-abiding people.

The basic rationale for this policy is that, if manufacturing countries impose restrictions on the exportation of encryption products, the overall dissemination and circulation of strong encryption on the international level will be effectively limited. There is little doubt that international co-ordination and harmonisation are highly essential in order for this policy to be absolutely effective, since a single country can unilaterally have little effect on the world market. However, this is not an absolute assumption as the world production of encryption software and hardware is not evenly divided. For example, almost 70% of this production belongs to the US. This market share is sufficiently big to conclude that US export restrictions on encryption could have a considerable, even if not absolute, effect on the proliferation and free distribution of cryptography at an international level. Furthermore, since encryption is not a popular science, the sources of cryptographic products are very few and any restrictions can have a substantial effect on the overall availability of encryption.

Export controls are an indirect way of controlling and eliminating the use of cryptography. Delimiting the dissemination of strong encryption products by imposing restrictions and complicated procedures before they can circulate in the world market renders them less attractive for users and traders. Strong encryption products become less cost-effective both for consumers and manufacturers. A government study conducted in the US in 1996 showed that export controls in the US and other countries have considerably slowed the global market on encryption.[18] In addition to that, export controls can reduce the overall availability of encryption in common programs such as operating systems, electronic mail and word processors, especially those originating from American companies, who dominate the world market of hardware and software. The restrictions make it difficult to develop international standards for encryption and interoperability of different programs. Countries must develop their own local programs, which do not interoperate well, if at all, with programs developed independently in other countries. Targeted markets, in this way, become smaller, and companies and individuals become less interested in developing new programs because of

[18] See G G Yerkey, "Special Report: Export Controls: US Controls on Encryption Software Have Hurt Exporters, Government Finds", (1996) *International Trade Report*, Jan. 17, at 85 (referring to Government Report: A Study of the International Market for Computer Software with Encryption).

smaller potential profits.

The effectiveness of export controls has been adversely affected by the Internet; strong encryption programs can be easily downloaded from anywhere in the world within seconds. In any case it is far more difficult to implement effective controls in an environment with complete lack of physical borders. This possibility, however, has not worked as a complete remedy for the restrictive effects of export controls, since a considerable part of encryption applications depends on hardware that can only circulate internationally by crossing physical borders. Yet, it has conveyed another important result. The possibility of downloading strong encryption software through the Internet diminishes the effectiveness of controls in the free circulation of encryption, as a way to delimit their use to conceal illegal activity. Export controls on cryptographic products have been considered necessary in order to reduce, among others, the potential abuse of such products by criminals who use encryption to enhance their illegal operation by evading law enforcement. The kind of cryptography that is available through the Internet is adequately strong to cover the needs of criminals. Criminals are mainly interested in encrypting their communications and stored data that have an incriminating nature, in order to render them useless for law enforcement, even if intercepted or discovered. That can be easily achieved by software downloaded through the Internet.

However, commercial sites and monetary or governmental institutions, that keep precious databases with personal information and handle vast amounts of money through on-line transactions, need hardware infrastructure or specially designed software in order to operate securely. This is the kind of products most directly affected by export controls. Furthermore, legitimate users are deterred more easily than criminals from using strong encryption when its availability is restricted. The obvious result of encryption software freely circulating through the Internet while strict export controls still apply is a considerable reduction in the ability of such measures to limit the effective use of strong encryption by criminals, while at the same time managing to eliminate the circulation of the sort of encryption products that are needed for legal uses. In other words, it has an adverse effect on the *targeting* principle (page 63), according to which regulation should aim at the problem, avoid a scattergun approach and be effective and able to achieve the goal for which it was initially designed.

The Wassenaar Arrangement

It is difficult to present a brief and comprehensive picture of the existing export controls on

cryptographic products that apply throughout the world. Existing measures are not homogenous and they change rapidly in order to meet the altering needs of the global market. On the international level, export controls of cryptographic products are basically regulated by the *Wassenaar Arrangement,*[19] an agreement of 33 industrialised countries to control the export of conventional weapons and 'dual use' goods (meaning goods that can be used both for military and civil purposes). The WA is neither a binding international treaty nor a law; it merely sets out a framework for national policies by specifying the items to be subject to export controls on a Control List, which is implemented into national export control policies on a discretionary basis.[20] This means that participating countries are in effect free to differentiate their policies when they consider it appropriate, which results in a lack of uniformity in the overall picture of export controls. Roughly described, under the WA cryptography is considered a dual use technology and the exportation of encryption products requires a licence, unless it uses symmetric encryption of up to 56-bit or asymmetric of up to 512-bit of key length. In effect, weak encryption is not regulated by this Agreement. The exportation of mass-market symmetric crypto software and hardware up to a certain key-length is free, and so is the exportation of products that use encryption to protect intellectual property, or encryption software that is already in the public domain. Nothing is said about electronic exports via the Internet, a field that consequently remains unclear.[21]

The inclusion of cryptographic products in the Control List of the WA is increasingly becoming the subject of criticism for two major reasons. First, cryptography is a purely defensive technology in terms of military applications and as such it arguably does not fall under the scope of the WA, which seeks to control the proliferation of weapons and technologies with an offensive nature. Second, export controls on cryptographic products now have a detrimental impact on genuine civil transactions and applications, again contrary

[19] The *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual Use Goods and Technologies*, signed in 1995, henceforth referred to as WA. It replaced the *Co-ordinating Committee for Multilateral Export Controls* (COCOM), an international organisation for the mutual control of the export of strategic products and technical data from country members to proscribed destinations study of US and European , that was dissolved in 1994. The WA can be found at < `http://www.wassenaar.org` > (last visited on 14/06/2002).

[20] See S Andrews, "Who Holds the Key? - A Comparative Study of US and European Encryption Policies", (2000) *Journal of Information Law and Technology*, issue 2.

[21] See *Bert-Jaap Koops* homepage - Crypto Law Survey, Version 18.4, January 2001, available at <

to a basic principle of the WA that it is not supposed to impede *bona fide* civil transactions.[22] Whether these are viable arguments or not largely depends on political rather than legal factors. What can be said with relative certainty is that the WA, being a forum with a predominant military and intelligence orientation and strongly lead by US interests, does not provide guarantees that commercial and privacy concerns will be equally taken into account when the Control List is drafted. The encryption that can circulate freely according to the WA is not sufficiently strong to resist serious efforts to break it. But let us now turn to more specific approaches.

US Export Controls

The US, being the heart of software and hardware production, has been one of the countries with the strictest export controls on cryptography. Interestingly enough, it applies no restrictions in the domestic use, creation, or sale of encryption products. Exportation of cryptographic technology has a history of heavy restrictions[23] that were considerably relaxed only in summer 2000.[24] The main reason for this relaxation was the strong complaints by manufacturing companies about the adverse effect of these measures on the competitiveness of their products in the world market. The new regulations substantially loosened restrictions, and virtually all encryption products on the retail market can now be sold overseas after a 'one-time' government review.

The revised encryption export policy rests on three principles: first, the government should have an opportunity to conduct a technical review of encryption products prior to export; second, it should receive a post-export reporting with respect to some cryptographic

[22] See B Gladman, "Wassenaar Controls, Cyber-Crime and Information Terrorism" (A Report by Cyber-Rights and Cyber-Liberties UK, September 1998), available at <http://www.cyber-rights.org/crypto/wassenaar.htm> (last visited on 23/04/2002).

[23] Until 1996, many encryption technologies were classified as "munitions", based on the predominant military use of cryptography, and their export was forbidden under the Export Administration Regulation. In 1996, President Clinton transferred the regulation of all encryption technologies (as a dual-use good) to the Commerce Department, except those developed solely for military use. Under this regulation, it could take a significant amount of time for a company to obtain an export license and only very weak encryption products could be exported without a license. Relaxation begun in 1998, that the government started to allow the export of increased bit-length products and relief for certain industry groups, including US subsidiaries and insurance companies.

[24] On January 12, 2000 the US Department of Commerce Bureau of Export Regulation issued new encryption export regulations that removed most of the prior limitations on the export of US encryption technology. This policy was updated in July 2000, as a response to the EU's creation of a license-free zone. See R C Thomsen and A D Paytas, "US To EU: Me Too", available at <http://www.t-b.com/cryptoarticle.htm> (last visited on 23/04/2002).

products; and third, it should have the right to review and restrict - when necessary - exports to foreign government end-users.[25] Even though controls are now considerably relaxed compared to the past, and the US government has got rid of almost all licence requirements for exports of encryption products in the EU and some other specified countries (as a response to the EU's creation of a licence-free zone in June 2000[26]), several problems still remain.[27] First of all, the one-time technical review of encryption products prior to export makes the products unattractive to foreign consumers as well as privacy proponents. This review serves one of the objectives of export controls that goes virtually unnoticed: to maintain an ongoing assessment of the quality, availability and functioning of commercially supplied cryptographic equipment. Second, the highly technical nature of the restrictions makes it difficult to cope without employing especially skilled personnel, an expensive requirement, inexpedient for small businesses. And third, a licence is still required when the end-user of cryptographic products is a foreign government, a restriction with a wide range of applications since a lot of telecommunications and other companies in the global market are partly or entirely owned and controlled by governments. An overall assessment would suggest that the US government is trying to keep as much control as possible, without damaging the competitiveness of American products in the world market. If it had not been for the strong commercial lobbying, strict restrictions would still have remained. Privacy considerations and the need for availability of strong encryption products do not seem to be the prime concern with respect to the new policies. This is a rather pessimistic conclusion as far as on-line privacy is concerned; US policy choices seem to imply that its effective protection is not one of the major priorities.

Export Controls in the EU

On the other side of the Atlantic the situation seems to be slightly different. Even though all

[25] See US Department of Commerce, Bureau of Export Administration, Office of Strategic Trade & Foreign Policy Controls, Inf. Tech. Controls Division, "Commercial Encryption Export Controls - Questions and Answers", available at <http://www.bxa.doc.gov/Encryption/qanda.htm> (last visited on 23/04/2002).

[26] The EU Regulations (that will be subsequently examined) created a harmonised EU General Licence (Community General Export Authorisation) which covers the export of encryption items (except cryptanalytic items) within the fifteen EU member states and ten of its close trading and security partners: Australia, Canada, Czech Republic, Japan, Hungary, Norway, New Zealand, Poland, Switzerland and the United States.

[27] See T E Black, "Taking Account of the World as it will be: The Shifting Course of US encryption Policy", (2001) 53 *Federal Communications Law Journal* 289, at p. 306.

Member States of the EU are members of the Wassenaar Arrangement, they never enforced such strict controls on the exportation of cryptographic products as the US did. The EU, being the major competitor of the US in the global software and hardware market, rightly takes the credit of being partly responsible for the world-wide relaxation of export controls. Export of dual-use goods, including cryptography, is regulated by the *Council Regulation No 1334/2000*[28] (in force since 29 September 2000) that replaced the earlier 1994 Council Regulation *No 3381/94*.[29] In general, export within the EU is liberalised (with the exception of some highly specialised products, such as cryptanalytical items) and remaining export licensing procedures have been simplified. In order for a manufacturer to export to ten trading partners of the EU a Community General Export Authorisation can be applied for, which is valid for export from all EU countries.[30] For export to all other countries, a General National Licence can be applied for (except for cryptanalytical items), which is valid for export to one particular country. Otherwise, exporters have to apply for an individual licence. EU export controls are certainly more relaxed than their US counterpart, even after the recent changes in both parts. There is no need for either a pre-export technical review or a post-export reporting, and no further requirements when the end-user is a foreign government. Even though how Member States will implement the new Regulation still remains to be seen, as it leaves a small margin of discretion for them on how to apply the controls,[31] it is highly unlikely that they will impose strict technical requirements due to fears of diminishing the competitiveness of their domestic production.

The UK, being a member of the EU and the Wassenaar Arrangement, applies export controls that are in accordance with both the EU Regulations[32] and the agreement under the Wassenaar Arrangement. Currently in force are the Export of Goods Control Order 1994, as amended in 2001,[33] the Dual-Use Items (Export Control) Regulations 2000, as amended in

[28] *Council Regulation (EC) No 1334/2000 Setting up a Community regime for the control of exports of dual-use items and technology* (Official Journal L159, 30.1.2000), as amended by *Council Regulation 2889/2000/EC* (OJ L336, 30.12.2000), *Council Regulation 458/2001/EC* (OJ L 65, 07.03.2001), *Council Regulation 2432/2001/EC* (OJ L 338, 20.12.2001), *Council Regulation 8802/2002/EC* (OJ L 139, 29.05.2002).

[29] *Council Regulation (EC) No 3381/94* (amended by Regulation (EC) 837/95).

[30] The creation of a free-licence zone, see *supra* note 26.

[31] Art. 6, 2 (Export Authorisation) of the EU Regulation for example states that "The authorisation may be subject, if appropriate, to certain requirements and conditions, such as an obligation to provide an end use statement".

[32] *Supra*, note 28.

[33] Export of Goods Control Order 1994, SI 1191, amended by the Export of Goods Control Order (Amendment) 2001, SI 729.

2001 and 2002[34] (introduced to comply with the terms of the EC Regulation[35]) and the Export Control Act 2002, a more general law, which in effect gives the legal base for the Orders. Cryptography, as a dual-use item falls under these provisions. It is interesting to note that the New Dual-Use Items (Export Control) Regulations 2000 (that replaced the 1996 one) cover the export of items both in tangible and intangible form. Under the previous regulation exports of cryptographic technology on paper or on computer disc (tangible) were caught by the regulations, whereas export vial file transfer on the Internet was not (intangible). Now Internet transfers of cryptography will also be subject to export control.[36]

A substantive change, effected for the first time by recent amendments in the US and EU cryptography export control policies, is the explicit inclusion of cryptography transfer via the Internet under the existing controls. Prior to that, no explicit mention was made on whether export controls would equally apply to digital transfers. Now, both US and EU regulations state that transmission of cryptographic software and technology by means of electronic media should also be subject to the same controls. US websites, for example, are required to have reasonable and sufficient screening procedures to implement the existing restrictions on exports to foreign government end-users.[37] Further, Article 8 of the EU Regulation states that transmission of software and technology by means of electronic media, fax or telephone to destinations outside the Community should also be subject to controls. This is an important inclusion since, as already said, the free circulation of encryption software through the Internet is considered as a factor weakening the overall effectiveness of export controls. Additionally, it may prove an indirect way to control domestic use of strong encryption, if used as a justification to limit the availability of encryption on domestic Internet sites.

The effects of export controls on on-line privacy

This brings us to the effect that export controls of cryptographic products can have on on-line

[34] Dual-Use Items (Export Control) Regulations 2000, SI 2620, as amended by the Dual-Use Items (Export Control) (Amendment) Regulations 2001, SI 729, the Dual-Use Items (Export Control) (Amendment) Regulations 2001, SI 1344, the Dual-Use Items (Export Control) Regulations 2002, SI 50 and the Dual-Use Items (Export Control) (Amendment) (No 2) Regulations 2002, SI 2033.
[35] *Supra*, note 28.
[36] See M Hogg, *supra* note 14, at p. 52.
[37] This means that the website must be configured to check the Internet Protocol address of the person requesting the encryption product for transfer or download to ensure that the requester's address is not a foreign government domain name. In addition, the receiver of the encryption download or transfer must indicate that the software is not intended to be used by a government end-user. See Section 734.2(b)(9)(iii) of the new policy.

privacy. It is obvious by now that such controls are certainly not a direct way of regulating the use of encryption. Little doubt is left, however, that eliminating the availability and dissuading the development of strong encryption has indeed an indirect but considerable effect on the use of encryption and, as a consequence, people's ability to protect a serious aspect of their on-line privacy. Unfortunately, privacy concerns do not seem to have influenced policy choices on export controls on encryption, unlike commercial concerns that seem to have dictated recent changes in both sides of the Atlantic. Export controls are scarcely the target of public disapproval, other than from manufacturers, even in their strictest form, basically because they do not seem to affect domestic use of strong encryption, and they certainly never did so in a direct way. It is also true that export controls target the dissemination of strong encryption, whereas they do not affect weak encryption. Since weak encryption is enough to protect people from most of the dangers they would whish to avoid, one could argue that export controls are not a real problem for users. In addition to that, one could argue that apart from companies and banks, few people knowingly use encryption to protect their privacy anyway. Encryption may be widely used in the e-commerce to protect credit card transactions, but this is usually automatic, and even though the user is usually informed that a secure server is being used for the transmitting of credit card details, he has no real choice on whether to use encryption and how strong it should be. It is in the discretion of the on-line company and the user sometimes does not even notice that encryption is being used. However, even the limited number of people who knowingly use encryption for their on-line communications and activity does not mean that they are not entitled to a strong version. And anyway, once deciding to use encryption, why use the weak option as long as a stronger one exists?

It is worth noting that export controls were challenged in front of the US Courts in a number of cases between DJ Bernstein, an American scientist dealing with cryptography, and the US government.[38] Although these cases are not directly founded on privacy law but on freedom of expression, they remain very interesting because they have implications for on-line privacy as well. The legal battles began in 1995, when Bernstein was a graduate student at UC Berkeley. He had invented an encryption system called Snuffle, which he wanted to share with colleagues and students (both Americans and foreigners) by publishing the algorithm

[38] *Bernstein v. United States Department of State,* 922 F. Supp. (1996), *Bernstein v. United States Department of State,* 945 F. Supp. (1996). For an analysis of the cases see T Nguyen, "Cryptography,

and the source code implementing the system, and including it in his teaching material. He was denied permission to do so by the State Department on the grounds that his system was munitions and as such was subject to export controls. Bernstein challenged the decision of the State Department on the grounds that it infringed his freedom of speech as recognised by the First Amendment of the American Constitution. Both the District and the Appellate Court decided in favour of Bernstein, ruling that the State Department was indeed infringing his freedom of speech in the academic context by denying him permission to publish and teach his work. Even though the US government changed the regulations on export controls of encryption (partly as a response to this decision), Bernstein continues to challenge the new regulations on the grounds that they still hinder academic intercourse. The new regulations require, for example, that whenever scientists disclose something new to a foreign colleague they simultaneously send it to the government, which makes in-person collaboration practically impossible.[39] It remains to be seen whether the Court will rule again in favour of Bernstein, or it will accept that the amended regulations meet the requirements of the Constitution.

Export controls on cryptography have a peculiar nature in respect of their effect on on-line privacy. Those implemented by the US, for example, affect the privacy of foreign nationals in a greater extent and much more directly than they affect the privacy of US nationals. Windows, for example, the Microsoft operating system that dominates the world market, circulates outside US in a less secure version. US citizens, on the one hand, have no reason to complain, as long as they can buy the more secure version, and foreigners, on the other, can do almost nothing to change US domestic policy. Of course there is an indirect way to influence US policy choices, and that is by harming the competitiveness of US products in the world market through the implementation of more liberal policies abroad. This is what was recently achieved by the EU, whose liberalising policy left little choice for the US government but to relax export controls to a considerable extent. Arguably, if it had not been for the various valuable uses of cryptography for commercial applications, such products would still be subject to strict export controls. But export controls also affect domestic use of

---

Export Controls, and the first Amendment in Bernstein v. United States Department of State", (1997) 10 *Harvard Journal of Law & Technology* 667.

[39] See Electronic Frontier Foundation (EFF), "Professor pushes for revised encryption regulations", January 7 2002, available at <http://www.eff.org/Legal/Cases/Bernstein_v_DoJ/20020107_eff_pr> (last visited on 23/04/2002).

strong encryption in an indirect way. In order to comply with export controls, industries have to implement double standards in their production and produce two different products: one with strong encryption for the domestic market and one with weak encryption for the export markets. Given the fact that this is not always economically expedient, especially for smaller companies, many of them choose to produce one product to cover both markets, which is of course the one with the weak encryption. As a result, domestic users are also affected.

The significance of strong encryption for the effective protection of on-line privacy seems to have been neglected by governments, whose main concern is to control the widespread deployment of cryptographic systems of sufficient strength to present a serious barrier to traffic selection or a military advantage to possible opponents.[40] Governments, however, are not only supposed to allow development but as already discussed in the first chapter, also have a positive obligation to afford the means necessary to preserve on-line privacy. Export controls seem to have worked as an indirect way of overlooking such obligations.

5.3.2 Controls on the domestic use of encryption

Regulating (and restricting) the domestic use of encryption as such is of course a much more direct way of controlling cryptography and its utilisation for the protection of on-line privacy, than export controls. That is certainly why the overall effort to limit and control the use of strong encryption as such has been less successful, if at all, than the implementation of export control measures. People's rights and interests are offended more directly when their ability to use strong encryption is compromised. Before proceeding any further, it should be mentioned that a considerable part of the regulatory issues concerning the use of encryption has to do with digital signatures, notably their legal validity or the liability of Trusted Third Parties or Certification Authorities who administer their issuing. The regulation of the use of cryptography for authentication purposes, however, has little relation to and effect on the protection of on-line privacy, so these legal issues will not be addressed here.

Key-escrow / key-recovery: the unsuccessful efforts to impose it

As already discussed, one of the major factors that serves as a justification for governments to interfere with the unhindered use of strong encryption is its potential use by criminals and the

[40] See W Diffie and S Landau, *Privacy on the Line - The politics of Wiretapping and Encryption*, MIT Press 1999, at p. 107.

subsequent inability of law enforcement agencies to investigate and prosecute crimes, where encryption has been used to conceal valuable investigatory information. Consequently, any regulative effort will be assessed by its effectiveness in deterring such negative results of strong encryption, without hindering legitimate uses more than absolutely necessary. Key-escrow or key-recovery, a scheme designed to prevent such abuses, was a concept conceived and promoted by the US government, whereby users would be able to use strong encryption in their systems, as long as the keys used would either be deposited to a third party, such as a governmental agency or a specially authorised company, or developed by the government which would retain in possession the necessary information to enable decryption. A 'back door' would thus be created that would guarantee immediate access to encrypted data or communications for law enforcement agencies, when considered essential for the investigation of criminal behaviour.

Beginning with the Clipper Chip in 1993,[41] the US government made more than one effort to impose such a mechanism, but they were all unsuccessful, at least until the present. The US also tried to promote this policy outside its territory, although unsuccessfully, in an effort to influence the world-wide status of strong cryptography. That effort was launched because a key-escrow scheme would be insufficient to deal with the overall problem of digital crime if enforced unilaterally. The adoption of an escrow policy was strongly lobbied for by the US government in international forums such as the Wassenaar Arrangement, the Organisation for Economic Co-operation and Development (OECD) and even the EU, but it was entirely rejected by them, mainly due to privacy concerns, and partly as a reaction to the US effort to impose its own policy aspirations.

The UK government, rather inspired by the US endeavour, also made some serious efforts to impose key-escrow but none of them was crowned with success.[42] These efforts started back in 1996, when the Department of Trade and Industry (DTI) published a discussion paper *On*

[41] At the beginning of the 90's the US government became concerned about the marketing of a secure telephone system by AT&T, that was finally persuaded to withdraw its product. In its place the US government offered NSA "Clipper" chips for incorporation in secure phones. The chip would be manufactured by NSA, who would also record Built-in keys and pass this information to other government agencies for storage or retrieval. This proposal was abandoned because it proved extremely unpopular. In its place, the US government proposed that non-government agencies should be required to keep copies of every user's key.

[42] For a detailed version of this "story" see Akdeniz, Y. and Walker, C. "Whisper who dares: encryption, privacy rights and the new world disorder" in Akdeniz, Y., Walker, C. and Wall, D. (eds) *The Internet, Law and Society* (Longman, Harlow, 2000).

Regulatory Intent Concerning Use of Encryption on Public Networks.[43] The government proposed the introduction of the licensing of Trusted Third Parties (TTPs) who would hold the copies of all private encryption keys to facilitate key recovery and verification. From then on, a key-escrow scheme was incorporated in a number of Consultation Papers and Policy Statements, but the most serious effort was its inclusion in a proposed legislation in 1998, the Electronic Commerce Bill, the aim of which was to make the UK the most favourable place for e-commerce.[44] This plan was heavily criticised and fought against by the House of Commons (who set up a Select Committee to investigate the issue of electronic commerce),[45] the industry sector, non-governmental organisations and groups championing cyber-rights and liberties and the Data Protection Registrar. The debate came to an end by the DTI Command Paper, *Promoting Electronic Commerce*, which incorporated draft legislation that has now become the Electronic Communications Act 2000.[46] The plans for compulsory licensing of Trusted Service Providers were replaced by a voluntary 'approvals regime' in which the industry itself was to adopt self-regulatory measures.

It is true that key-escrow has a lot of flaws as a scheme to deter the negative effects of strong encryption in the prosecution of crimes. First of all, such a scheme has to be obligatory in order to be a little, if at all, effective. It is naive to assume that criminals and law-evaders will deposit their keys with governmental agencies, if they have a legal option not to do so. Even if it was made obligatory, there is still no way of guaranteeing that outlaws will compromise their keys, as they will probably choose to use more conventional means of protection than to face potential prosecution. As a result, the major effect of a key-escrow scheme would be a detrimental one, namely a restriction on the legitimate users' ability to protect their on-line privacy in absolute terms. There are two reasons for that. First of all, lawfully acting individuals would be completely exposed in the eyes of their government. Acceptable though it may seem, this is a negative rather than a positive outcome, since such a system creates a great potential for exploitation by, for example, corrupt employees or governmental

[43] Department of Trade and Industry, *On Regulatory Intent Concerning Use of Encryption on Public Networks* (DTI, London 1996 available at <http://dtiinfo1.dti.gov.uk/cii/encrypt/>).
[44] See DTI, *Our Competitive future: building the knowledge driven economy* (Cm. 4176, Stationery Office, London 1998), DTI, *Net Benefit: The Electronic Commerce Agenda for the UK*, DTI/Pub 3619 October 1998, DTI, *Building Confidence in Electronic Commerce*, 1999, available at <http://www.dti.gov.uk/CII/elec/elec_com_1.html>.
[45] This Committee published two reports lobbying against key-escrow. See House of Commons Select Committee on trade and Industry, *Report on Building Confidence in Electronic Commerce* (1998-9 HC 187, *Electronic Commerce* (1998-9 HC 648).
[46] DTI, *Promoting Electronic Commerce* (Cm. 4417, Stationery Office, London 1999).

authorities, even when adequate guarantees exist. Apart from that, it opens up dangerous possibilities for state control over its citizens. This may seem an exaggerated concern for a state under democratic governance, but it may prove a very real scenario, were things to change (there are nowhere absolute guarantees that a totalitarian government could never take power). Second, there is a serious danger of abuse by criminals; the concentration of great amounts of cryptographic keys constitutes a very attractive target for people who would be willing to misuse them for illegal purposes (such as theft of confidential information or property). In addition to that, there are serious concerns as for the operational complexity and cost-effectiveness of such a scheme, unavoidably weighty issues when deciding to adopt a certain policy.[47]

Even though the US government failed to pass all its key-escrow proposals, both in the interior and abroad, it cannot be said with certainty that such a scheme will not become legislation at some point in the future. In 1999, for example, the Clinton Administration submitted a new law for transmittal to Congress, the Cyberspace Electronic Security Act (CESA), that, even though adapted to address expressed concerns, was very reminiscent of the previous escrow proposals.[48] Having relaxed export controls, the then administration probably thought it would be easier to make such a scheme acceptable, especially to powerful industry groups. Even though CESA never became law, and is doubtful whether it will ever be, especially after the Presidential administration changed hands in 2001, it is indicative of the fact that the use of strong cryptography is not a forgotten issue for the US government, which seems to be turning its focus on enabling law enforcement access to decryption keys rather than limiting the use of strong unescrowed encryption. Especially now, after the events of September 11 2001 that initiated strong speculation on how encryption might have helped the terrorists plan their attack and communicate between them, it is highly probable that the attitude against the use of strong encryption will become less liberal. However, it is more probable that future policies will focus on the retention of communications data for longer periods of time and the possibility to access decryption keys, rather than restriction on the use of strong encryption as such. That is because, since strong encryption is out in public, there seems to be no way back.

---

[47] See R Anderson and others, "The Risks of Key Recovery, Key Escrow & Trusted Third Party Encryption", A Report by an ad hoc Group of Cryptographers and Computer Scientists, at <http://www.cdt.org/crypto/risks98/> (last visited on 23/04/2002).

[48] See T E Black, *supra* note 27, at p. 311.

A survey conducted in 1999 by EPIC[49] showed that most countries around the world do not restrict the domestic use of encryption by their citizens, and of those who do, few are democracies and most have authoritarian governments. The 1997 OECD Guidelines on Cryptography Policy and the European Commission both rejected the idea of key-escrow and expressed strong support for the unrestricted development of encryption products and services, which seems to have had a strong influence on the global status of controls in the use of encryption.

OECD Guidelines on Cryptographic Policy and their effect on encryption policies

In 1997 the OECD, in an effort to prevent future obstacles to international trade and commerce resulting from divergent national cryptographic policies, issued its *Guidelines on Cryptographic Policy*. These are made up of eight basic principles that were supposed to be respected by countries when regulating cryptography. These Guidelines do not have a binding nature for participating governments; their status is that of a soft law. However, they are an important indication of what the international forum would consider as acceptable principles of controlling the use of encryption. To the surprise of many, and especially the US, which used its power in an effort to persuade the OECD to include key-escrow or key-recovery in the Guidelines, there is no direct reference to such a concept. The principles are more of a general nature. Let us take a look at some of them.

According to principle 2, users should have the right to choose any cryptographic method they want, subject to applicable law. This last sentence (subject to applicable law) may seem to leave room for restrictions, but the Guidelines explicitly suggest that the term 'subject to applicable law' should not be interpreted as implying that governments can or should initiate legislation which limits user choice; it should rather remain unaffected. Principle 5 recognises that the fundamental right of individuals to privacy, including secrecy of communications and protection of personal data, *should* be respected in national cryptography policies and in the implementation and use of cryptographic methods. This is a very important principle, since it explicitly recognises the vital role that cryptography plays for the protection of on-line privacy. It is, in addition, interesting to note the use of the word 'should' in this principle, especially when considered in combination with the use of the

[49] Electronic Privacy Information Centre, Washington DC, "Cryptography and Liberty 1999 - An International Survey of Encryption Policy", available at <http://www.gilc.org/crypto/crypto-survey-99.html> (last visited on 23/04/2002).

word 'may' (rather than 'should') in the next principle. Principle 6 states "national cryptography policies 'may' allow access to cryptographic keys or encrypted data"; furthermore, it concludes that these policies 'should' respect the other principles of the Guidelines to the greatest extent possible. Since *should* is a stronger word than *may*, a construction of this combination of words seems to suggest that the protection of privacy is a heavier duty, one that should be taken into serious account when deciding to limit the use of encryption.[50] Overall, the major importance of the Guidelines is that it was recognised (for the first time in international level) that respect for individual privacy in emerging technologies is a value not to be compromised without adequate justification. The exact limits of potential governmental interference are not adequately defined; it is, however, obvious that the whole approach seems to be conscious of the potential risks for individual privacy, stemming from restrictive policies such as the elimination of the use of strong encryption. Still, it is doubtful how influential these principles can be, given the status of the *Guidelines* as a soft law with non-binding nature.

EU policy on the domestic use of encryption

The EU has also played an important role in rejecting restrictions on encryption. With the release in 1997 of a Communication from the Commission, *Towards a European Framework for Digital Signature and Encryption,*[51] it has chosen a direction away from key-escrow. The EU examined the idea of implementing such a scheme, but it has come to the conclusion that it would not prevent criminals from using strong non-escrowed encryption, and it would be difficult to implement, very expensive to maintain, and involve high security risks. The Communication also points out the privacy concerns of encryption policies, recognising that the debate about the prohibition or limitation of the use of encryption directly affects the right to privacy and its effective exercise, a right guaranteed by many legal documents in both national and international level. So even though the EU has chosen to regulate the legal issues arising from the use of encryption for authentication purposes,[52] it chose to do nothing to restrict domestic use of strong encryption.

---

[50] See Y Akdeniz, "No Chance for Key-Recovery: Encryption and International Principles of Human and Political Rights", (1998) *Web Journal of Current Legal Issues* 1, at <http://webjcli.ncl.ac.uk/1998/issue1/akdeniz1.html> (last visited on 23/04/2002).

[51] COM (97)503, 10 October 1997, available at <http://www.droit.fundp.ac.be/textes/EurFram.pdf> (last visited on 23/04/2002).

[52] See the *Directive on a Community Framework for Electronic Signatures*, Dir. 1999/93/EC.

The outcome of all these policy choices is that key-escrow has not been adopted as an international standard of regulating encryption that would have rendered it obligatory for all cryptography users. Non-obligatory schemes do exist, of course, and they are mainly used by those who feel more comfortable with the idea of entrusting their keys to a third party, such as big companies, who may dislike the idea of their employees being the sole administrator of valuable encryption keys. Non-obligatory key-escrow has no adverse effect for on-line privacy, since it respects the element of choice in deciding how far one's privacy needs protection and what compromise one is ready to accept.

However, since non-obligatory key-escrow does not solve the problem of the potential use of cryptography by outlaws to circumvent law enforcement, the latest regulatory efforts seem to focus on another direction: that is enabling law enforcement agencies to demand the disclosure of decryption keys. This policy is based on the idea that, as long as people are free to use strong encryption, the only way to address the adverse effects of possible abuse is by giving law enforcement agencies the ability to demand the disclosure of plaintext or the decryption keys themselves, when it is considered necessary. Although this policy has no direct effect on the use of encryption itself, its indirect effect should not be underestimated. The way access to decryption keys is substantially regulated may well affect people's choice to use encryption in the first place. For example, if refusal to comply with a disclosure demand becomes a criminal offence on its own, several criminals may choose to be convicted under such a charge, rather than reveal evidence that would support a heavier conviction. Law abiding individuals on the other hand may choose to use other measures of protection. People may overall be deterred from using strong encryption, if the conditions under which decryption can be demanded are not sufficiently clear. The non-existence of strict safeguard provisions against abuse may also have the same dissuasive effect. Another influential issue is whether decryption of the document in question, without disclosing the actual key, would be considered sufficient for law enforcement needs.

It is not long since efforts to control encryption begun to turn towards this direction. The sole collective effort can be found in the 2001 *Council of Europe's Convention on Cybercrime*,[53]

[53] The Council of Europe is a 41-member Intergovernmental Organisation, not exclusively of European Countries, whose treaties are not directly applicable in national law. The final version of the Convention can be found at <http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm> (last visited on 23/04/2002).

a convention aiming to lay out a legislative model of how combating cybercrime should be regulated by contracting states, and allow the co-operation between law enforcement agencies in the investigation and prosecution of cybercrime. The final version of the Convention was adopted in November 2001, but is not yet implemented by the signatory states. Cryptography is not directly referred to, but Article 19 of the Convention says that contracting states should take legislative measures to make sure that their competent authorities can order, for the purpose of criminal investigation, any person who has knowledge about, *inter alia*, measures applied to secure the computer data to provide all necessary information to enable investigation. These measures include cryptography, although the text is not quite clear as to whether it refers to a decryption order or to the handing over of decryption keys. It is left to participating states to decide the details of enforcing this provision, making sure that the conditions and safeguards that exist under national law are respected. Although the inclusion of key-escrow was a possibility earlier on,[54] the final text does not contain anything to suggest that such a scheme should be adopted. Law enforcement access to decryption keys is becoming the trend in national legislation. The UK has just enacted a new law, the Regulation of Investigatory Powers Act 2000, the subject of the next chapter that addresses this issue in much detail. This direction seems in principle to be more privacy-friendly, since it is not directly affecting people's choice to use strong encryption, unless of course regulatory details of substantive issues have such a result.

5.4 Assessment

The effect that direct regulation of the use of encryption can have upon on-line privacy is much more explicit and imminent than that of export controls. Given the fact that encryption is one of the few available technological tools to protect on-line privacy, any restriction on the potential to use strong versions of encryption eliminates people's choice on how far to let their privacy be exposed. Both reduction in the availability and restriction in the use of strong encryption have a much more detrimental effect for law-abiding users than for those with criminal intentions. That is because strict regulation is likely to vest the use of cryptography with a negative preconception that its major value rests on its potential to hide something suspicious, and stigmatise cryptography as something used particularly by outlaws. Such a

[54] According to the 25 November 1998 *minutes* of the EU's Legal Advisory Board, it was unclear "whether the convention will contain any provisions on escrow of encryption keys".

preconception will put off simple users, while it is arguable whether it can have any positive effect on eliminating the adverse consequences of criminals using encryption. As it was successfully said: if we outlaw encryption only outlaws will use it.[55] Anyway, it is still arguable whether and how far law enforcement is indeed hindered by the use of strong encryption. Most available data show that in most of the cases where strong encryption was used, law enforcement agencies were still able to prosecute the perpetrators successfully.[56]

After having a look at the recent changes in the policies analysed, cryptography seems to be on the way to liberalisation and not restriction. It remains unknown, however, how many of the cryptographic products that we have today can be cracked by powerful intelligence agencies. NSA and other agencies around the world are known to develop cryptanalytic techniques as soon as a new encryption possibility becomes publicly available. Such researches are not made public, of course, because it is in their being kept secret that the diplomatic and military advantage of a country depends. The regulation of cryptography goes far beyond the limits of being a mere legal issue; its strong political character seems to render privacy concerns a secondary issue.

What becomes obvious from the cryptography policies presented here is that governments around the world, and especially those with the power to influence international standards such as the US or the EU, possess the capacity to interfere with on-line privacy and they certainly have done so through the implementation of export control policies. However, it is interesting to note that the effort to restrict the use of strong encryption directly has overall been less successful than export controls, which seem to have a rather indirect effect in the availability (and therefore ability to choose) strong encryption. Since the aim of this thesis is to identify the limits of governmental interference with on-line privacy, what can be inferred from this chapter is that, at least when it comes to the issue of encryption, privacy concerns and the needs of the global Internet community do manage to dictate some borders as to how far interference can go. First of all, it is practically impossible to prevent the use of encryption once it has been released to the public. Apart from protecting on-line privacy, encryption plays a vital role for electronic commerce that is becoming more and more popular, at least in Western societies. The need to safeguard the smooth and safe functioning

[55] See W Diffie and S Landau, *supra* note 40, p. 5.
[56] See B J Koops, *The Crypto Controversy - A Key Conflict in the Information Society*, Kluwer Law International 1998, at pp. 90-91.

of e-commerce requires allowing the development of strong encryption products. This is a point where governments would need to interfere positively in order to allow the use of effective encryption for the needs of electronic commerce. Second, the fact that eliminating encryption would prevent its misuse by criminals and law evaders has become an argument with a diminishing power. Strong encryption can of course be very useful in avoiding law enforcement, but it is certainly not the only way. Once its use becomes restricted, criminals will probably find another way to conceal illegal activity. This may seem to be an oversimplification, but it is very close to the truth. As an example, it was already discussed in the second chapter that the perpetrators of the 9/11 2001 attacks in America seem to have used very conventional methods to conceal their communications and planning on the attacks, even though there was strong speculation at the beginning that encryption must have played a vital role. Furthermore, the fact that law enforcement does have the power to investigate crimes even in cases where strong encryption has been used, as many cases of paedophiles have shown, indicates that encryption is not the only problem and restricting its use would not be a panacea for criminal on-line activity. Finally, given the fact that on-line privacy is a right that users need to make positive efforts in order to preserve, they should not be deprived from the means that enhance effective protection.

Chapter 6

The UK Regulation of Investigatory Powers Act 2000: Assessing a paradigm of governmental interference with on-line privacy

6.1 Preface

Even though on-line privacy and its conflicting interest with the need to control the on-line environment in order to prevent or confront potential abuse, is becoming all the more important, there are few concrete legislative efforts that purport to have a direct effect on this issue. One of the most interesting cases is the UK Regulation of Investigatory Powers Act 2000 (RIPA), a recently enacted statute, to be fully implemented by the end of 2002. This legislation has quite a long history. Its roots go back to 1996, when the first governmental initiatives to regulate on-line security through the control of encryption services appeared. This effort went on for a few years through several proposals, with the *1999 Electronic Commerce Bill* being the main one. This Bill finally became a law during 2000, leaving out the provisions referring to surveillance that had become the target of severe criticism. As an alternative, surveillance provisions were incorporated in the RIPA, as the official rationale of this statute was thought to offer a far more satisfactory background to render them publicly acceptable.[1]

RIPA's official objective was to regulate surveillance powers in general, so as to bring UK law in conformity with the European Convention of Human Rights, after the latter had been incorporated into UK law by the Human Rights Act 1998 (brought into force on the 2nd of October 2000). It also sought to update investigatory powers and extend them so as to cover the new technological landscape, namely the Internet and electronic communications. RIPA completed its passage through the Commons and the House of Lords on 13 July 2000, and received Royal Assent on 28 July 2000. Some parts have been in force since October 2000,

[1] For a short description of the history of the regulation see The British Chambers of Commerce, "The Economic Impact of the RIP Bill", June 12 2000 (an independent report), available at <http://www.britishchambers.org.uk/newsandpolicy/downloads/lsereport.pdf> (last visited on 23/04/2002).

and the rest by the end of 2002. There is no doubt as to the good intentions of the government to update UK legislation in order to meet the changing needs of society and law; it is certainly a positive step that had to be taken. However, some uncertainty remains as to whether this effort was accomplished in the optimum way. Notwithstanding the government's efforts to present RIPA as a step towards making sure that investigatory powers are used in accordance with human rights, it has been the subject of intense criticism as to whether it manages to respect the needs of on-line privacy, and the requirements laid down by the European Convention of Human Rights and case law of the respective Court for interfering with privacy.[2] It has to be pointed out that the views on that subject are quite polarised, which also explains the nature of the sources used for the writing of this chapter. Since the statute is quite new, there are very few articles or commentaries from independent scholars. Most of the references come from organisations or individuals who are either pro-cyber-liberalism and express strong criticism of the law, or governmental sources who are favourably predisposed to the positive outcome of RIPA. The intention here is to present an objective opinion (to the extent that this is possible) on how RIPA affects on-line privacy.

The Act is divided in five parts: Part I regulates the interception of communications, chapter 1 of this Part deals with the interception as such (in force since October 2000), while chapter 2 regulates the acquisition and disclosure of communications data (its implementation due in mid 2002), Part II addresses the issues of surveillance and covert human sources (in force since October 2000), Part III deals with access to encrypted data (its implementation due in mid 2002), Part IV regulates scrutiny and Part V contains miscellaneous provisions. Even though it is rather early to assess RIPA and its overall effectiveness as an effort to balance law enforcement needs with individual privacy rights, several points can already be made as to how far the regulation has succeeded or failed in taking into account the special needs of privacy as they are gradually being shaped by the on-line environment. The purpose of this

[2] See for example "Open Letter by Amnesty International to Members of the House of Lords on the RIP Bill", at <http://www.fipr.org/rip/AmnestyRIPletter.htm> (last visited on 23/04/2002), "STAND's Guide to the RIP v1.0", at <http://www.stand.org.uk/ripnotes/> (last visited on 23/04/2002), Data Protection Commissioner, "Response of the Data Protection Commissioner to the Government's Regulation of Investigatory Powers Bill", at <http://www.fipr.org/rip/DPCparlRIP.htm> (visited on 23/04/2002), "Advice Paper on the RIP Bill(In the Matter of a Human Rights Audit for Justice and FIPR", by Justice Tim Eicke of the Essex Court Chambers, at <http://www.fipr.org/rip/ripaudP3.html> (visited on 01/09/2001), "A Further Open Letter to the House of Lords from Cyber-Rights and Cyber-Liberties (UK) concerning the Regulation of Investigatory Powers Bill" (29 June, 2000), at <http://www.cyber-rights.org/reports/hl-let2.htm> (visited on 26/04/2002).

chapter is not to provide a detailed assessment of RIPA as a whole (since not all issues arising are relevant for the present study), but to focus on those points that have a greater effect on people's ability to protect and control their privacy in the on-line environment. Part II, for example, which regulates Surveillance and Covert Human Intelligence Sources, is not going to be analysed, since it has no particular effect for on-line privacy. The five principles of good regulation (chapter 2, page 63) will be used as criteria for assessment, not to judge the Act as a whole but as a regulation affecting on-line privacy.

Before turning to a separate analysis of the several parts, I consider it important to point out that the Act contains a number of provisions for secondary legislation where the scope, intent and safeguards of the delegated powers are insufficiently set out in the statute (Section 71 lays out the issuing and revision of codes of practice, Section 78 the issuing of orders, regulations and rules). This renders it more complicated to assess whether some of the provisions will, in fact, operate in a way that is privacy-compatible, since most of these documents have not been written at all or are not in their final form yet.[3] It also has to be pointed out that in analysing Part I chapter 2 of RIPA about the acquisition and disclosure of communications data, it is necessary to cover Part XI of the Anti-terrorism Crime and Security Act 2001 as well, which regulates the retention of communications data and operates as a complement to Part I chapter 2 of RIPA.

6.2 Interception of Communications

Part I, chapter 1 of RIPA regulates the interception of communications by laying down the terms and conditions to be respected and the procedure to be followed in order for an interception to be legal. The new Act extends the interception of communications regime to cover not only public but also private communications services, whereas the previous legislation (the Interception of Communications Act 1985[4] that was repealed by RIPA) affected only the Post Office and public telecommunications operators. Of course, it is worth noting that RIPA does not cover interception of communications on wholly private networks, as the definition of 'private telecommunications system' requires that there be a connection to a public system (Section 2). This means that systems such as, for example, an internal

[3] See "Regulation of Investigatory Powers Bill - Secondary Reading Briefing", available at <http://www.fipr.org/rip/Justice%20RIP%20Bill%202nd%20reading%20brief.pdf> (visited on 26/04/2002).

[4] Henceforth referred to as IOCA.

network of a company that does not communicate with a public system will not be covered by the Act. Electronic communications carried out through the Internet are covered for the first time, as Internet Service Providers (ISPs) fall under the definition of private telecommunications services (ISPs offer their services by being attached to public telecommunications systems).[5] This is acceptable and welcome in the first place, since it repeals the previous situation where the interception of electronic communications on the Internet was not regulated at all. At least theoretically, it was legally acceptable to intercept such communications since there was no restriction in force.[6] Even though it is quite recently that the Internet has become one of the major telecommunications media, so widely used that it is worth having the ability to intercept it, it seems that Internet communications were indeed monitored. Understandably, we can have no official evidence on how far Internet communications were intercepted by the state (i.e. through Secret Services or the Police). When it comes to workplace surveillance, however, there are several cases in the last years that arose from evidence collected through the Internet, which means that interception of on-line communications is indeed taking place.[7]

RIPA covers a gap that existed in the previous legislation (the Interception of Communications Act 1985), a gap recognised by the Interception of Communications Consultation Paper (Cm 4368)[8] published in summer 1999. According to this paper, there was a need to extend interception of communications legislation to cover surveillance on private telecommunications networks. The Act has also enabled the government to give effect to the judgment of the European Court of Human Rights in the case of Halford v UK.[9] This case had indicated that the law needs to recognise that there are perfectly respectable reasons for allowing employers to record telephone conversations in the work place; for example, in order to provide evidence of commercial transactions or to counter fraud. But the practice needs to be regulated by law, in a way that ensures that the rights of employees are respected in circumstances where they have a reasonable expectation of privacy. RIPA is supposed to provide a clear framework governing the interception of private networks

[5] See Section 2 of RIPA.
[6] According to the principle that what is not explicitly prohibited is permitted.
[7] See for example a survey conducted by Klegal, a legal firm dedicated to workplace disputes, at <http://www.klegal.co.uk>. A large number of workplace disputes arise as the result of employers' surveillance of the Internet access and e-mails sent by their employees.
[8] Available at <http://www.homeoffice.gov.uk/docs/interint/html>.
[9] Case *Halford v. UK* (1997) 24 EHRR 523.

(including Internet telecommunications), setting out the circumstances in which it may be authorised and the safeguards which should apply. Apart from that, it is practically almost impossible for governmental authorities to intercept the Internet without the co-operation of the ISPs, who have no reason to compromise the security of their systems by rendering them interception-friendly, unless obliged by legislation. RIPA, as a consequence, is seen as a step towards enabling the interception of Internet communications and that is why it is essential to see whether it compromises on-line privacy in a balanced way. It has to be pointed out at this point that the history of the regulation's drafting and application seems to satisfy the principle of *consistency* (page 63 of the thesis); the Interception of Communications scheme seems to have been drafted on the lessons of the past and the needs of the present. But also the rest of the Act has come to complete the gaps of the past and the needs of the future.

Chapter 1 begins by making it an offence for a person intentionally and without lawful authority to intercept, anywhere within the UK, a communication passing through a public postal service or a public or, in certain circumstances, private telecommunications service or system (section 1(1),(2)). It then goes on to analyse the exceptions to this offence. First, section 1(3) states that when a private telecommunications network is intercepted without lawful authority but with the express or implied consent of the person controlling the operation and use of the system, this is only actionable in civil law (tort or, in Scottish law, delict). Conduct is anyway excluded from criminal liability by section 1(6), if perpetrated or permitted by the person with the right to control the operation or use of the system. Second, section 4 provides for various forms of lawful authority for interception, such as when it is carried out under an international mutual assistance agreement, or for purposes of carrying out a business, or the discretion given to certain authorities to intercept the communications of prisoners and high security psychiatric patients. And finally, section 5 lays down the conditions under which a warrant can be issued to authorise interception.

Several objections have been raised to the scheme for the issuing of warrants. Even though not 'Internet-specific', they raise important concerns with an equal impact on both on-line and off-line privacy. Let us begin with these.

6.2.1 Authorisation

The major objection to this scheme is the issue of authorisation. Section 7 gives the Secretary of State, rather than a court, the power to authorise a warrant requiring interception of any

form. What is argued here is that the Secretary of State, being a member of the executive, lacks the necessary independence to authorise interception that will be carried out by a state authority; it is seen as an offence against the concept of the separation of powers,[10] and does not seem to satisfy the principle of *accountability*. The European Court of Human Rights has many times stressed the importance of judicial oversight. In *Klass v. Germany*[11] it underlined its significance as a safeguard for surveillance operations. In *Huvig v. France*,[12] while discussing the safeguards offered by the French law on telecommunications interceptions, it again placed considerable emphasis on the safeguard of prior judicial authorisation.

Interception warrants can be issued *inter alia* when an issue of national security or concerning the economic well-being of a country is at stake. The government suggested[13] that judges would be inappropriate to decide whether the issue arising is one of such a nature, whereas the Secretary of State would be the right person for such a decision. This argument is not absolutely convincing, however, since most cases of interception arise during criminal investigations; it is inappropriate to construct a system that is reflective of a minority rather than a majority of cases.[14] The government could, anyway, easily overcome this problem by establishing two separate systems: judicial warrants would be used in relation to criminal matters, while administrative warrants would mainly be relied upon in cases involving national security or the economic well-being of the UK.[15] This would also help to address the issue of accepting intercept material as evidence in a trial, which remains problematic. Under RIPA, the use of intercept material as evidence in a trial is prohibited (section 17). Section 17 and 18, however, create a peculiar situation where the prosecution may be ordered to disclose the material to the trial judge who, in turn, may direct the making of an admission of fact, without in any stage disclosing any of the material to the defendant. The right to a fair trial under Article 6 of the ECHR, particularly the 'equality of arms' principle, seems to be

[10] See JUSTICE, "Second Reading Briefing", available at <http://www.fipr.org/rip/Justice%20RIP%20Bill%202nd%20reading%20brief.pdf> (visited on 26/04/2002).

[11] Case *Klass and Others v. Federal Republic of Germany* (1979-80) 2 EHRR 214.

[12] Case *Huvig v. France* (1990) 12 EHRR 528.

[13] Home Office, "Interception of Communications in the United Kingdom", (Cm.4368, 1999) para.7.2.

[14] See Y Akdeniz, N Taylor and C Walker, "Regulation of Investigatory Powers Act 2000 (1): BigBrother.gov.uk: State Surveillance in the age of information and rights", (2001) *Criminal Law Review* (February), pp. 73-90, at p. 78.

[15] See "Response of the Data Protection Commissioner to the Government's Regulation of Investigatory Powers Bill", a briefing for Parliamentarians, March 2000, paras 4-7, available at <http://www.fipr.org/rip/DPCparlRIP.htm> (visited on 26/04/2002).

seriously compromised by this provision.

It is a fundamental aspect of the right to a fair trial that criminal proceedings should be adversarial and that there should be equality of arms between the prosecution and defence; both defence and prosecution should be given the right to use the same judicial arms during a trial. Article 6 para. 1 of the ECHR requires that the prosecution authorities disclose to the defence all material evidence in their possession for or against the accused. The fact that some valuable information, such as the content of an intercepted communication, may be revealed to the prosecution but not to the defendant seems to come in conflict with this principle. However, as the European Court of Human Rights has accepted in *Rowe and Davis v UK*[16] and *Jasper v UK*,[17] the entitlement to disclosure of relevant evidence is not an absolute right. In any criminal proceedings there may be competing interests, such as national security or the need to protect witnesses at risk of reprisals or keep secret police methods of investigation of crime, which must be weighed against the rights of the accused. In some cases it may be necessary to withhold certain evidence from the defence so as to preserve the fundamental rights of another individual or to safeguard an important public interest. Nevertheless, the Court also recognised that only such measures restricting the rights of the defence, which are strictly necessary, are permissible under Article 6 § 1. Moreover, in order to ensure that the accused receives a fair trial, any difficulties caused to the defence by a limitation on its rights must be sufficiently counterbalanced by the procedures followed by the judicial authorities. These procedures should incorporate adequate safeguards to protect the interests of the accused. It was these procedures that were considered inadequate in *Rowe and Davis v UK* and the Court accepted that there had been a violation of Article 6 para. 1, whereas it accepted that they were adequate in *Jasper v UK*, so there was no violation of Article 6 para. 1 of the ECHR. In effect, the government should provide for adequate safeguards to counterbalance the injustice caused by concealing the content of intercepted communications from the accused, as laid down in RIPA.

Apart from that, an attentive reading of sections 7 (issuing of warrants) and 10 (modification of warrants and certificates) reveals that the authority given to the Secretary of State is not vested with adequate safeguards to make sure that it is always exercised impeccably. For example, section 7 lays out the possibility for a warrant to be issued or modified by a senior

[16] *Rowe and Davis v UK* (16 February 2000) Appl. No. 28901/95, (paras 60-62).
[17] *Jasper v UK* (16 February 2000) Appl. No. 27052/95, (paras 51-53).

official. Even though the Act states that this is permissible only in urgent cases and when the Secretary of State has expressly authorised the issue of the warrant for the particular case, it fails to provide for guarantees that this procedure will be always followed. It neither requires this authorisation to be in a particular form, nor makes sure that it is given before the issuing of the warrant. The former entails that, in cases where no authorisation has been given in breach of this provision, it would be difficult, if not impossible, to prove it; and the latter that any mistakes may well be subsequently corrected to avoid political reactions.

6.2.2 Reasons

A further objection to the scheme of issuing of warrants is the vagueness and subjectivity of the reasons that justify the authorisation of interception by the Secretary of State. Under section 5(2) interception of communications can be authorised when it is considered necessary in the interest of national security, for the purpose of preventing or detecting serious crime or safeguarding the economic well-being of the UK. The conduct authorised should be 'proportionate' to what is sought to be achieved and 'necessary' for this scope, a wording that is deliberately reminiscent of the ECHR Article 8 para. 2, so as to forestall allegations of inconsistency with the Convention requirements, and satisfy the *proportionality* principle. However, the lack of a further definition or explanation of the reasons justifying interception renders the provision insufficiently clear. One could argue that, due to the uncertainty created, the provision could fail to cover one of the three conditions for governmental interference laid down in Article 8 para. 2 of the ECHR, namely to be 'in accordance with law'. That is because it may be considered as failing to provide for the security of law, an element that is inherent in this sentence, as interpreted in many cases by the European Court of Human Rights (see chapter 4). Apart from the fact that 'national security' and 'economic well-being' can be constructed to include almost anything, the fact that this judgement should only be based on the Secretary of State's 'belief' (section 5(2)) makes it a very weak provision in terms of objectivity.

However, as already discussed in chapter 4, this uncertainty does not seem to create specific problems of compatibility with the ECHR; the Court of the ECHR does not seem to be very willing to challenge the reasoning presented by governments for a specific action interfering with privacy. It prefers to avoid transgressing the limits between purely legal decisions and those with a political nuance. Furthermore, RIPA is not the only statute where the terms 'national security' or 'economic well-being' are not defined, it is rather a standard practice

throughout law in general. So, even though a further definition would be welcome, this is an issue that goes beyond the limits of RIPA.

6.2.3 Definitions

Let us now turn to more Internet-specific comments. A lot of complaints have been raised as to the RIPA's failure to take into account the special needs and characteristics of the on-line environment in drafting the scheme of interception. First of all, the definitions of a public or private telecommunications service or systems in section 2 of Part I are so wide that they cover almost anyone that provides some kind of communications service.[18] For example, according to section 2(1)

> "pubic telecommunications service means any telecommunications service which is offered or provided to, or to a substantial section of, the public in any one or more parts of the United Kingdom".

And

> "public telecommunications system means any such parts of a telecommunication system by means of which any public telecommunications service is provided as are located in the United Kingdom".

Even though harmless for conventional telecommunication services, this width becomes rather problematic when it comes to Internet services. That is because the architecture of the Internet is such that it allows the supply of services by people who are not necessarily professionals. There is a considerable number of websites that provide e-mail or other services, such as anonymous remailers for example, that are administered by amateurs and have no intention of profit. Under the new regulation, all these people could be obliged to obey interception warrants, facing a maximum of two years imprisonment if they fail to do so, or up to five years if they reveal its content or existence to others. This possibility may well deter people from offering such services in the first place, a detrimental result considering their valuable contribution to people's ability to protect their on-line privacy.

6.2.4 Interception capabilities

However, the major concern raised in this direction (and the one most widely discussed in the media) is the RIPA's provisions that require ISPs to create and maintain interception capabilities in their systems, in order to be able to comply with a potential interception

[18] See Section 2(1) RIPA.

warrant (section 12). This requirement is questionable for many reasons. First and foremost, it compromises the security of systems as such, since it actually demands the creation of a security 'backdoor' to be used by the government when it is considered essential. What the government has not fully appreciated, however, is that such backdoors could well constitute an attractive target for capable hackers with criminal intentions.[19] It eliminates for ISPs the possibility of offering the best possible security to their clients, who may well choose to buy Internet services from providers abroad. However, this is not in fact a major issue, since most everyday users lack the adequate knowledge and capacity to choose the best available option on security criteria (that may well be the most complicated or expensive one).[20] The subsequent result is a disproportionate compromise on people's ability to enjoy the best possible security and to protect their on-line privacy. Second, the Internet is not like telephone systems, where it is technically feasible to tap into a particular individual's communication link. In order to intercept all possible communication it is necessary to intercept all Internet Protocol (IP) traffic,[21] which means that it is necessary to view all the traffic running through an ISP in order to monitor just one person.[22] The government seems to have overlooked the technical details that render interception of Internet communications much more complicated and severely expensive, if it is to be proper.

To make the situation more onerous, ISPs have practically no opportunity to refuse compliance with the government's requirements to build interception capabilities in their systems, even when there are major technical or economic objections as to the actual implementation of these requirements. Section 11(5)(6) reads as follows:

> "11 (5) A person who is under a duty by virtue of subsection (4) to take steps for giving effect to a warrant shall not be required to take any steps which it is not reasonably practicable for him to take.
>
> (6) For the purposes of subsection (5) the steps which it is reasonably practicable for a person to take in a case in which obligations have been imposed on him by or under section 12 shall include every step which it would have been reasonably

[19] See R Chandrani, "R.I.P. E-Commerce?", (2000) *Computers and Law* (June/July) 30, at p.31.
[20] For example, it is possible for a UK resident to subscribe with an ISP that is based in another country, but the dial up connection would be much more expensive than using a domestic ISP.
[21] See "The Economic Impact of the Regulation of Investigatory Powers Bill" (An independent report prepared for the British Chambers of Commerce), edited by I Brown, S Davis and G Hosein, pp. 8-10, available at <http://www.britishchambers.org.uk/newsandpolicy/downloads/lsereport.pdf> (visited on 10/06/2001)
[22] See "Your Privacy Ends Here", June 4 2000 *The Observer*, available at <http://www.observer.co.uk/Print/0,3858,4025471,00.html> (visited on 26/04/2002).

> practicable for him to take had he complied with all the obligations so imposed on him".

This means that a person served with an interception warrant has the duty to comply by taking any steps that are reasonably practicable for him to take, an assessment based on the assumption that he has complied with the obligations imposed on him under section 12 to build interception capabilities into his system. These obligations, however, are imposed by the Secretary of State (section 12(1)). Even though the Act creates a Technical Advisory Board (section 13) that is supposed to check and review the imposition of such obligations, an attentive reading of the Act reveals that the Secretary of State is not actually obliged to accept the objections raised by the Technical Advisory Board as to these obligations. According to section 12(6)(c)(ii), the Secretary of State, after considering any report of the Board relating to a notice imposing such obligations to an ISP, may give a further notice confirming the effect of the first one, without giving effect to the modifications proposed by the Board, with which the ISP is of course obliged to comply (section 12(6)(a)). Although an impression is given throughout this section that a lot of people participate in deciding the technical requirements to be imposed, there are a number of loopholes that give the Secretary of State the power to impose a subjective decision.[23] However delicate it may be in practical terms to ignore a decision of the Board, the mere existence of such a possibility is a severe compromise for the safeguards provided by the rest of the Act. It is not preposterous to assume that there may well be substantial disagreement between the Secretary of State and the Board, judging by the disagreement that has already arisen between the Home Office and technical experts concerning the estimation of the overall financial consequences RIPA will have on ISPs.[24]

6.2.5 Possibilities of mass surveillance

Another controversial issue with potential detrimental effect for on-line privacy is the

---

[23] For example, section 12(9) states that: "Before making an order under this section the Secretary of State shall consult with
(a) such persons appearing to him to be likely to be subject to the obligations for which it provides,
(b) the Technical Advisory Board,
(c) such persons representing persons falling within paragraph (a), and
(d) such persons with statutory functions in relation to persons falling within that paragraph,
as he considers appropriate" (emphasis added).

[24] See R Calleja, "The Regulation of Investigatory Powers Act 2000", (2000) *Computers and Law* (August/September) p.21, at p.21.

creation under RIPA of possibilities for mass surveillance,[25] an allegation that the government denies without, however, addressing the particular section that causes the concern.[26] Section 8(1) states that:

> "8 (1) An interception warrant must name or describe either-
>
> (a) one person as an interception subject; or
>
> (b) a single set of premises as the premises in relation to which the interception to which the warrant relates is to take place."

However, a reading of the rest of Section 8 reveals that the Secretary of State is given the power to ignore this requirement and issue an interception warrant without specifying any particular person or premises as the target, provided that the warrant refers to the interception of 'external communications' in the course of their transmission by means of a telecommunication system, whose examination he considers necessary in the interest of national security, the economic well-being of the UK, or for the purpose of preventing or detecting serious crime. 'External communications' means any message sent or received from outside the UK. Under this clause, as a consequence, security services may have a mandate to monitor all incoming and outgoing international traffic, without regard to whom it is from or addressed, merely under the control of a general permission from the Home Secretary, for reasons that are not difficult to justify. In the light of the Internet, where almost all traffic passes through international networks, this means that any communication can be tracked down lawfully by governmental authorities. It seems here that the government has failed to take into account the unique nature of the Internet, that defies any territorial border even for the simplest communication or transaction. The route that a packet with data travelling through the Internet follows will often not stay within the national borders, even if its destination is the computer next door. In addition, it is almost impossible to imagine an everyday Internet experience without communicating even once with a website that is hosted on foreign servers. Just imagine how many people use e-mail providers or post to mailing lists or buy products from Internet sites that are based abroad. The percentage of a person's everyday Internet communications that is likely to fall into the category of 'external

[25] See "STAND's Guide to the RIP v1.0", available at <http://www.stand.org.uk/ripnotes/> (visited on 26/04/2002).
[26] See The Home Office, "Myths and Misunderstandings (Mass surveillance?)", available at <http://www.homeoffice.gov.uk/ripa/mass.htm> (visited on 26/04/2002).

communications' is so great, that the possibility created by section 8 constitutes a compromise for on-line privacy that falls short of justifying the principle of *proportionality*.

In addition to all these, section 5(6)(a) states that:

> "5 (6) The conduct authorised by an interception warrant shall be taken to include-
>
> > (a) all such conduct (including the interception of communications not identified by the warrant) as it is necessary to undertake in order to do what is expressly authorised or required by the warrant."

This means that on-line communications of an individual who is not the actual target of the interception may well be intercepted, if it is unavoidable in the process of intercepting the targeted communications. We already saw that in the context of the Internet this could be a usual incident, unless the government takes special measures to avoid it, a responsibility that it is not obliged to undertake. Again this is considered disproportionate and it creates an uncertainty on whether the government will manage to address the special needs of on-line privacy.

6.2.6 Workplace surveillance

Last, but certainly not least, RIPA opens the door for workplace surveillance, a highly controversial issue at present day. Section 4 lays out the circumstances where interception is considered lawful by the Act, without the need of acquiring a warrant. Under section 4(2) the Secretary of State is given the authority to publish regulations that will lay down the circumstances under which interception of communications in a business environment will be considered lawful. Any conduct approved by these regulations should constitute a legitimate practice, reasonably required for the purpose (in connection with the carrying on of a business) of monitoring or keeping a record of communications of that business. This is a very serious clause, given the important role that the Internet plays in contemporary workplace environment. There are a large number of employees who work on-line, using the private network of their employers; this allows the possibility of constant monitoring by their employers. Even though there are numerous legitimate reasons why employers or businesses may wish to monitor their employees (to check their productivity, for example, or to prevent misuse of the business network), there are certain limits on how far this monitoring can go.

The European Court of Human Rights in *Niemetz v. Germany*[27] recognised that there is a reasonable expectation of privacy in the working environment and employees should be guaranteed at least a minimum space of privacy.[28]

The regulations provided for by RIPA have already been published and came into force in October 2000 as the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.[29] The Regulations allow the system controller to monitor or record on its system *without consent* for several reasons:

- ⇒ to establish the existence of facts (e.g. recording transactions); to ascertain compliance with regulatory practices or procedures;
- ⇒ to ascertain or demonstrate standards which are or ought to be achieved by employers using the system in the course of their duties (like quality control and staff training);
- ⇒ to prevent or detect crime (e.g. monitoring to detect employees for fraud or corruption);
- ⇒ to investigate or detect the unauthorised use of its system (which will cover monitoring employee's Internet usage and e-mails to ensure that they complied with the business policy);
- ⇒ to ensure the effective operation of the system (that can cover almost anything).

In addition to all that, businesses can monitor (but not record) communications in order to determine whether they are of a professional or personal character. The only obligation imposed upon the employer is to inform employees that interceptions may take place, and that only if the employees have not already consented beforehand.

There are several indications of how far the government has failed to take into adequate account the unique nature of the Internet and to provide for the minimum of reasonably

---

[27] Case *Niemetz v.Germany* (1992) 16 EHRR 97.

[28] The Court in word said that "...Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. There appears, furthermore, to be no reason of principle why this understanding of the notion of "private life" should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world..."

[29] Statutory Instrument 2000 No. 2699, available at <http://www.hmso.gov.uk/si/si2000/20002699.htm> (visited on 26/04/2002).

expected privacy. The circumstances where interception is permitted are unnecessarily wide. In the context of the Internet their effect is that an employee's on-line behaviour could be under constant monitoring, which is unnecessary and disproportionate to what is sought to be achieved. For all those people who work through a networked system this will remove any possible space of privacy, without correspondingly erasing their expectation of privacy. A simple notification that interceptions may occur is certainly not enough. There should be an obligation for employers to offer detailed guidance as to the circumstances in which monitoring will occur, why it is necessary and the use that will be made of the information gathered (if not a concrete notification every time that monitoring is taking place).[30] In addition, by allowing any kind of interception under the simple precondition that employees should have consented in advance, the Regulations fail to provide for a minimum of privacy; the disadvantageous position in which employees are in relation to their employer means that they have little, if any, choice to deny consent when asked for.

A question that has caused preoccupation in the context of these Regulations is whether they would legitimise blanket monitoring of employees. As commented above, the circumstances under which monitoring is allowed are so wide that one can easily imagine an employee being constantly under observation. However, it is doubtful whether blanket monitoring could be applied as such, meaning that it would be rather against the Regulations for an employer to impose constant monitoring of all communications. Even though there is no explicit provision forbidding blanket monitoring, it is clear from the way the Regulations are written that monitoring of communications is the exception rather than the rule in business practice; it takes place under certain conditions and for certain reasons. Nevertheless, if it had not been for the Information Commissioner's Employment Code of Practice, one could easily imagine the provisions of the Regulations being abused by employers so as to apply constant monitoring. The aim of this Code of Practice (still in a draft version) is to explain and analyse how the Data Protection Act 1998 applies to employers with regard to the protection of their employees' personal data. This Code explicitly refers to its relation with the Lawful Business Practice Regulations 2000 under RIPA, stating that the latter do not constitute an exemption from the Data Protection Act. This means that the Data Protection Act cannot be ignored when implementing the Lawful Business Practice Regulations, so abuse can be avoided

[30] See Justice's Response to the Government Consultation Paper "Interception of Communications in the United Kingdom", pp. 4-5, available at <http://www.fipr.org/ioca/justice.pdf> (visited on 26/04/2002).

through the more cautious rules laid down by the Data Protection Act. The Employers Code of Practice is more cautious and strict with regard to the protection of the employee's privacy. It explicitly recognises that monitoring should be designed to operate in such a way that it does not intrude unnecessarily on the right of employees to expect respect for their private lives and correspondence, and goes on to admit that employees have a right to expect a degree of trust from employers, and to be given reasonable freedom to determine their own actions without constantly being watched or listened to.[31]

6.3 Communications Data

6.3.1 Acquisition and disclosure of communications data under RIPA

Part I chapter 2 of RIPA provides for a legislative framework for the acquisition and disclosure of communications data. Communications or, as otherwise called, traffic data are the information relating to a communication apart from the content as such. They can be, for example, the source and destination address of a message, the names of the sender and recipient, the time and date the message was sent or its size. However, the definition that RIPA has adopted is a much wider one, as will be subsequently explained. This scheme is very welcome in the first place, since it covers a serious legislative gap of the previous situation. Following the *Malone*[32] case in 1984, in which the European Court of Human Rights said that such data fell within Article 8, the government inserted a new section 45 into the Telecommunications Act 1984, that has allowed disclosure of communications data on the broad grounds of the prevention and detection of crime without any of the Article 8 safeguards. That was considered unacceptable, especially after the introduction of the *Data Protection Act 1998* that lays down stricter conditions under which disclosure of communications data may be allowed. It is arguable, however, whether the new framework succeeds in covering this gap in the most 'privacy-friendly' way, especially when it comes to the Internet.

To begin with, RIPA makes an express distinction between the interception of communications and the obtaining of communications data. Section 21(a) reads as follows:

> "21 (1) This Chapter applies to-

[31] See the Employment Practices Data Protection Code, Part 3 Monitoring at work (draft), available at <http://specials.ft.com/spdocs/monitoringdraft3.pdf>.
[32] Case *Malone v. UK* (1985) 7 EHRR 14.

> (a) any conduct in relation to a postal service or telecommunication system for obtaining communications data, other than conduct consisting in the interception of communications in the course of their transmission by means of such a service or system;"

In general terms, the Act permits access to communications data on much broader grounds and under less severe requirements than those applying in the previous chapter with regard to the interception of communications. This attitude is clearly based on the assumption that access to communications data represents a lesser intrusion into privacy than the interception of the content of a communication. It is questionable, however, whether this assumption is a correct one. The European Court of Human Rights in *Malone v. UK* (1984) made clear that even the limited nature of communications data available at that time (essentially a print out of a list of numbers called) was covered by Article 8 of the ECHR.[33] Since then, metering technology has undergone rapid change, and has become much more intrusive and valuable for investigation purposes.[34] In addition to that, the advent of the Internet has completely changed the nature of 'communications' or 'traffic data'. They can be a full list of the websites visited by a user, or the times one logs on, from where and for how long, the details of the e-mails sent and received (address, date, time, route followed), or even the programs downloaded or the newsgroups red and the commercial transactions effected. As more and more personal and professional activity moves towards the on-line environment, the acquisition of traffic data becomes all the more intrusive in terms of privacy. A full picture of a person's life can be easily constructed by such data. As a result, RIPA's lax requirements for the obtaining of communications data can be seen as a serious flaw in the effective protection of on-line privacy.

The first issue I would like to draw attention on is the definition of communications and traffic data. Section 21 (4) reads as follows:

> "21 (4) In this Chapter "communications data" means any of the following-
>
> (a) any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any

[33] The Court said that "...The records of metering contain information, in particular the numbers dialed, which is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of the subscriber also amounts, in the opinion of the Court, to an interference with a right guaranteed by Article 8..."

[34] See Justice's Response to the Government Consultation Paper "Interception of Communications in the United Kingdom", p. 25, *supra* note 30.

> postal service or telecommunications system by means of which it is being or may be transmitted;
>
> (b) any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person-
>
> (i) of any postal service or telecommunications service; or
>
> (ii) in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system;
>
> (c) any information not falling within paragraph (a) or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service."

This definition is broad enough to include any data relating to the use of the communications service, other than the contents of the communication itself, without allowing any room for exceptions in the context of the Internet, where communication data can be of a much more personal nature than in off-line communications. It even covers, according to section 21(4)(c), any other information that is held or obtained by a telecommunications service provider in relation to its clients. This provision is unnecessarily wide; it may include any piece of information, irrespective of whether it is of a personal nature or not, that happens to be in the possession of a service provider with regard to his clients. Such information may include contact details, marital status, income, profession, or even personal preferences. Providers sometimes gather information that is not directly relevant to the offering of their services, but have a statistical or advertising value. It is clear that this is an unnecessarily broad definition that goes far beyond the limits of communications data as we know are. The principles of *proportionality* and *targeting* do not seem to be met here. This provision may prove problematic in terms of the data protection legislation, since it effectively involves the handling of personal data that are maintained by a service provider.

Furthermore, there is no warrant system in order to obtain such data, and the procedure is much simpler and more open than the one laid down in Chapter I. According to Section 22 (4):

> "22 (4) Subject to subsection (5), where it appears to the designated person that a postal or telecommunications operator is or may be in possession of, or be capable of obtaining, any communications data, the designated person may, by notice to the postal or telecommunications operator, require the operator-

> (a) if the operator is not already in possession of the data, to obtain the data; and
>
> (b) in any case, to disclose all of the data in his possession or subsequently obtained by him.

A major flaw of this procedure is the breadth of persons who can require the data. The 'designated person' is nothing more than a person designated for the purposes of this Chapter, who can also grant an authorisation for persons holding offices, ranks or positions with the same relevant authority as his, to engage in any conduct to which this Chapter applies. 'Relevant authorities' include the police, the national criminal intelligence service, the crime squad, customs and excise, the Inland Revenue and the Intelligence Services, together with any other authority specified by the Secretary of State from time to time by order (section 25(1)). There is no further indication as to the rank or position of the persons that will be designated by these authorities for the purpose of obtaining communications data; this is to be decided by an order made by the Secretary of State (section 25(2)). This means that literally anyone can be designated with such powers, an unnecessarily wide possibility, far from the view expressed by many, including the Information Commissioner,[35] that access to such data should also be made subject to prior judicial scrutiny in order to provide for the safeguards laid down by Article 8 of the European Convention of Human Rights. *Accountability* is again in question here since the divergence of the people who may be designated with the authority to obtain communications data creates possibilities of abuse and exaggeration.

In addition to that, the specific reasons for which obtaining of communications data may be considered necessary (section 22(2)) are very wide, much wider than those justifying the issuing of a warrant to intercept the content of communications that have already been greatly criticised for their general character and the lack of any further definition. Apart from national security and the economic well-being of the country, they include the purpose of preventing and detecting 'any' crime or simple disorder, much wider than the equivalent purpose for interception of communications which is limited to the prevention or detection of 'serious' crime. The catalogue also includes *inter alia* the protection of public safety, public health, the assessment or collection of any tax or duty by a government department and any other (not specified in RIPA) purpose that the Secretary of State will decide with an order to

[35] See "Response of the Data Protection Commissioner to the Government's Regulation of Investigatory Powers Bill", a briefing for Parliamentarians, *supra* note 15.

add to this catalogue. Even though, expressly under RIPA (section 22(5)), the acquisition and disclosure of specific communications data should be proportionate to what is sought to be achieved in order for an authorisation to be granted or a notice to be served, this provision fails to work as a remedy for the unnecessary amplitude of the reasons, as it will usually be based on a subjective assessment. The Interception of Communications Commissioner is required to review the working of these provisions (section 57) (a requirement that works as a safeguard in the first place), but it is not clear how this is to be achieved. There is an absence of a specific requirement for the designated person to notify the Commissioner of each authorisation; there is only a general duty to disclose documents and information when particularly asked for by the Commissioner (section 58(1)). Moreover, RIPA fails to provide for any specific safeguards for the holding and destruction of obtained data, as it does for interception material, which again is indicative of how much the seriousness of such data has been underestimated.

Finally, under section 22(3), the person designated to obtain communications data may grant an authorisation for persons holding offices, ranks or positions with the same relevant public authority as his, to engage in 'any conduct' to which chapter 2 applies (emphasis added). There is no further explanation to this provision, which means that it can be constructed wide enough to include any possible conduct in which a person may engage in his effort to acquire communications or traffic data, however outrageous it may be, as for example acquiring these data without the co-operation of the service operator (by hacking for instance into the operator's system). Even though this is an exaggerated possibility, certainly not intentionally implied by the drafters of the Act, the non-existence of express limits as to how far this conduct can go render this provision unacceptably dangerous in terms of privacy.

6.3.2 The retention of communications data under the Anti-terrorism Crime and Security Act 2001

As the government had many times asserted during its passage through Parliament, RIPA contains no powers to force companies to retain communications data for a certain period of time. It simply provides for lawful powers to access communications data by introducing comprehensive statutory controls governing access to billing information or subscriber details. At the time of its passage it was not considered necessary to regulate the compulsory retention of communications data for a specific period of time. However, the question of data retention was revisited in the wake of the terrorist attacks of 11 September 2001 in the US.

The UK government adopted the Anti-terrorism Crime and Security Act 2001 as a response to these attacks, in an effort to fill legislative gaps left by the Terrorism Act 2000 and make sure that the government have the necessary powers to counter terrorist threat in the UK. Compulsory retention of communications data for a specific period of time is now regulated in Part XI of this Act.

The Anti-Terrorism, Crime and Security Act 2001, that received Royal Assent on 14 December 2001, is divided in 14 parts. The measures adopted in these parts, according to the explanatory notes,[36] are intended to: cut off terrorist funding, ensure that government departments and agencies can collect and share information required for countering the terrorist threat, streamline relevant immigration procedures, ensure the security of the nuclear and aviation industries, improve the security of dangerous substances that may be targeted or used by terrorists, extend police powers available to relevant forces, ensure that the UK can meet its European obligations in the area of police and judicial co-operation and its international obligations to counter bribery and corruption, and update parts of the UK's anti-terrorist powers. The adoption of this Act is a proof of the fact (discussed in chapter 3) that terrorism constitutes one of the actual reasons justifying governmental decision to act and interfere with the exercise of human rights and liberties. For the needs of the present chapter we are not going to cover the Act as a whole, but simply Part XI, which regulates the retention of communications data.

As the explanatory notes to the Act clarify, Part XI sets up a structure within which the Secretary of State can issue a code of practice relating to the retention of communications data by communications service providers, such as telephone and Internet companies. According to Section 107(1), "communications data" has the same meaning as in RIPA, which means that the concerns raised as to the unnecessary width of this definition remain the same. Prior to this Act, the retention of communications data was regulated by the Telecommunications (Data Protection and Privacy) Regulations 1999.[37] According to these regulations such data could only be retained for certain specific purposes, otherwise it should be erased or made anonymous. However, whilst the Regulations permitted the retention of communications data on national security and crime prevention grounds, they did not give

[36] See Explanatory Notes to the Anti-terrorism, Crime and Security Act 2001, available at <http://www.hmso.gov.uk>.
[37] Statutory Instrument 1999 No. 2093

any general guidance as to when these might apply. Accordingly, before the Anti-terrorism, Crime and Security Act 2001, communications service providers did not have a clear lawful basis for retaining communications data beyond the period for which it was required for their own business purposes. Part 11 of the new Act establishes a structure to regulate the continued retention of such data on national security and crime related to national security grounds, so that they may then be accessed by public authorities under RIPA. Section 102 provides that the Secretary of State shall issue a code of practice on the communications data retention that may be revised from time to time, or enter into individual agreements with communications providers. This code is voluntary since failure to comply with a code or agreement under this section does not entail criminal or civil liability. Section 103 lays down the procedure that should be followed in order for a code to be adopted. The Secretary of state should, *inter alia*, consult with the Information Commissioner and the communications providers to whom the code will apply, and lay the draft code of practice before the Parliament. Section 104 provides that if the voluntary scheme proves ineffective the Secretary of State may by affirmative order be authorised to impose mandatory retention directions on communications service providers. Subsection 3 requires that the maximum retention period for communications data should be specified by an order. According to the Consultation Paper[38] that was published on March 2003, the proposed maximum period is one year. Section 105 provides that the power to invoke the mandatory scheme in Section 104 will itself lapse unless renewed by affirmative order.

There is no doubt that communications data is a valuable investigative tool, as the Home Office has many times repeated in defending the retention of such data for a period of time in order to be accessed by the authorities if necessary. However, it is doubtful whether Part XI of this Act has managed to come up with an all-encompassing and successful solution for the problem of data retention. First of all, as discussed before in accessing communications data under RIPA, the definition of communications data is so wide that it covers any possible information a communications provider may posses on a certain client. Second, the retention of communications data may be allowed not only for the safeguarding of national security or very serious crime, but for the prevention or detection of any crime. Many concerns have been raised as to whether allowing the creation of databases with such sensitive data is a measure proportionate to the fighting of minor crimes such as for example public order and

[38] See "Consultation Paper on a Code of Practice for voluntary retention of Communications Data", available at <http://www.homeoffice.gov.uk/docs/vol_retention.pdf>.

tax offences, or attendance at demonstrations.[39] Third, as the Information Commissioner has commented,[40] there is a lack of any overt safeguard against abuse of the broad powers that have been entrusted to the Secretary of State. Of course, the procedure provided by the Act for the adoption of the code of practice (consultation and passage through Parliament) operates as a safeguard, but still there is no provision on how an interested party could file a possible complain, which is against the principle of *accountability*. However, the effectiveness of Part XI of the Anti-terrorism, Crime and Security Act 2001 will very much depend on its exact implementation by the code of practice (once adopted) and the possible individual orders or agreements made under it.[41]

6.4 Government Access to Keys

Part III of RIPA, scheduled to come into force by the end of 2001, regulates the "investigation of electronic data protected by encryption etc.", as the title suggests. It has been the most controversial part of the Act since it introduces a power that did not exist before, namely the power of law enforcement agencies and other public authorities to require the delivery up of either decrypted text or the keys that are used to encrypt communications or other data. It is worth noticing that this part was re-introduced with few changes, after being withdrawn from the Electronic Communications Bill in 1999. As part of that Bill it became the subject of intense public reaction and debate and was dropped in order to fast track the more acceptable proposals of the Bill regarding the status of electronic signatures and the licensing of cryptography service providers. Apart from that, UK is the first and only G8 country to regulate explicitly state access to encryption keys, even thought the use of cryptography by criminals has not been proved to pose a greater threat for UK law enforcement than it does for other countries.[42] The importance of cryptography as one of the few available tools affording protection to on-line privacy has already been analysed in chapter 5. Any power conferred on public authorities to demand access on decrypted material

[39] See for example FIPR press release, *Emergency powers allow mass-surveillance for non-terrorist investigations*, 16 October 2001.

[40] Information Commissioner news release, *Information Commissioner contributes to scrutiny of anti-terrorism Bill*, 13 November 2001.

[41] The writing of these lines took place in May 2003, when the code of practice for the retention of communications data had not been adopted yet.

[42] Germany, for example, has made a public statement that the use of cryptography by criminals does not pose a current threat to law enforcement. See B Gladman (for the FIPR), "The Regulation of Investigatory Powers Bill - The Provisions for Government Access to Keys", available at <http://www.fipr.org/rip/RIPGAKBG.pdf> (visited on 26/04/2002).

or decryption keys is a direct interference with privacy, which means that, if not regulated with utmost attention or vested with adequate safeguards, is destined to have a detrimental effect on people's ability to protect it in the electronic environment. But let us take things in order.

6.4.1 Authorisation

First of all, the issue of authorisation: who is given the power to require disclosure? The answer to this question is not straightforward, there is no single authority invested with the power to give authorisation to demand decryption, as for example in Part I where the Secretary of State is the sole authority invested with the power to give interception authorisation. The issue is regulated in Schedule 2 of RIPA. The appropriate level of permission required to serve a disclosure notice will vary according to the public authority involved and to the power under which protected material has been, or is likely to be, obtained in a particular instance. The general principle is that permission to serve a disclosure notice must be given by at least the same level of authority as required for the exercise of the underlying power to obtain the encrypted material. As the Draft Code of Practice explains, the general practice will be that permission should be giv1en by the same person who authorised the use of this underlying power. Schedule 2 begins by stating that when permission to require disclosure is given by a judge it is always sufficient, even if the underlying power to obtain the encrypted information was given under another authority. Judicial authorisation, however, is obligatory only when the underlying power to obtain the material was also given by a judge. In all other cases, authorisation to serve a disclosure notice will usually be given by the person who authorised the obtaining power. In the case of material obtained as a result of interception or surveillance (Part I or II of RIPA), for example, authorisation by the Secretary of State will be sufficient.

Leaving aside the objections already raised as to whether or not interference with privacy should be authorised by a member of the executive authority, this scheme seems to have some kind of rationale. It works, however, under the assumption that a disclosed key has the same value as the information it protects, which is not always the case, especially in the context of the Internet. The value of the content of an encrypted communication may be trivial compared to the value of the encryption key itself, whose disclosure can have detrimental effects in the course of a business for example. Even though demanding the key itself, as opposed to the information in a decrypted format, is supposed to be the exception

and not the rule, as will be subsequently analysed, the fact that what needs to be disclosed is to be decided by any authority in possession of the information seems to undermine the importance of the keys. Actually, demanding the key itself may be considered necessary more frequently than a first glance at the Act would suggest.[43] For example, according to Section 49(1) a person can ask permission to serve a disclosure notice even for material that is 'likely to come into his possession' through a lawful procedure. It is obvious that, when it comes to a communication that is 'likely to come into possession', a person can only ask for the decryption key as it is practically impossible to ask for the disclosure of material that have not yet been generated by the source (as in the case of future communication). Even though this is a weakness not yet tested in practice (the relevant authority may for example decide that disclosure of the key is disproportionate in such cases), it is indicative of why authorisation to serve a disclosure notice should be drafted more attentively, since it may result in a much more serious compromise for privacy than acquiring the material itself.

6.4.2 Reasons

As for the grounds on which a disclosure requirement may be considered necessary (section 49(3)), the objections raised in Part I equally apply here.[44] The lack of a further definition for 'national security' or the 'economic well-being of the UK', combined with the vagueness and subjectivity of these terms, could be seen as raising questions of inadequacy to provide for the security and forseeability of the law, as demanded by the European Court of Human Rights.[45] Additionally, disclosure may be considered necessary for the purpose of preventing or detecting 'any' crime, not only 'serious' crime as in Part I, a term that, having the potential to cover even the most trivial malfeasance, renders the potential reasoning unnecessarily wide. However, as already discussed for the reasons justifying the interception of communications, it is doubtful whether they will actually cause any particular problems. The generality of the reasons justifying a governmental action and the lack of a further definition has become a common practice in laws.

6.4.3 Content of a disclosure requirement

Let us turn now to what can be asked by a section 49 notice imposing a disclosure

[43] See V Mitliaga "Regulation of Investigatory Powers Act 2000 and the Truth about the Disclosure of Keys" (2001) *E-Law Review* 6, Issue 2/December 2001.
[44] See section 6.2.2, page 134.
[45] See, for example, Case *Amann v. Switzerland* (2000) 30 EHRR 843.

requirement. Section 50(1) reads as follows:

> "50 (1) Subject to the following provisions of this section, the effect of a section 49 notice imposing a disclosure requirement in respect of any protected information on a person who is in possession at a relevant time of both the protected information and a means of obtaining access to the information and of disclosing it in an intelligible form is that he-
>
> (a) shall be entitled to use any key in his possession to obtain access to the information or to put it into an intelligible form; and
>
> (b) shall be required, in accordance with the notice imposing the requirement, to make a disclosure of the information in an intelligible form."

The effect of such a notice is that the person served with it shall be required to make a disclosure of the information in an intelligible form. This means that a person is not by default required to disclose the key used; plain-text of the encrypted material is sufficient, unless of course he/she decides to disclose the key itself, which is also considered a valid way of complying with the notice (section 50(2)). However, section 50(3) introduces some serious exceptions to that rule:

> "50 (3) Where, in a case in which a disclosure requirement in respect of any protected information is imposed on any person by a section 49 notice-
>
> (a) that person is not in possession of the information,
>
> (b) that person is incapable, without the use of a key that is not in his possession, of obtaining access to the information and of disclosing it in an intelligible form, or
>
> (c) the notice states, in pursuance of a direction under section 51, that it can be complied with only by the disclosure of a key to the information,
>
> the effect of imposing that disclosure requirement on that person is that he shall be required, in accordance with the notice imposing the requirement, to make disclosure of any key to the protected information that is in his possession at a relevant time.

This means that, apart from the fact that a person may be directly required to hand over the key itself under certain circumstances (as will be subsequently shown), it seems that the same is required when the person is no longer in possession of the information itself (section 50(3)(a)). However, even though this is supposed to be an exception, it is likely to be the case much more often than the drafters of the Act have probably thought. Intercepted communications, for example, for which the person served with the notice has not kept a

record (which is usually the case in the context of the Internet unless it is part of a commercial transaction) or data stored in computers or floppy disks that have been seized by the relevant authorities, all constitute material that may be in the hands of the authorities but not in the hands of the person having the ability to decrypt them. All these are cases where the handing over of keys will be required, even though not particularly asked for by the authorities, and without respecting the special circumstances where plain-text is not enough and handing over of keys is considered necessary (section 51). So even though the government tried to ease concerns by explicitly making handing over of keys the exception rather than the rule, with this provision (section 50(3)(a)) it is effectively taking away with one hand what has already given by the other. Not being in possession of the information is not a mere possibility but rather a strong probability for the person served with a section 49 notice. The Draft Code of Practice does not seem to suggest anything different as it does not provide for any further clarification, even though it makes clear that a person served with a section 49 notice who is in possession of both the information and the key has the right to choose which one to disclose.

This possibility is somehow eased by the fact that a person is given the right to comply with a disclosure notice by giving away only the specific key that was used to encrypt the information in question (the session key as otherwise called) (section 50(4)(5)(6)). He is, however, still required to disclose 'any key' to the protected information that is in his possession at a relevant time, if he is no longer in possession of this specific key (section 50(3)(b)). Section 56(1) defines the term 'key' as any key, code, password, algorithm or other data the use of which (with or without other keys) allows access to the electronic data or facilitates the putting of the data into an intelligible form. This wide definition of 'keys' means that, if a person is no longer in possession of a session key, he may be required to disclose any other kind of data that is in his possession that provide even an indirect access to the protected information, as for example a system password or a general key password. This is a disproportionate possibility given that disclosure of such other 'keys' can be far more detrimental than the disclosure of the information itself, as it may compromise a whole system. The wide definition of 'keys' seems to suggest that RIPA may have implications not just for encrypted data, but also for wider categories of electronic data, as the Data Protection Commissioner has observed,[46] which is an unnecessary extension of the scope of the

[46] See "Response of the Data Protection Commissioner to the Government's Regulation of Investigatory Powers Bill", March 2000.

legislation.

6.4.4 Explicit disclosure of key requirement

Section 51 is devoted to the cases where a section 49 notice can require the disclosure of the key itself, even though the person served with the notice is in possession of both the key and the data. First of all, the person serving the notice should have a special direction to include such a requirement, given by the person handing the general permission for serving this notice. A direction to ask for the key itself should only be given when there are 'special' circumstances of the case that render it necessary, as otherwise the purposes for which a disclosure notice is being served would be defeated. The giving of such a direction should also be proportionate to what is sought to be achieved (section 51(4)). The use of the word 'special' rather than 'exceptional', as originally proposed, has been criticised as being unnecessarily wide and causing considerable uncertainty and concern about the precise circumstances in which keys should be seized. This is aggravated by the fact that the 'special' nature of the circumstances is to be based on a subjective decision, as section 51(4) states that a person should not give a direction unless 'he believes' (not necessarily on reasonable grounds) that the requirements are met. Further clarification of these 'special' circumstances was to be provided for by the Code of Practice which, however, fails to do so in an adequate way, at least as it is drafted at present. It says that, by way of illustration, the circumstances should be considered as special either when trust or timeliness is an issue, meaning (a) when there is doubt about the *bona fides* of the person or organisation asked to comply with a disclosure notice, or (b) the person having the key cannot, for whatever reason, carry out the necessary decryption and provide the relevant plain-text quickly enough in time critical situations (and the relevant authority can). This clarification has been criticised as inadequate because the concern about trust would be better met by imposing a requirement on the recipient to prove that the plain-text is genuine (as for example decryption in front of the authority), and the concern about timeliness is not meaningful without a more detailed explanation of the sort of scenarios that are envisaged.[47] It is true that handing over keys is a serious interference with privacy and, as such, should be based on a law drafted adequately clear so as to provide for security and foreseeability, which is certainly not the case when it

[47] See B R Gladman, "Comments on Preliminary Draft of the Draft Code of Practice on the Investigation of Electronic Data protected by encryption etc.", 11th July 2000, available at <http://www.fipr.org/rip/BG_p3copcom.pdf> (visited on 26/04/2002).

comes to this provision.

6.4.5 Signature keys

Disclosure of a key can have serious implications in the on-line environment when it is a signature key, especially one that is used for business purposes. RIPA has tried to eliminate the possibility of compromising such keys by explicitly stating that a section 49 notice shall not require the disclosure of a key intended to be used only for the purpose of generating electronic signatures (section 49(9)(a)).

> "49 (9) A notice under this section shall not require the disclosure of any key which -
>
> (a) is intended to be used for the purpose only of generating electronic signatures; and
>
> (b) has not in fact been used for any other purpose.

The Act, however, allows the disclosure of such keys, if they have in fact been used for purposes other than signature. As a result, even though RIPA is trying to ensure the integrity of digital signatures, these provisions will probably fail to protect the majority of signature keys that are currently in widespread use because they have not taken into account important elements of the current practice. First, the way cryptographic products are being designed at the moment encourages users to rely on single keys. The government is itself advocating a 'one key protects it all' philosophy by promoting the use of multi-purpose smart cards where a single security mechanism protects many disparate data items. Second, even where different keys are used to provide digital signatures and confidentiality, they are very often controlled by passwords or pass-phrases that are the same for both sorts of keys. The difficulty of remembering different passwords has as a result that key owners often use identical ones, even when it is not necessary due to software. It is therefore very likely that access to a single key or a password for an information protection key will also give access to the owner's signature key, with serious implications for the course of on-line conduct.

6.4.6 Safeguards

One of the most vital issues with respect to seizure of keys is the safeguards provided for by RIPA, as to how these keys are to be used and stored by the authorities. The importance of this issue has to do with the fact that a seized key, when it is a general use one (not a single session key), will most of the time have a great value for its owner, extending far beyond the

protection of the specific information for which it was disclosed. The seizure of a signature key, for example, possibly a frequent occurrence as we already saw, compromises its owner's ability to provide for reliable authentication. The fact that the key has escaped from his exclusive control opens the potential of being misused to forge his signature, with devastating results for his reliability. Apart from that, a general confidentiality key or a password will often provide access to many more information than those in question. As for the storage of such keys, RIPA simply states that they should be stored in a secure manner (section 55(2)(e)), without laying down specific details of how this is to be achieved or whether the security provided will have to take into account the value that is attributed to them by their owner. The Draft Code of Practice does not provide for any further details as to how security is to be achieved. RIPA also fails to take into account the fact that many of the keys seized will belong to people who are not themselves under suspicion. The widespread use of public-key cryptography, where a message can only be decrypted by the secret key of its intended recipient, creates a situation where the generator of a suspicious message is not in possession to decrypt the message, whereas the unsuspecting recipient can, by disclosing his secret key. Such keys would probably deserve further protection. The amount of protection to be afforded will be decided by the authorities who have seized the key as they 'consider necessary' (section 55(2)). It has to be mentioned here that arrangements for secure storage of seized keys will incur a considerable cost for the relevant authorities, who are not obliged in any sense to go for the best possible option. The breach of this obligation may be actionable under civil law (section 55(4)), but there is no provision of criminal liability either for failure to provide for adequate protection or for possible misuse of seized keys, the fear of which would probably work as an incentive for greater attention.

6.4.7 Use of seized keys

As for the use of seized keys (section 55(2)), RIPA makes sure that it will be limited to what is absolutely necessary and proportionate to the scope for which it was seized. The use should be reasonable with regard to both the standard use of the key by its owner and the circumstances of the case. All records of the key should be destroyed as soon as they are no longer needed for the purpose of putting information into an intelligible form, and the number of copies made of the key or the number of persons to whom the key is disclosed should be kept to the minimum necessary (section 55(3)). However, the law is not absolute and strict as to whether the key should be only used for decrypting the information for which

it was seized in the first place. According to section 55(a), a key can be used to put into an intelligible form only protected information in relation to which power to give such a notice was indeed exercised or 'could have been exercised' if the key had not already been disclosed. This effectively means that a key can be lawfully used to decrypt many more pieces of information than specified in the notice, provided that they were obtained by lawful means and could also justify a disclosure requirement. This is reasonable and acceptable in the first place; it opens however a possibility of abuse since it could essentially allow decryption by overcoming the procedure provided for by the Act (acquiring a permission to serve a notice). There is no further indication as to whether or what kind of oversight should be in force when a key is used to decrypt an extra piece of information, or who is going to decide whether this information is of a nature that would also dictate a section 49 notice for seizure of the same key.

6.4.8 Offences and their subsequent complications

According to section 53, a person who has been served with a section 49 notice will be guilty of an offence (with a maximum penalty of two years' imprisonment) if he knowingly fails to make the disclosure required. This provision has been accused as ineffective to combat the use of cryptography by criminals, while managing to deter lawful users from taking full advantage of available technology. The threat of two years' imprisonment may well intimidate simple users (who may use cryptography merely to enhance their on-line privacy) and deter them from taking full advantage of available technology, while it provides an opportunity for serious criminals to escape longer conviction.[48] A criminal will probably choose to face two years' imprisonment by refusing to comply with a section 49 notice rather than disclose the keys to much more incriminating material.

As for the argument that this provision will not have an adverse effect for law-abiding individuals, who will not have any reason to deny decryption, the situation is not that simple. Section 53(2) states that in proceedings against a person for an offence under this section, a person shall be taken to be in possession of the key to the encrypted information, if it is shown that he was in possession of that key at any time before the time of the giving of the notice. In order to refute this presumption, the defendant has to show that the key in question was not in his possession after the giving of the notice and before the time by which he was

[48] See "STAND's Guide to the RIP v1.0", *supra* note 25.

required to disclose it, which will be taken to be shown if "there is sufficient evidence of that fact, and the contrary is not proved beyond a reasonable doubt" (section 53(2)). This places the burden of proof on the defendant to show that he no longer holds a key that he may previously have held, which has been criticised as unfair since the burden should remain throughout on the prosecution to show that the defendant is in possession of the key, which he deliberately denies to disclose.[49] At least the situation has improved dramatically since this provision was initially introduced in the draft Electronic Communications Bill, and the defendant does not have to meet a very heavy subsequent burden, since he is taken to have proved that he is no longer in possession of the key if he has presented sufficient evidence to raise a reasonable doubt. Even this, however, is frustrating enough for an innocent person who cannot comply with a section 49 notice (i.e. when the 'key' is a password that has simply been forgotten). In addition, a person is not given the right to deny disclosure on the ground that compromise of his key is disproportionate to what is sought to be achieved, which may usually be the case in the context of the Internet. Waiting for the case to get to the Tribunal (the one laid down by this Act as will be seen later in this chapter) may be too late to avoid a disproportionate disclosure, with detrimental effects for the key owner.

By section 54, RIPA introduces a second offence, 'tipping-off', where a person faces a five-year maximum penalty if he fails to keep secret the giving of the notice, its contents and the things done in pursuance of it. A person will have the obligation to keep such secrecy only when it is explicitly required by the notice, which has to refer to information that has come or is likely to come into the possession of the police, Customs and Excise, or any of the Intelligence Services. The secrecy requirement also applies to anyone who becomes aware of the notice, even though he is not the intended recipient, but it is a defence to show that he neither knew nor had reasonable grounds for suspecting that the notice contained a secrecy requirement (section 54(10)). The secrecy requirement should be considered reasonable in order to maintain the effectiveness of any investigation or operation, or investigatory techniques generally, or the safety or well-being of any person (section 54(3)). It is interesting to note that a person failing to keep secret the existence of a section 49 notice, faces a much heavier penalty (maximum of five years) than the one he faces if he fails to make the actual disclosure required by the notice (maximum of two years). One would expect that failing to comply with a disclosure notice would be a heavier offence than revealing the

[49] See Y Akdeniz, N Taylor and C Walker, *supra* note 14, at p. 87.

existence of a notice to a third person.

The 'tipping-off' offence seems to be meaningless with respect to a disclosure notice requiring the handing in of keys. The Government has indicated that a seized key can be revoked immediately by its possessor, and a new key can be issued to replace it, provided that no explicit reason is given for this action. In other words, a person served with a notice to hand in a decryption key may inform his clients or colleagues that the key is no longer in use, provided there is no reference to the section 49 notice that he has been served with. Section 54(5) states that in proceedings against a person for a tipping-off offence it is a defence to show that the disclosure was entirely effected by the operation of software, designed to give an automatic warning when a key ceases to be secure, and the person could not reasonably have been expected to take steps to prevent this disclosure. The existence of this subsection may be taken as an indication that revocation of seized keys will not be permitted after all. What is the use of this subsection since the key owner should be anyway safe from prosecution, provided that this software simply revokes keys without giving any reasons?[50] The government has not given any reasonable answer to this question.

Apart from that, under RIPA it is possible to require a key to decrypt information that is not yet but is 'likely to come' in to the possession of the relevant authorities. This may well be the case when a section 49 notice is served in order to ensure instant decryption of the information that will be gathered during interception of a communication stream. If instant revocation of the compromised key is considered legal, as the government has indicated, it will have as an effect the ineffectiveness of both interception and consequent decryption, since it is irrational to expect that a compromised key will be subsequently used as long as it is legally acceptable to revoke it. The effectiveness, and probably the whole existence, of this offence with regard to keys is very arguable, as it is difficult for the government to deny the right to revoke seized keys, since keys are anyway revoked many times for other reasons.[51]

6.5 Scrutiny

Part IV of RIPA is dedicated to the oversight mechanisms that are to be in force in relation to the exercise of the powers conferred to the authorities by this Act. Even though oversight is

[50] See B R Gladman, *supra* note 42.
[51] See also C H Lindsey, "Regulation of Investigatory Powers Bill - Some Scenarios", available at <http://www.cs.man.ac.uk/~chl/scenarios.html> (visited on 26/04/2002).

not an issue of exclusive relation to governmental interference with on-line privacy, it merits some reference in the context of this chapter, as any critique on a regime of interference would be incomplete without a minimum reference to the mechanisms of redress. Anyway *accountability* is one of the basic criteria when judging the quality of a regulation. The European Court of Human Rights has repeatedly stressed that an effective oversight and redress mechanism is an indispensable part of any law regulating governmental interference with privacy, if it is to meet the requirement of being 'in accordance with law'.

6.5.1 The Commissioners

RIPA introduces a system that is not substantially different from the one that existed under the Interception of Communications Act 1985. Section 57 provides for the appointment of the Interception of Communications Commissioner (replacing the one appointed by IOCA), who should be a senior judicial figure and is assigned with keeping under review the exercise and performance of the powers and duties under Part I and Part III of RIPA (only to the extent that they are exercised by the Secretary of State). The Commissioner should report on any specific defects and make an annual report, which is laid before Parliament. Section 59 provides for the appointment of the Intelligence Services Commissioner (replacing two previous Commissioners appointed under the Security Services Act 1989 and the Intelligence Services Act 1994), who is assigned with the same form of review with regard to the powers exercised by the Intelligence Services.[52] As already said, the main task of the Commissioners is to report on an annual basis to the Prime Minister on the operation of the Act. Although these reports are published and laid down before the Parliament, this is done after sensitive and confidential material is removed if it appears to the Prime Minister that publication of such information would be contrary to the public interest or prejudicial to national security, the prevention and detection of serious crime, the economic-well being of the UK or the continued discharge of the functions of any public authority whose activities are subject to review by the Commissioner (section 58 (7)). The obvious effect of these widely drafted exceptions is that what reaches the eyes of the public can be effectively controlled and decided by the executive, a potential that seriously diminishes the importance of having an independent judicial authority to overview the exercise of powers granted to the public

[52] The jurisdiction of the Intelligence Services Commissioner does not extend to Northern Ireland. RIPA (section 61) provides for the appointment of a separate Commissioner, the Investigatory Powers Commissioner for Northern Ireland, with separate oversight capacity for the exercise of investigatory powers in this area.

authorities by this Act. It has also been argued that, in order to have proper accountability, there should be an express requirement in the Act for more detailed and all-encompassing annual reports by the Commissioners. Information on such matters as the cost and effectiveness of the particular surveillance or interception method in terms of arrests, prosecutions and convictions would help towards a more substantive evaluation of whether these powers have been used correctly.[53]

6.5.2 The Tribunal

Apart from the Commissioners, section 65 of RIPA establishes a Tribunal to deal with complaints regarding the performance of investigatory powers by the relevant authorities. Even though the existence of such a Tribunal is very welcome, there is a major flaw throughout RIPA that is expected to have a negative effect on the function of this Tribunal as a whole. A necessary precondition before filing a complaint is for the individual to become aware that he has been the target of an investigatory power, exercised under this Act. However, there is no notification procedure throughout the Act, designed to make sure that a targeted person will become - sooner or later - aware of having constituted the target of an investigation and all the details of how this power has been exercised by the relevant authorities. Without such a procedure it is literally impossible for a person to become aware of such information, especially given the fact that the Act is throughout designed so as to exclude this possibility. Under Part I (section 19), it is a criminal offence (with a maximum penalty of five years' imprisonment) for a person to reveal even the existence of an interception warrant, and section 17 excludes intercepted material from ever being used in legal proceedings, or revealed in any case to the defendant. Part II contains analogous provisions and Part III also makes sure that the authorities can impose a secrecy requirement as to whether a section 49 notice has been served. In addition to all that, section 67 (5) states that the Tribunal, as a rule, shall not consider or determine complaints made more than one year after the taking place of the conduct to which they relate. With all these provisions in mind, it is highly unlikely that a person will become aware that he has been the target of an investigatory within a year of its occurrence, if at all.

The Tribunal may be given the power to accept complaints made at a later time, if it considers it equitable to do so (section 65 (5)), but the fact that this is an exceptional

[53] See JUSTICE's Response to the Government Consultation Paper "Interception of Communications

possibility, to be decided *in concreto*, diminishes its power as a remedy to the above-described adverse situation. Although notification is a controversial issue, as it may diminish the effectiveness of an investigation, many other countries including the US, Canada, Germany, Denmark and the Netherlands have some form of notification after the event, subject to the investigation not being prejudiced. Of course the issue is very delicate, since the success of an interception largely depends on it being secret. However, I would suggest that it would not be devastating for an investigatory procedure if the target of the investigation were to be notified after the investigation had been completed, and before proceedings are initiated in front of a court. This may well happen anyway, with an arrest, charge, seizure of assets etc. The European Court of Justice, in *Klass v. Germany*,[54] placed considerable emphasis on the fact that the German law required notification of the individuals concerned as soon as this was not prejudicing police activities.

It is also arguable whether the Tribunal will be effective after all, for several other reasons. First of all, as laid down in section 67, the Tribunal will not operate as a normal court, but is supposed to exercise merely a form of 'judicial review'. Any person familiar with the UK law comprehends that judicial review has a different function than that of a normal judicial procedure. Its fundamental purpose is the supervision of the exercise of lawful authority so as to ensure that it is being exercised lawfully and properly.[55] In other words, what can be decided under judicial review is whether an act of the executive or a governmental authority is valid or not, without necessarily examining the substantive issues of a case. This means that the Tribunal will not give a straight answer to a complainant but will simply state whether the determination is favourable or not, not necessarily revealing any details[56] and without having the obligation to give a reasoned decision. Judicial review in general, is a residual remedy; it must not normally be regarded as a remedy of first resort but rather, if not always a remedy of last resort, at least an exceptional remedy.[57] However, according to sections 65 and 67, the Tribunal will have exclusive jurisdiction to decide on complaints made as a result of the implementation of RIPA. In this way, the statute virtually excludes the possibility of a complaint being raised in front of a normal court. The applicant has no right

---

in the United Kingdom", *supra* note 30.

[54] Case *Klass and Others v. Federal Republic of Germany* (1979-80) 2 EHRR 214.

[55] See Lord Clyde, P.C. and D J Edwards, *Judicial Review*, Scottish Universities Law Institute Ltd, Edinburgh/ W. Green 2000, at chapter 1.

[56] See Y Akdeniz, N Taylor and C Walker, *supra* note 14, at p.90.

[57] *supra*, note 55, p. 318.

to an oral hearing; it is in the discretion of the Tribunal to hold oral hearings if it is considered necessary, but it is no under a duty to do so in any circumstances.[58]

The second issue that arises with respect to the function of the Tribunal has to do with the existence of a second stage of review. According to section 67, an appeal stage of jurisdiction is principally excluded, except if the Secretary of State decides otherwise:

> "67 (8) Except to such extent as the Secretary of State may by order otherwise provide, determinations, awards, orders and other decisions of the Tribunal (including decisions as to whether they have jurisdiction) shall not be subject to appeal or be liable to be questioned in any court.

The Secretary of State is in effect given the exclusive power to decide whether there will be a second stage of jurisdiction, and what form this is to take. However, this discretion seems to be an obligation with regard to certain cases. Section 67 (9) seems to suggest that the Secretary of State has the duty to provide for a second stage of jurisdiction, at least for a particular group of cases. What seems to be in his discretion in these cases is the form that this second stage is going to take. Section 67 (9) reads as follows:

> "67 (9) It shall be the duty of the Secretary of State to secure that there is at all times an order under subsection (8) in force allowing for an appeal to a court against any exercise by the Tribunal of their jurisdiction under section 65(2)(c) or (d)."

But this exception is not enough. There is in essence a lack of a second stage of jurisdiction. Even with the exception provided that the Secretary of State may decide otherwise, this situation is wholly insufficient to cover the needs of a person who has constituted the victim of a procedure under RIPA that was not exercised legally. In fact, it seems to eliminate the possibility of a complaint ever reaching adjudication under a normal court by default. The only possibility that does not appear to be affected is a case ending up at the European Court of Human Rights, if a person considers that his human rights as protected by the ECHR are breached, either as a result of an investigatory power exercised by the authorities, or by the inadequacy of the remedies provided by the statute itself.

As a final remark, the data available as to the performance of the Tribunal so far (as it already existed under IOCA), are very poor to support the reliability of the new Tribunal. The records suggest that the Tribunal has never found a breach of the law and rarely considers cases of

[58] Section 9 of Statutory Instrument 2000 No. 2665 (regulating the internal procedures of the Tribunal). It can be found at `http://www.hmso.gov.uk/si/si2000/20002665.htm`> (last visited on 25/06/2002).

interception, due to the non-disclosure rules.[59] The new scheme of scrutiny, as laid down by RIPA, does not provide for any substantial cases that would indicate a possible change in the previous record.

6.6 Assessment

It is difficult to say with certainty what the impact of this Act on the protection of on-line privacy will be, since most of the relevant provisions are not yet, or will not be for a long time, in force to allow for such an evaluation. It remains to be seen whether the possibilities opened by RIPA will be used on a privacy-friendly way or whether privacy concerns will be undermined for the sake of law enforcement effectiveness. According to this author's point of view, the drafters of RIPA seem to have failed the task of taking into full account the unique nature of the on-line environment and the differentiated potential impact of its provisions on the effective protection of on-line privacy. The five principles of good regulation are not always met; there are many points where they are not satisfied properly.

A striking example justifying these comments is the procedure laid down for the acquisition and disclosure of communications data. As already discussed, there is a considerable difference between the nature of communications data relating to an on-line activity, and those relating to a normal communication. The former are considerably more privacy intrusive than the latter, but there is no special scheme to deal with their disclosure. It would not have been difficult for the drafters of RIPA to lay down two separate schemes, each one taking into account the special nature of the communications data seized. Communications data relating to on-line activity, for example, could be defined to include only such information as the time, date and destination of messages sent and received, or the time and duration spent on-line. Information such as the websites visited, for how long, or what the subscriber did while on-line (which is certainly much more intrusive upon privacy) could be disclosed under a different procedure, more similar to the one laid down for the interception of the content of communications. Furthermore, the definition of communications data could be more limited, leaving out all the information that a service provider may hold with respect to his clients (which is not in essence 'communications data'). This scheme, according to this author's point of view, falls short of the principle of *targeting* since it fails to take into account the different needs of dissimilar cases and resorts to a more general approach.

[59] See Y Akdeniz, N Taylor and C Walker, *supra* note 14, at p.90.

Another issue that could have been dealt with greater care is the creation of interception capabilities. We already saw that as far as the Internet is concerned, intercepting one person's communications and on-line activity cannot be easily achieved without also intercepting all the data travelling through the targeted route. There are no adequate guarantees that this possibility will not be abused when a particular person's communications are targeted. In addition to that, the government does not seem to be willing to undertake the cost that falls upon ISPs in order to meet with the requirements laid down by the Secretary of State and the Advisory Board. This cost is very large if the technical standards are to allow interception in the most privacy-friendly way. It is a very heavy burden, especially for small ISPs who could be easily dissuaded from providing the service in the first place. This concern, however, has been eased by the Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002.[60] According to Section 2(3) of this order, small ISPs (those who do not intend to provide their services to more than 10,000 persons in the UK, and do not do so), are exempted form the obligations laid down in Part II of the Schedule to maintain certain interception capabilities in their system. Still, the creation of such extended interception capabilities is in the verge of falling short of the principle of *proportionality*; a great potential for abuse is created, as systems are rendered vulnerable to exploitation by both governmental agents and third parties.

Encryption is another questionable issue. As discussed in this chapter, the scheme for the investigation of electronic data protected by encryption leaves a lot of unnecessary loopholes for abuse. Even though disclosure of the keys themselves is supposed to be the exception rather than the rule (with disclosure of the data in a decrypted format being the standard requirement), we saw that this is actually going to be the case much more often than initially believed. Especially in the context of the Internet, disclosure of keys is probably going to be more common than disclosure of the plaintext. People overall do not tend to keep copies of all the messages sent and received by them for long periods of time, except for some businesses that tend to keep a record of all the communications and transactions made in the course of their work. The provisions of RIPA may dissuade simple users from taking full advantage of encryption, due to the fear of being exposed to a decryption requirement that would be detrimental for both personal and professional reasons. The situations where disclosure of keys is considered essential could have been described in much more detail by

[60] The Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002, Statutory Instrument 2002 No. 1931.

the law, and the requirements to be fulfilled could be far stricter than they are at present. The principle of *transparency* fails to be met here; the situation is not adequately clear for users who may easily find themselves in a difficult position unnecessarily and, in many cases, unjustifiably.

As discussed in 6.5, even though a scrutiny procedure is laid down by RIPA, it has many deficiencies that pose many questions as to whether the principle of *accountability* is indeed satisfied. According to this author's opinion it is not, since the complaints procedure is not sufficiently accessible, fair and efficient. Furthermore, even though the Commissioners lay down an annual report on the operation of the Act, this report can be greatly scrutinised by the Prime Minister as to what is going to see the light of publicity or not, a potential that diminishes the importance of having independent Commissioners in the first place. The principle of *accountability* is also compromised by the several schemes of authorisation (for the interception of communications, acquisition of communications data and decryption keys): authorisation is entrusted to members of the executive rather the judiciary; the former does not guarantee the objectivity and independency of the latter.

We could go on and on referring to provisions that could have been dealt with greater care and sensitivity as to their effect on on-line privacy and the respect of the five principles, but this has already been done in the course of this chapter. Although RIPA is overall a good effort to address issues that should be, sooner or later, addressed (and it is certainly preferable to having no regulation at all), it still fails to take into account the special needs of on-line privacy and the differences between the attitude of people in the on-line and off-line environment. In general, what seems to be unacceptable is that potential for abuse has in fact been left open, while the government ought to make sure that such possibilities were as eliminated as much as possible. It is certainly not easy to find the right balance between such conflicting interests as the need to protect privacy and investigate crime for the sake of the common good. The future impact and the practical implications of enforcing such provisions, however, should have played a much more prominent role when drafting this legislation.

Finally, according to this author's point of view, RIPA is much less privacy-oriented than it should have been, if it was to succeed the task of making governmental investigatory powers compatible with the ECHR. Of course, RIPA has not yet been challenged in front of the European Court of Justice, but it is very possible that sooner or later it will be. Since it regulates governmental interference with privacy, actions of interference should be

compatible with the conditions laid down in Article 8 para. 2 of the ECHR. As was analysed in chapter 4, according to this Article, interference with privacy is acceptable *inter alia*[61] when it is provided for in an adequately accurate, accessible and foreseeable law that provides effective safeguards against abuse. A remedy against abuse should also exist which, if not judicial, should at least provide the guarantees of independence and impartiality that are inherent in a judicial system of supervision and control. RIPA may be accessible, but is it accurate and foreseeable enough to pass this test? There are many points in the law that are unnecessarily vague, such as, for example, the reasons for which interception of communications or acquisition of communications data is allowed, the definition of communications data, the situations where the disclosure of the plaintext is not enough and the decryption key should be handed in to the authorities. Furthermore, RIPA does not provide for sufficient guarantees against abuse. For example, warrants allowing the interception of communications or the acquisition of communications data are issued by the government and not by an independent judicial authority that would be a more neutral option. RIPA fails to provide adequate guarantees that the keys seized by the authorities will be kept safe and will be used for very limited purposes. Finally, it is doubtful whether the existing remedy (the Tribunal) provides adequate guarantees of independence and impartiality, since its procedure is not open to the public and there is not an appeal stage. Above all, since RIPA fails to make sure that the subject of interception will be sooner or later informed of the fact that his communications have been intercepted, it is difficult to get a complaint to the Tribunal in the first place. Nevertheless, these are only speculations since the compatibility of RIPA with the ECHR will be better judged by the way it is implemented in particular cases.

[61] The other two conditions laid down in Article 8 para 2 of the ECHR (interference should be based on a legitimate reason and be necessary in a democratic society) refer to a particular action of interference in question, and not to the law allowing it. So, they are not relevant for judging the compatibility of RIPA with the ECHR.

Chapter 7

Covert governmental surveillance: the real threat for on-line privacy?

7.1 Preface

Up to now, this thesis has focused on interference with on-line privacy that is perpetrated by a government against its own nationals (or at least within its jurisdiction) and how far this should go. In order to underline the antithesis between this kind of interference and the one that constitutes the subject of the present chapter, the former could be described as 'overt' interference, in a sense that it is, or should be explicitly laid down by a law, and it can be (rather usually than always) communicated to the targeted individuals, as for example the restrictions in the availability of strong encryption or a notice to disclose the decryption keys used. However, on-line privacy is also threatened by another form of governmental interference: the 'covert' surveillance that takes place around the world. This interference has an international character in a sense that it is not about a government interfering with its own nationals' privacy, but rather about a general potential of governments to interfere with the on-line privacy of individuals all over the world. Covert surveillance has a distinctive feature: it is arbitrary, in a sense that it is not usually subject to rules, principles or laws (or at least not so detailed ones that would cover all its possible aspects).[1] It is part of the 'secret' activities of a country, operated for diplomatic and military purposes, and is considered an important element for the exercise of foreign policy. Governments consider this lack of detailed legal rules as an indispensable characteristic of covert surveillance, because otherwise it would have a completely different nature (first and foremost, it would not be secret). However, the lack of a detailed legal basis means that there is a big possibility of abuse, which may be greatly exploited by governments. As far as citizens are concerned, it entails little or no safeguards to make sure that their basic rights and liberties will only be compromised to a degree proportionate to the aim pursued. Keeping this in mind, the

[1] In the UK, for example, there is a legal base for the operation of the Intelligence and Secret Services (MI5, MI6 and GCHQ), meaning the Security Services Act 1989 (as amended) and the Intelligence Services Act 1994. But these laws, as will be subsequently analysed, do not offer a complete legal base for all possible secret activities of these agencies.

assessment of how far the vulnerabilities created for privacy in the on-line environment are necessary and proportionate to the intended result acquires a new dimension. The reason is that it is very much dependent on the extent to which these vulnerabilities could be exploited and by whom. Let us proceed to some general comments in order to make these issues clear.

In general terms, individual privacy is prone to invasion perpetrated either by another person or by larger organisations such as a government, foreign or domestic, or an intelligence agency. There is a substantial, even though not absolute, difference between the effects of a 'personal' and a 'governmental' invasion, both in terms of feeling and result. The effects of the former are usually more obtrusive and directly insulting, while the effects of the latter can be much more serious and devastating in the long run, even though the invasion as such is usually unobtrusive. In other words, an invasion perpetrated by another individual may entail a strong feeling of insult with no far-reaching consequences (as for example trespass in a private sphere), while an invasion perpetrated by a government may have severe implications without directly causing a negative feeling (interception of communications or secret surveillance, for example, is unobtrusive to the target but may lead to, sometimes arbitrary, legal prosecution). There is an additional dimension to this distinction when we move from the real world to cyberspace.

The invasion of on-line privacy, on the one hand, is mainly unobtrusive to the target, irrespective of its perpetrator (information gathering, for example, is usually unobtrusive irrespective of the identity of the perpetrator).[2] Protecting oneself from governmental interference, on the other, is a different endeavour altogether from avoiding invasion by other individuals. For example, any kind of encryption (even the weakest form) suffices to secure data or communications from individual eavesdroppers or business rivals, but only strong encryption can make sure that the same information is unreadable to any governmental organisation or intelligence agency. Likewise, the use of an anonymous remailer may prevent an individual from discovering your real identity but it is necessary to use more complicated techniques (several different anonymous remailers to send one message, for example) in order to exclude any possibility of being discovered by a law enforcement agency.

[2] To make things clear, apart from cookies or on-line monitoring, a very common way of gathering information on the Internet is when the users fill in forms with personal data, which is of course something they do consciously (so it is not unobtrusive as such). However, even in this case, the invasion of on-line privacy can be unobtrusive, in a sense that most people are not really aware of how this information is going to be used or abused.

The reason why I am underlining these features is because allowing the existence of vulnerabilities for privacy in the on-line environment may have far-reaching effects, depending on how far they are being exploited and by whom. Governments may claim that weak cryptography, for example, is enough to protect on-line privacy, but they fail to recognise that, for data travelling through the Internet, the more vulnerable it is, the more possible it is for it to be intercepted by a government itself or the intelligence services of another country. Having this in mind, and given the nature of the Internet and the amount of activity that has moved towards the electronic environment, it becomes obvious that the existence of covert surveillance capabilities may have dangerous results of a social, political or even economic nature. That is why the actual threat posed to on-line privacy by covert surveillance capabilities should play an important role in deciding how far to allow governmental interference or restrict the circulation of security mechanisms. Our aim here is to describe (to the extent allowed by information that has seen the light of publicity) how far the Internet has or is becoming a target of covert surveillance perpetrated by governments, either against foreigners or their own nationals, and to assess the effect of such possibilities in the drafting of a policy or law affecting our ability to protect on-line privacy.

7.2 Covert on-line surveillance

7.2.1 Surveillance in general

It is certainly very difficult, if not impossible, to describe the existing surveillance and interception of communications' capabilities, as it is an issue traditionally surrounded by secrecy. Especially when it comes to the Internet, it is only recently that information has come to light concerning the efforts made around the world to build interception capabilities and obtain intelligence through this new medium. One thing can be said with certainty at the moment: the Internet has not been left untouched by the intelligence community, even though the degree to which interception can be effective is still uncertain.

Communications intelligence is defined by the National Security Agency of the US (NSA) as "technical and intelligence information derived from foreign communications by other than the intended recipient".[3] Originally, the targets of defence and intelligence agencies were mostly military and diplomatic communications, since the Cold War offered a strong reason

[3] National Security Council Intelligence Directive No 6, National Security Council of the United States, 17 Feb. 1972.

to justify their collection. However, the growth of the world trade after the 1960's and the rapid scientific and technological development signalled a significant shift in the focus of intelligence operations. An increasingly important aspect of such operations became the collection of economic intelligence and information about scientific and technological developments.[4] With the end of the Cold War in the 1990's, intelligence agencies lost their publicly accepted mission, and having to seek for a new one in order to justify their budgets, they turned to the combat of economic espionage and issues such as terrorism, drug trafficking and money laundering, matters of an admittedly lesser diplomatic or military nature.[5] The 1990's was also the time when computers started to become ubiquitous. We have reached a point by now where computers and the Internet have become an integral part of everyday activity. There is a vast amount of information and communications stored in computers or travelling between them that constitutes a valuable source for intelligence agencies. The Internet has become an attractive target for intelligence gathering, offering possibilities that did not exist before.

7.2.2 The Echelon and other major international surveillance systems

Today, the most powerful *known* system of intercepting electronic communications is the so-called *Echelon*,[6] a system that works by indiscriminately intercepting very large quantities of electronic communications, such as e-mail, fax or telex, and then using computers to identify and extract the useful from the mass of the unwanted ones. Even though it is thought that electronic surveillance began more than thirty years ago,[7] it is only very recently that specific information has come to light. The existence of the *Echelon* first appeared in print in 1988, in a *New Statesman* article written by a British investigative reporter, the by now well known

[4] See D Campbell, "Interception Capabilities 2000", part 4 of A Scientific and Technological Options Assessment conducted by STOA for the European Parliament ("Development of Surveillance Technology and Risk of Economic Information" an appraisal of technologies of political control), at <http://www.cyber-rights.org/interception/stoa/interception_capabilities_2000.htm> (visited 26/04/2002).

[5] See D Banisar, "Big Brother Goes High-Tech", Covert Action Quarterly, 56 (Issue of Spring 1996), available at <http://www.media-awareness.ca/eng/issues/priv/resource/brother.html> (visited on 26/04/2002).

[6] There is still some uncertainty on whether this is the actual name of this specific surveillance system, although its existence is no longer in doubt.

[7] See J Richelson, "Desperately Seeking Signals", (2000) *Bulletin of the Atomic Scientists* March/April 2000, Vol. 56, No. 2, pp. 47-51, available at <http://www.bullatomsci.org/issues/2000/ma00/ma00richelson.html> (visited on 26/04/ 2002).

Duncan Campbell.[8] This article spoke of a surveillance system code named as Project P415, run by the US National Security Agency with the participation of other countries' intelligence agencies, especially the UK, targeting the civilian electronic communications of the 21st century. More details and information about *Echelon* came to light in 1996 by the New Zealand peace activist Nicky Hager, who provided a detailed description of the program in his book *Secret Power: New Zealand's role in the International Spy Network,*[9] describing New Zealand's signals intelligence agency and its place in a UK-USA surveillance alliance. These are still among the most valuable sources of information about the *Echelon* system.

In 1997 the system came under the scrutiny of the European Parliament through a report prepared by the Scientific and Technological Options Assessment[10] on "An Appraisal of Technologies of Political Control", that described *Echelon* in a chapter concerning national and international communications interception networks. This study revealed *inter alia* that within Europe all e-mail, fax and telephone messages were routinely intercepted by means of a global surveillance system administered by the UK/USA alliance. What raised particular concern was the fact that, unlike many of the electronic spy systems developed during the Cold War, *Echelon* was said to be designed primarily for targets such as foreign governments, organisations and businesses in virtually every country, and not for military and defence purposes. In order to find more about this issue, STOA in 1999 commissioned a five-part study of the "development of surveillance technology and risk of abuse of economic information", which ended up in five separate reports that became publicly available around June 2000. These reports revealed, *inter alia*, the existing interception capabilities[11] and a number of cases where communications gathered by the *Echelon* system were used to afford a negotiatory advantage for US companies against their European rivals, who lost, as a result, commercial agreements worth millions of dollars.[12] These allegations raised severe concerns throughout the European Union and on 5 July 2000 the European Parliament decided to set up a temporary committee to investigate the *Echelon* system. Almost a year later, this

[8] D Campbell, "Somebody's listening", New Statesman 12 August 1988, pp.10-12, available at <http://jya.com/echelon-dc.htm> (visited on 26/04/2002).
[9] N Hager, *Secret Power: New Zealand's Role in the International Spy Network*, Nelson, New Zealand: Craig Potton Publishing, 1996.
[10] Henceforth referred to as STOA. STOA is a department of the Directorate-General for Research of the European Parliament that commissions research.
[11] "Interception Capabilities 2000", by Duncan Campbell, *supra* note 4.
[12] "The Perception of Economic Risks Arising from the Potential Vulnerability of Electronic Commercial Media to Interception", by N Bogonikolos, Part 1/5 of the above mentioned study, available at <http://cryptome.org/dst-1.htm> (visited on 26/04/2002).

committee prepared a draft report containing the result of its investigation,[13] which was approved by the European Parliament at the beginning of July 2001.[14]

The diplomatic foundation that constituted the genesis of the *Echelon* is the UK/USA agreement. Following wartime collaboration in gathering intelligence and intercepting radio transmissions, in 1947 the US and UK made a secret agreement to continue their collaborative global communications intelligence activities, despite the end of World War II. The alliance was formalised in 1948, with the participation of three other English-speaking nations, namely Canada, Australia and New Zealand, who joined the UK/USA Agreement as 'Second Parties'.[15] There are also 'Third Parties' to the Agreement (with less tight bonds to the co-operation) that include Germany, Japan, Norway, South Korea and Turkey. The existence of this agreement was not acknowledged publicly until March 1999, while its text and exact terms still remain secret. What is known is that it is an agreement of co-operation between the intelligence agencies of the signatory states,[16] with the NSA being the prime mover, as the majority of funds for joint projects and facilities and the direction for intelligence gathering operations are primarily issued through the US agency. A chain of secret interception facilities has been established around the world to tap into all the major components of the international telecommunications networks.[17] Some monitor communications satellites, others land-based communications networks, and others radio communications. The *Echelon* network links these facilities and it works by indiscriminately gathering all e-mail, fax, telex, or telephone communications travelling through its range of access (which is effectively a large proportion of the communications of the planet as these

[13] See *Draft Report on the existence of a global system for the interception of private and commercial communications (Echelon)*, prepared by the Temporary Committee on the Echelon Interception System, 18 May 2001, available at <http://www.bof.nl/docs/echelon_draft.html> (visited 26/04/2002).

[14] See (news article) "Echelon Furor Ends in a Whimper", by S Ketmann, 3 July 2001, Wired News, available at <http://www.wired.com/news/politics/0,1283,44984,00.html> (visited on 26/04/2002).

[15] See D Ball and J Richelson, *The Ties That Bind: Intelligence Co-operation Between the UKUSA Countries*, Boston: Allen & Unwin, 1985.

[16] The National Security Agency (NSA) for the US, the Government Communications Headquarters (GCHQ) for the UK, the Defense Signals Directorate (DSD) for Australia, the Communications Security Establishment (CSE) for Canada and the Government Communications Security Bureau (GCSB) for New Zealand.

[17] See N Hager, "Exposing the Global surveillance system", *Covert Action Quarterly*, available at <http://mediafilter.org/caq/CAQ59GlobalSnoop.html> (visited on 26/04/2002).

facilities are strategically spread to cover all different areas[18]). Powerful computers at each station of the network automatically search through the millions of messages intercepted for ones containing pre-programmed target keywords. The messages containing these words are separated in categories of interest and are separately examined and analysed by agents. We could go into further detail, describing the potential of the several facilities and how this system works and is administered between the agencies, but what is said is enough to assess the threat posed for privacy from the existence of such a system.

It is often argued by intelligence and governmental circles that there is literally no conflict between surveillance operations and individual privacy, since the scope of such operations is the collection of information of a diplomatic or military interest, both issues of national security that outweigh by far any privacy concern. However, the Temporary Committee set up by the European Parliament to investigate *Echelon* came to the conclusion that one of the most important features of the system is that it is designed to intercept private and commercial rather than military communications.[19] Apart from that, this line of argument also fails to recognise the fact that the legal status and limits of intelligence operations has always been a 'no entry' zone in terms of public discussion, and since most of the operations remain secret, intelligence agencies can act without being under a judicial overview that would guarantee non-abuse of their powers. In fact, scattered data have shown that the *Echelon* system has indeed been used several times for more than simply diplomatic or defence purposes.

First, governments may not be allowed to spy on their own nationals, but the UK/USA Agreement participants can and have allegedly done it in several occasions, using the help of their intelligence allies. A government may be restricted by law from spying on its own nationals, but there is no barrier in receiving information about them, gathered by a foreign intelligence agency, which is an indirect way of overcoming this restriction. Both UK and US political leaders have allegedly used the *Echelon* facilities to spy on their political opponents or even allies (in an effort to gain knowledge on their true intentions), rendering the system a powerful tool of political advancement.[20] Furthermore, 'spying' ability at the disposal of a

[18] See P S Poole, "Echelon: America's Secret Global Surveillance Network", 1999-2000, available at <http://fly.hiwaay.net/~pspoole/echelon.html> (visited on the 26/04/2002).
[19] See *Draft Report on the existence of a global system for the interception of private and commercial communications (Echelon)*, *supra* note 13.
[20] For further details and allegations see P S Poole, *supra*, note 18.

government can easily be used against such targets as political activists who try to promote opposite ideologies or expose corrupt governmental activity. History has shown that most governments have not resisted the temptation of taking advantage of such possibilities once they have them at their disposal.[21] Second, the *Echelon* network has also been allegedly used for economic espionage, apart from diplomatic or military, an endeavour that crosses the limits of acceptability between countries in the diplomatic arena. Given the volume of commercial transactions and communications that travel in an electronic form, the system can be used to gather precious information concerning commercial rivals. The research conducted by STOA for the European Parliament revealed a number of cases where *Echelon* was used to afford a negotiating advantage for US companies against European companies and other rivals. US companies used the information provided to them to prevail in commercial agreements and gain millions of dollars.[22] The use of *Echelon* for both political and commercial purposes underlines the fact that its existence poses serious privacy concerns, given the vast possibilities of misuse or abuse that are opened for its administrators. The risk becomes more severe when it comes to on-line privacy, since the amount of personal and professional activity (not simply communications) that has moved towards the Internet opens unprecedented potential of surveillance and privacy intrusion. Data travelling through the Internet are already in digital form, which means they can be easily processed and analysed by powerful computers, a fact that places Internet surveillance amongst the most valuable sources of information.

There are, however, several other factors that should also be considered in order to reach an objective view on how much threat is posed for on-line privacy by the existence of such a system, since operating it is not as easy as it initially sounds. The European Parliament's Temporary Committee came to the conclusion that there are certain limits in the capacity of this interception system. According to their view, the fact that the majority of communications travel through cables or in the form of radio signals, to which the *Echelon* states have limited access (in contrast with satellite communications in which they have extended access),[23] means that the system cannot be as extensive as was initially assumed. It is difficult, however, to make definitive conclusions, since there are no definitive data on the design of the system.

---

[21] See W Diffie and S Landau, *Privacy on the Line*, The MIT Press 1999.
[22] *supra*, note 12.
[23] See *Draft Report*, *supra* note 13.

What can be said with relative certainty is the fact that the expanding use of fibre-optic cables is causing difficulties for the system, since tapping them has proved a major challenge in ways that tapping conventional cables or collecting signals transmitted through the air have not.[24] But even that is not a definitive element since it can be overcome by architectural solutions. In 1997, for example, during the trial of two women peace campaigners appealing their convictions for trespassing on the facilities of Menwith Hill (a major US intelligence base in Britain), it came into light through several documents and a testimony that at least three major domestic fibre-optic telephone trunk lines (BT) were wired through Menwith Hill,[25] a base that participates in the *Echelon* network. Of course the issue was left untouched and did not become a subject of further investigation, as it was considered an issue of 'national security'. This incident is, however, indicative of the fact that we can never be sure of the exact potential of the *Echelon* system without possessing definitive information.

A second important factor is the problem caused to the operation of such a system by the volume of data that is being collected. The amount of data exchanged between computers all over the world is so great that by itself it constitutes a hindrance to the collection and processing of electronic communications. It is certainly very complicated and time consuming to pick out the useful ones from the mass of unnecessary data.[26] After powerful 'dictionary' computers discern the ones containing targeted keywords, from then on it is a 'manual' job to read them, pick out the ones containing valuable intelligence drops and prepare detailed reports, before they become of any particular use. The volume of data collected reduces the speed by which this process can produce useful results. This, however, is again a mere speculation, since we know little detail about how the system works and the amount of manpower it employs. Above all, even that difficulty does not erode the possibility created for an innocent person to be targeted and his privacy arbitrarily invaded by a governmental agency.

Last, but certainly not least, the use of strong encryption is said to constitute the greatest challenge for such a system. The data collected is of no use if it is unreadable in real time (or at least no later than useful) by the collector. The use of weak encryption does not seem to constitute a real problem, since it can be broken in little time by a powerful computer. The

[24] See D Campbell, "Interception Capabilities 2000", *supra* note 4.
[25] D Campbell, "BT Condemned for Listing Cables to US SIGINT Station", September 4, 1997.
[26] See J Richelson, *supra* note 7.

use of adequately strong encryption, however, means that the data is only readable by the person holding the decryption key. It is difficult to estimate the amount of strong encryption that is in use around the world - we already saw in the fourth chapter that there have been numerous efforts to restrict the dissemination of strong encryption. What can be said with relative certainty is that, although strong encryption software circulates freely through the Internet, its use is not the standard among average Internet users, who lack the minimum expertise needed and are not well informed on the possible risks.

Even though it is difficult to draw any definitive conclusions, the mere existence of this system plays a significant role in assessing the vulnerabilities in the on-line environment. It should be stressed, however, that *Echelon* is not the only existing system of Internet surveillance. There are at least thirty other nations operating major intelligence organisations, the largest one being that of Russia,[27] which are gradually becoming involved in electronic surveillance of the Internet.[28] *Echelon*, however, is of a distinctive importance since it is the only one operated with the co-operation of several countries and is strategically planned so as to have a worldwide range of activity. The only other country that is believed to be in a position to apply electronic surveillance on a worldwide basis is France, because of the bases it maintains in its former colonies, spread in strategic points around the world. Indeed, several allegations came recently to light concerning the operation of a system similar to *Echelon* by the French government.[29]

Compatibility of ECHELON with UK and EU Law

Before turning to domestic surveillance it would be interesting to see how far the *Echelon* monitoring operations, at least when it comes to UK participation, are or can be compatible with domestic and European law. It has to be mentioned, however, that since the UK/USA Agreement on which this intelligence co-operation is based is a secret one, not much can be said for its legality as such, or for certain details of the agreement. As mentioned above (footnote 16 of this chapter) the UK participates to this Agreement by its Government

[27] FAPSI (Federalnoe Agenstvo Pravitelstvennoi Svyazi i Informatsii) the Russian Federal agency for Government Communications and Information, with 54.000 employees.
[28] See D Campbell, "The Spy in your Server", The Guardian, 10 August 2000, available at <http://www.guardianunlimited.co.uk/online/story/0,3605,352394,00.html> (visited on 26/04/2002).
[29] See J Thorel (news article), "Frenchelon - France has nothing to envy in Echelon", ZDNet France, 30 June 2000, available at <http://news.zdnet.co.uk/story/0,,t269-s2079875,00.html> (visited on 26/04/2002).

Communications Headquarters (GCHQ), an agency whose function is, in a few words, to monitor or interfere with electromagnetic, acoustic and other emissions, and any equipment producing such emission, gather intelligence concerning such emissions or equipment, and provide advice and assistance to the government when it comes to intelligence in foreign languages or a certain terminology and encrypted material.[30] The existence and operation of the GCHQ is regulated by the Intelligence Services Act 1994. To begin with, *Echelon* operations seem to fall under the functions of the agency. However, there are a number of objections to their legality. First of all, as analysed before, *Echelon* is designed to gather indiscriminately all communication passing through targeted international communications networks. The Intelligence Service Act 1994 does not differentiate between internal and external communications, but it does not give blank permission for intercepting all communications emitted. A warrant from the Secretary of State is needed in order to authorise entry or interference with property or wireless telegraphy (Section 5). Additionally, the director of the GCHQ has the duty to ensure that no information is obtained except so far as necessary for the proper discharge of its functions and that no information is disclosed except so far as necessary for that purpose or for the purpose of any criminal proceedings (Section 4(2)(a)). Finally, the director is also responsible to ensure that GCHQ does not take any action to further the interests of any United Kingdom political party (Section (2)(b)). From the information available it can be said that *Echelon* operations do not totally comply with these rules. The warrant procedure does not seem to be followed (unless if done in secret), intercepting all communication passing through the targeted networks is not in compliance with the duty to gather only the information necessary for the intended scope, and we have already seen that *Echelon* has been used by political leaders to further their ends (page 204). In addition to that, *Echelon* is a system that has not been designed primarily for military and defence targets, but for eavesdropping foreign governments, organisations and businesses. This fact makes its legal status more doubtful since it poses the question of how far its operations, which clearly infringe privacy, can be justified under accepted reasons. Apart from that, since interception of communications is now covered by RIPA, there is also a question of whether *Echelon* operations comply with the rules laid down under this Act. Under RIPA interception of communications is unlawful unless it is authorised under this Act. As analysed in the previous chapter, interception conditions are stricter when it comes to internal communications, but the secretary of State can issue a general warrant for the

[30] Intelligence Services Act 1994, section 3.

interception of external communications when it is considered essential in the interest of national security etc. (See 6.2.5). However, the wording of the law does not make it clear whether the non-targeted interception of communications, which are then checked using key-words, would also be covered by the concept of 'interception' as defined in RIPA, if the intercepted material was not analysed in British soil but merely transmitted abroad as 'raw material'. In effect, the legal status of *Echelon* operations under UK law is uncertain.

Let us now turn to the compatibility of UK *Echelon* operations with EU law.[31] As far as Community law is concerned, the first observation that can be made is that activities and measures of the member states for the purpose of state security or law enforcement do not fall within the scope of the EC Treaty. According to the principle of limited authority, the European Community can take action only where a corresponding competence has been conferred upon it. In particular, The European Union Temporary Committee on *Echelon* concluded that the involvement of a member state in an interception system for the purposes of state security cannot be in breach of the EC data protection Directives, because they all recognise that they do not apply when it comes to the processing of data concerning public security, defence, state security (including the economic well-being of a country when the data relate to state security matters) and the enforcement of criminal law. As for the rest of the EU law, Title V (common foreign and security policy) and Title VI (police and judicial co-operation in criminal matters), there are no data protection provisions comparable to those adopted under the EC Treaty, so there seems to be no particular problem of legality. However, the question of *Echelon* UK operations' compatibility with EU law is put in a whole different level when this system is used for industrial espionage. Under Art 10 of the Treaty of the European Community (TEC), member states are committed to acting in good faith and, in particular, from abstaining from any measure which would jeopardise the attainment of the objectives of the Treaty. When interception of communications is carried out by a state for the benefit of its domestic industry, this is equivalent to state aid and there is a breach of Art 87 TEC. But even when such activity is taking place for the benefit of a non-member state, this comes at odds with the concept of the common market since it amounts to distortion of competition.[32] Finally, as far as privacy protection is concerned, UK

---

[31] See the European Parliament, Temporary Committee on the ECHELON Interception System, Report on the existence of a global system for the interception of private and commercial communications, 11 July 2001.
[32] Ibid., page 82.

has the right to interfere with this right under the conditions analysed in Chapter 4 (i.e. when done for an accepted reason, interference is laid down by law, and is necessary in a democratic society). This author is very much in doubt whether UK *Echelon* operations would manage to pass this test; even if it can be claimed that they are done for acceptable reasons, it would be very difficult to convince that they are laid down by a clear and foreseeable law and that blank interception of all communications passing through targeted networks is proportional to what is sought to be achieved.

7.2.3 Domestic Surveillance - Carnivore

Apart from covert surveillance targeting the communications of a foreign country, there is of course domestic surveillance, which is of no lesser importance with respect to privacy. Domestic surveillance (interception of communications) is not secret by default and it is usually subject to legislation; but it would be silly to take this for granted, or to deny that, in reality, there is a considerable amount of domestic surveillance that is taking place secretly and without complying with any law. Secret domestic interception of communications usually explodes the interception capabilities that are built within systems in order to serve the needs of legal interception. So, the possible abuse of such systems is the reason why domestic surveillance is included in this chapter.

The amount of human conduct that shifted towards the electronic environment has compelled governments to develop techniques of on-line surveillance, in an effort to keep their ability to investigate crime intact. These techniques, however, are admittedly becoming much more intrusive than their real-world counterparts. In US, for example, it recently came into light that the FBI is using a questionable tool in its fight against crime. Its initial name was Carnivore, but it recently changed to a more neutral one, DCS 1000,[33] as part of a governmental effort to ease the public concern that arose from its existence. Carnivore is a software and hardware device that provides the FBI with the ability to intercept and collect all kinds of data that travel through the Internet, such as e-mail or file transfers. It is installed at an ISP, and can be configured to capture and save data from specific users or sites. Although the FBI claims that the program has the capacity to distinguish between data that can be lawfully intercepted through a Court order from those that cannot, and it is subject to

[33] Actually DCS 1000 is a revised edition of the old Carnivore with greater potential, also known as "Enhanced Carnivore".

intense judicial and internal oversight with significant penalties for its misuse, privacy groups are concerned with its capacity to gather all kinds of data. Since the FBI is refusing to reveal the code for the program, there is still some uncertainty as to whether it is indeed designed to gather only the data for which there is a judicial order, which as experts say is not easy in technical terms, or whether it is used to collect all data passing through an ISP, which would be a major invasion of privacy.[34]

The US is not the only country applying domestic Internet surveillance. The Chinese government has built an Internet police force, which has operated since 1998,[35] and it is planning to build a surveillance system to monitor activities on the Internet, similar to the data-recording 'black box' that is installed in commercial aeroplanes.[36] While such a system could help the government in its fight against cybercrime, it could also be used to curb the free flow of information and invade individual privacy, since dissident groups' activities or information are likely to be closely watched under such a system. Other countries such as Russia, Germany, Holland and Israel are known to have been engaged in Internet surveillance, targeting both foreign and domestic exchange of data.[37]

The existence of various Internet surveillance systems, either of a worldwide or a domestic range, has a considerable effect on the proportionality of the measures adopted to combat cybercrime, which seriously diminishes people's ability to protect their on-line privacy. Vulnerabilities allowed (such as hindering the development and use of strong encryption) and possibilities created (such as building an interception capability in a service provider's system) have as a consequence the exposure of individuals to the disposal of systems of foreign or domestic surveillance. This exposure may have far reaching results of a social, political or economic nature, that outweigh by far the awaited potential to combat illegal conduct on the Internet. That is why such possibilities should be considered an important

---

[34] See M Figueroa, "Carnivore - Diagnostic Tool or Invasion of Privacy?", 1 September 2000, available at <http://www.sans.org/infosecFAQ/legal/carnivore.htm> (visited on 26/04/2002).

[35] See K Platt (news article), "Cybercops Police China", The Christian Science Monitor, 17 November 1999, available at <http://more.abcnews.go.com/sections/.../chinacybercops991117.htm> (visited on 26/07/2001) not available anymore.

[36] See (news article) "China Plans to Build Internet Monitoring System", CND 20 March 2001, available at <http://www.cnd.org/Global/01/03/20/010320-3.html> (visited on 26/04/2002).

[37] See "Echelon's Counterparts" (last updated and verified on June 28, 2001) in Echelon Watch web page, at <http://www.aclu.org/echelonwatch/networks.html> (visited on 26/04/2002).

factor in the process of drafting a policy of interference with on-line privacy.

7.3 Assessment

So, is secret surveillance a real threat for on-line privacy? This author thinks it is, perhaps even more than we think, given the fact that what has seen the light of publicity up to present is probably just the tip of the iceberg. It is only recently that the actual existence of surveillance systems, such as the *Echelon,* has started to be openly discussed in public. We are still far from the point (if we ever reach it) where verified information on their operation and capacity will be openly available. It seems that we are even further from the point where they will be openly taken into consideration when a measure that regulates (or affects) cyberspace is being drafted.

However, this author believes that the existence of covert international and domestic surveillance should have an effect on the drafting of a law that could enhance the operation of such a system. Take for example cryptography: restricting the availability and use of strong encryption deprives users of their ability to protect themselves against secret surveillance. Likewise, requiring ISPs to make their systems directly interceptable opens up the possibility of abuse by either foreign or domestic surveillance systems. Both are considerable effects that should be taken into account. Arguably, there is a form of irrationality in this argument; one could claim that you cannot expect from a government to protect its citizens against itself. Undoubtedly, secret surveillance serves the interests of powerful factors (be they a government or individual politicians or even private entities). However, all this information that has seen the light of publicity cannot be simply ignored. In fact, reducing the ability to abuse such systems should be a major priority. Governments are not something stable and aloof; they do change hands (and at times quite quickly), and it is citizens who actually decide (at least theoretically) whether to hold on a government or not. Above all, citizens are threatened probably more from covert surveillance operated by foreign governments, and this is something that cannot be ignored. Finally, such kind of secret surveillance is an element that affects *proportionality* and *targeting*, two of the five principles of good regulation. If a regulation affecting on-line privacy is to be adopted, the existence of such extended surveillance capabilities will mean two things. First, the proportionality of a regulation that eliminates on-line privacy and creates possibilities of compromising it will have to be measured against the extended surveillance capabilities of such systems. In other words, it is

not only the compromise that a measure itself will have as an effect, but also the doors for further surveillance that may be opened. Second, the actual effect of such a regulation may be very different from what initially assumed, due to the fact that secret surveillance systems tend to change the scenery and put reality into a different perspective. That affects targeting since the effects of a regulation turn to be different from the intentions of the drafters.

In concluding this chapter, it is important to point out that the recent terrorist attacks of 11 September 2001 in New York and Washington have changed the scenery quite dramatically. Before these events, there was an augmenting mobility of the international community around the issue of secret surveillance. Information regarding *Echelon* had started to see the light of publicity; the European Parliament had ordered an official report regarding *Echelon* and so on. The terrorist attacks on the Twin Towers and Pentagon, however, seem to have put a break to this mobility and stopped the flow of information or any mood for co-operation, especially from the part of the US. Most importantly, they have provided the US government with a strong 'argument' to support its efforts to control cyberspace, limit on-line privacy and restrict the dissemination of strong encryption. These events, according to the US government approach, came as evidence that the US territory and people are in a great danger from international terrorism, a danger that calls for strong reaction in order to be eliminated. The recent wars against Afghanistan (2001-2) and Iraq (2003), a part of the US campaign/fight against terrorism, clearly revealed the cruel face of this campaign. The diplomatic scenery surrounding these wars have indicated the US hard-core attitude against terrorism, and it's little - if no - inclination to water down its absolute position and co-operate with the rest of the world. The danger from international terrorism has also been considered to highlight the need for interception and intelligence capabilities, and the investigative and diplomatic advantage gained through them. As far as the citizens' privacy is concerned, it seems to have descended many steps in the hierarchy of priorities for the US government.

Cyberspace has not been left untouched by this climate, especially due to the fact that the perpetrators of the 9/11 2001 attacks were claimed to have used the Internet resources (using cryptography and steganography) to communicate and exchange information between them. On-line privacy is being compromised in the name of security and censorship is being applied in the name of fighting terrorism. The Patriot Act, introduced less than a week after 9/11 2001, has allowed Carnivore to do what CALEA (the 1994 Communications Assistance to Law Enforcement Act) did not: to tap Internet communications under very lax conditions.

The position of the US has become considerably stricter in order to avoid possible misuses of the Internet resources; the effect on on-line privacy is certainly not positive. On-line privacy, however, is not an isolated issue for every single country (as conventional privacy can be); it is a necessarily transnational one, since the lack of borders in cyberspace forbids isolation of a certain community (as discussed in chapter 2). The US, however, being one of the protagonist agents affecting Internet attitudes and technology, is probably in a position to affect the whole Internet community through its attitude, certainly more than any other single country would be able to do. As a result, the events of 9/11 2001 are possibly going to affect on-line privacy in general, and not simply the on-line privacy of American users. There is little doubt that the US government has the power to affect decision making in a worldwide scale and, as a result, the events of 9/11 2001 considerably eliminate the possibility of an international agreement for the respect of on-line privacy to be achieved.

That does not mean of course that there is no hope for a change of attitude in the future. This author wants to believe that there will come a point - sooner or later - where it will be inevitable for the international community to come up with an international convention with regard to privacy (and possibly other rights and liberties as well) on the Internet. It is in the nature of cyberspace to be impervious to unilateral regulation, to resist the imposition of rules that generate from a single country. As was seen in chapter 2 (page 61), for example, there is no point to restrict the operation of anonymous remailers in a country since its citizens can equally use those operating in foreign countries. Of course, the negative stance of a single country has the ability to affect the whole Internet community (especially when this country is the US), but an optimistic way of thinking would suggest that the rest of the world has the power to stop the US from rendering cyberspace a controlled area with little space for privacy. Above all, we should not underestimate the power of Internet users and their potential to mould the evolution of cyberspace.

Chapter 8
Conclusions

Reaching the final part of the thesis, one wonders what is the overall outcome of the analysis, and whether it has managed to give specific answers to the question of how far governments should interfere with on-line privacy and in what way. The thesis tackled various issues, connected one way or another with the questions posed at the beginning, and each chapter reached an individual conclusion; so at this final stage we need to look at the total and combined outcome that emanates from the whole of the preceding analysis.

To sum up, the research carried out addressed the issue of on-line privacy and tried to examine the steps that ought to be followed in order for a governmental interference with this right to be drafted in the best possible way. There is no doubt that the target of any policy should be to respect the balance between users' need to preserve their privacy in the on-line environment, and the need of society to combat computer-related crime and other forms of abuse that take place in cyberspace. The route that has been chosen here in order to achieve this balance may not be the ideal one, but one encompassing the major issues that demand questioning in the process of drafting a policy or law. As was underlined in the introduction, the aim of the thesis is not to propose this policy or law as such, but rather to trace the steps to be followed in order to achieve an acceptable solution.

8.1 The problems of the current approach

It was made clear throughout the thesis that the current approach to governmental interference with on-line privacy presents several problems. Let us take a look at those problems. First and foremost, there is no consistent approach to the issue, even though the Internet is a transnational environment with a special nature that demands a uniform approach of a global scale (however impossible this may sound). What has been observed up to now is a tendency of governments to rush into emergency and individual legislation, whenever they try to address a certain problem or implement a certain policy concerning the Internet, legislation that affects on-line privacy directly or indirectly. This was clearly shown, for example, in chapter 5 that discussed cryptography. Being one of the most sizeable sources

of encryption products, the US made persistent unilateral efforts to restrict the free circulation and use of strong encryption through strict export controls and key-escrow proposals. The US also tried to promote its policy outside its territory, in an effort to affect the worldwide circulation of strong encryption. As discussed in chapter 5, the US used its power persistently in an effort to persuade the OECD to include key-escrow or key-recovery in its *Guidelines on Cryptographic Policy* (page 150), and it remains one of the countries that strongly affect decision-making within the *Wassenaar Arrangement* (page 138). These are unilateral efforts that managed to affect on-line privacy on a global scale. Nevertheless, unilateral efforts are doomed to fail in the long run, however effect they might have in the on-line environment. For example, export controls of strong encryption have admittedly slowed down its global dissemination, but have not managed to hinder it in its entirety; strong encryption software is circulating through the Internet. As repeated many times in the thesis, the transnational nature of the Internet calls for a generalised approach on the issue of on-line privacy, emanating from the entirety of the global community.

Second, there is a tendency to undervalue privacy as a considerable value in the on-line environment. Most of the relevant laws affecting on-line privacy were adopted without privacy being one of their major concerns. For example, RIPA 2000 was adopted by the UK government in order to fill the legislative gap of Investigatory Powers for new technologies in the UK, rather than to address the issue of on-line privacy. That is why, even though this law is a positive step, it overall failed to take into account the special needs of on-line privacy. As was seen in chapter 6, RIPA *inter alia* requires from ISPs to create and maintain interception capabilities in their systems (page 164), it opens up possibilities of mass surveillance (page 166), it allows the collection of communications data under lax conditions (page 174), it makes encryption keys accessible to the government without providing sufficient safeguards against abuse (page 185), and it fails to set up an efficient system of oversight to protect people against abuse (page 188). All these indicate that the protection of on-line privacy was not one of the major concerns for the government, but rather an issue that was touched upon as a necessary consequence. The tendency to undervalue privacy has also become obvious through cryptography regulation: neither the US nor the EU designed their cryptographic policies by taking into serious account the fact that encryption is one of the major tools for the protection of privacy in the on-line environment (chapter 5). They rather confined their concern in its role as a tool to conceal criminal activity and, as such, a hindrance to law enforcement agencies.

Third, governments tend to show a lack of concern for users and their privacy, whereas they are greatly influenced by e-commerce and industry interests. For example, as was seen in chapter 5, the US government decided to relax restrictions in export controls of encryption products mainly due to strong complaints by manufacturing companies about the adverse effect of these measures on the competitiveness of their products in the world market, especially after the EU loosened its own restrictions and created a license-free zone, where encryption products would circulate without restrictions (pages 141). It was the first time that the US government decided to relax its policy, even though several cyber-rights groups had expressed privacy concerns many times in the past (page 144). The EU itself did not create this license-free zone due to privacy concerns, but rather to facilitate the circulation of encryption products and promote the competitiveness of its industry in the world market.

Apart from e-commerce and industry needs, governments also tend to undermine on-line privacy for the sake of diplomacy, meaning the existence of systems of covert surveillance. As discussed in chapter 7, there is a considerable number of covert surveillance systems, created and maintained by the secret services of countries, with *Echelon* being the most powerful and the one with the widest range (according to the information that have seen the light of publicity). The existence of interception systems that target on-line behaviour and communications is one of the most serious threats for on-line privacy, one of the factors that augment its sensitivity and render its protection a vital need. However, governments tend to 'forget' the existence of such systems, and do not hesitate to adopt measures that enhance, directly or indirectly, the operation of such systems (such as imposing restrictions in the use of strong and unbreakable encryption). The terrorist attacks of 11 September 2001 in New York and Washington have provided the US with a strong argument to support and reinforce such systems, as they might help in the prevention of future terrorist attacks. This can possibly affect cyberspace as a whole, or at least slow down the process of decision-making, since the US is one of the major factors with the ability to affect decision-making in the Internet community. A US extended ability to intercept e-mail communications and spy on our conduct in cyberspace can affect on-line privacy for every user of this planet.

A further, very serious problem that has become obvious throughout the thesis is that there seems to be a misunderstanding of how law works in the on-line environment and how effective certain measures can be. Cyberspace is an area where no physical borders apply; so when it comes to implementing laws, we have to overcome the problem of inconsistency

between the rules that are in force in different places around the world. But the most important factor that affects the nature of cyberspace and the effectiveness of measures is technology itself. The technical capability of computers is growing with an immense velocity; a new model with double the potential in terms of processing speed and memory capacity becomes available almost every six months. It has become obvious by now that the Internet is an open world of great potential, but it is difficult to foresee its exact route of progress. Technology is one of the greatest challenges for law in the on-line environment. Any legal approach to regulating the on-line environment should be technologically neutral, capable to maintain its original scope and effectiveness by absorbing the constant changes, either of a social or technological nature. Even though aware of this fact, governments do not seem to implement this knowledge in their policies. Let us see some examples of how the effectiveness of measures is affected by the worldwide inconsistency of policies and the constantly changing nature of the on-line environment.

1. Cryptography

Much of the regulatory effort around the world has focused on controlling the dissemination and use of strong encryption, in an attempt to reduce the difficulty of law enforcement agencies to investigate and prosecute crime, caused as a result of the use of unbreakable encryption by suspects. The measures adopted range from export controls, to key-escrow proposals and governmental access to encryption keys. There is little doubt that, even though not radical, such measures (especially export controls) have decelerated the development and worldwide dissemination of strong encryption. Their effect has been strongly felt by legitimate users, either in the personal or commercial environment. Export controls, on the other hand, have not managed to stop the circulation of strong encryption in its entirety, mainly through the Internet. Due to the lack of physical borders, once the genie is out of the bottle (the genie here is strong encryption software), there is little a single government can do to stop it. This means that for people with criminal intentions, the possibility of concealing suspicious communications or exchange of data from prying eyes has not completely vanished. That is, of course, provided they are adequately informed to avoid traps, and skilled to a minimum degree so as to be able to use the strong cryptography that circulates freely. As a result, the effect of such measures for those with criminal intention is comparatively trivial, since they maintain the ability to use strong encryption, even though with an additional effort. The case is different, however, for law-abiding individuals. As we saw in chapter 5, the

measures adopted to prevent the uncontrolled dissemination and use of strong encryption are more likely to discourage legitimate users than criminals, while their actual impact is mainly felt by companies and organisations who use the Internet for their professional activity (page 142).

2. Steganography

The science of cryptology (encryption and cryptanalysis) is not stagnant; new methods of hiding data and breaking codes are constantly developing, reinforced by the spectacular progress in computer capabilities. In other words, it is comparatively easy to overcome the barriers posed by law, by developing alternative techniques. Let us take an example. The effort to eliminate the possibility of concealing data has focused on cryptography, a method based on the concept of hiding the content of a message or data without hiding its existence as such. Anyone who obtains encrypted data will know that there is a key to it somewhere. Apart from the fact that this is an immediate vulnerability, the measures adopted up to the present seem to be drafted on the assumption that cryptography is the only (or at least the standard) method of securing data. Export controls, for example, explicitly target the dissemination of strong encryption, while RIPA's third part is dedicated to the "investigation of electronic data protected by encryption", regulating, *inter alia*, the ability of public authorities to ask for the decryption key.

However, a new technique of electronic information hiding is being developed that, if adequately exploited, can overcome the obstacles created by law on the use of encryption. Steganography[1] is an old art and science of protecting information, based on the concept of hiding the existence of a message or data itself. In its electronic version, steganography works by hiding a message or data in the 'noise' of the digital representation of sound or picture, usually of an innocent or trivial file that attracts no special attention. In effect, files of no particular interest can be exchanged between two parties without anyone knowing what really lies inside them. If it is done properly, it cannot be detected or proven.[2] An image or picture, for example, can contain a letter to a friend; a recording of a short sentence can

[1] See N F Johnson, "Steganography", available at <http://ise.gmu.edu/~njohnson/stegdoc/> (visited on 17/07/2001).not available anymore

[2] See R Anderson, R Needham and A Shamir, "The Steganographic File system" (for stored data in which the existence of a particular file cannot be proven unless both the filename and password are known), available at <http://www.cl.cam.ac.uk/ftp/users/rja14/sfs3.ps.gz> (visited on 17/07/2001) not available anymore.

contain a company's secret plans for a new product. This technique allows the exchange of messages or data without raising any suspicion, and it helps avoid the threat of being asked for the decryption key in the first place. It has to be made clear, however, that electronic steganography is not yet as developed as encryption. Furthermore, it is not a technique developed to replace cryptography; the data hidden in sound or picture files are first encrypted. What steganography can do is augment cryptogrpaphy by obscuring the fact that it has been used in the first place.

As a result, the significance of steganography does not lie in a potential ability to replace encryption (which is certainly not the case as already mentioned), but in the fact that it offers a serious solution for those who have a good reason to use encryption and still be sure that their communications will be kept away from any possible access by public authorities. On the other hand, simple encryption for both security and authentication purposes is widely recognised and utilised in the electronic environment; there is no doubt that it forms an integral part of Internet applications in many ways. That is why restriction in its use will most likely affect legitimate users, while the existence of sophisticated techniques, like steganography, are bound to benefit those with questionable intentions. Its mere existence poses a serious question mark on the measures adopted: how viable is it to eliminate the general potential of using encryption, as a measure to deter criminals from taking full advantage thereof, without taking into account techniques that may allow for undetected use of strong encryption? One could reasonably argue here that steganography or other techniques are not as developed as cryptographic tools, and they do not offer a valid solution, which is not far from the truth. However, the adoption of measures deterring the use of strong encryption will make sure that such solutions are exploited and developed as far as possible.

But we do not need to go that far in order to realise that there are considerable flaws in several measures. Apart from using technically complicated techniques to conceal communications on the Internet, there is a much more simple solution. A person may well resort to more conventional techniques in order to avoid giving away incriminating information. Perhaps the easiest way to communicate securely is by using conventional encryption, meaning a verbal code that would make sense only for those who know it. The perpetrators of the 11/09/2001 attacks may have used the Internet, exchanging messages written in a verbal code that only they could understand. Of course this is not a convenient technique to exchange big amounts of information, or data in the form of images or sound.

But it is still a possibility indicating that the law, as drafted at present, is certainly not a panacea to the problems related with the use of strong encryption.

3. The new Internet Protocol - IPv6

Steganography is certainly not the only technological advance that may render the measures adopted ineffective. Let us turn to another issue. Provisions regulating governmental access to keys are based on the assumption that encryption and decryption are applied by users or communicating parties, which is indeed the case at present with the Internet Protocol currently in use (IPv4). To make things clear, an Internet Protocol is a 'pre-agreed' set of principles that lays down the way in which two computers in a network are going to communicate with each other. The current Protocol was designed in the late 1960's to serve the needs of the then newborn Internet. Roughly described, its function is based on the idea that every information to be transmitted is divided into many small pieces (packets) that travel independently through the network bearing their origin and destination address. IPv4, however, is gradually becoming inadequate for the needs of the continuously expanding Internet; the reason is that it is running out of addresses, even though it can support more than 4 billion unique ones (it has a 32-bit address field)! In effect, a new Internet Protocol is being developed and progressively deployed, that is likely to become the universal standard for IP data exchange well before the end of this decade.

The new protocol, IPv6,[3] is designed to solve the issue of addresses by enlarging the number of bits in the address field from 32 to 128. Thus, the IPv6 address space is larger than anyone can imagine; it is enough to provide a billion billion addresses for each square metre of the earth's surface.[4] However, apart from expanding the address field, the designers of the new Protocol were given the chance to improve it in many more respects, taking into account the needs of the Internet in its new role as a worldwide communications medium. What is of greater interest for our analysis is that IPv6 is designed to have security integrated into the system; roughly described, it will allow two Internet-connected computers to negotiate, use and destroy unique encryption keys for each data exchange. This means that encryption will

[3] See W Stallings, "IPv6. The New Internet Protocol", available at <http://www.cs-ipv6.lancs.ac.uk/ipv6/documents/papers/stallings/> (visited on 26/04/2002).
[4] See B Frezza, "Where's all the outrage about the IPv6 privacy threat?", October 4, 1999, Internetweek.com, available at <http://www.internetweek.com/columns/frezz100499.htm> (visited on 12/11/2001).not available anymore

be used without the active participation of users, who will not be in possession of the key used to secure their communications and therefore unable to comply with a decryption or handing over of key notice, as is currently the case under RIPA for example.[5] This protocol will provide secure encryption using keys that cannot be seized or reused and will protect the confidentiality of all the traffic between the computer systems involved.

But this is only one side of the coin. The content of the information travelling through the network may be protected under the new Protocol, but the traffic data accompanying this information will be exposed by default. In other words, the fact that two parties are establishing some kind of communication will be revealed by default.[6] How is this done? It has to do with how the addresses are distributed. In essence, what is happening is that the 64 bits of the address are going to contain information permanently connected with a certain machine, and, in effect, with a certain user (unless of course more than one person has physical access to the equipment). So every packet sent out onto the public Internet using IPv6 has the fingerprints of its sender on it. Further, unlike IP addresses under IPv4, which can change, these addresses are embedded in every user's hardware.[7] Traffic data, in effect, will be easily gathered by eavesdroppers, for whatever reason, with no special effort, and without the necessary participation of ISPs.[8] The collection of traffic data, as discussed in the second chapter, is no less intrusive upon privacy than eavesdropping on the content of the information travelling through the Internet. In effect, what the new Protocol is doing is protecting by default one aspect of on-line privacy, while at the same time exposing another.

Even though it is impossible to foresee how far the introduction of this protocol will eliminate the use of conventional encryption, its mere development is indicative of the fact that the introduction of laws based on the assumption that the Internet works in a standard way may prove ineffective. It is of course understandable that for laws regulating a certain

---

[5] See I Brown and B Gladman, "The Regulation of Investigatory Powers Bill - Technically inept: ineffective against criminals while undermining the privacy, safety and security of honest citizens and businesses", available at <http://www.fipr.org/rip/RIPcountermeasures.pdf> (visited on 26/04/2002).

[6] See A Escudero, "Comments to the working document of the Temporary Committee on the ECHELON Interception System (European Parliament)", June 2001, available at <http://www.it.kth.se/~aep/publications/echelon-wd-comments-escuderoa.pdf> (visited on 26/04/2002).

[7] See B Frezza, *supra*, note 4.

[8] See also A Escudero, "Privacy in the next generation Internet - Data protection in the context of the European policy", (a Doctoral Dissertation Proposal at the Royal Institute of Technology, Sweden),

conduct it is the present practice that is taken into account. For an environment like the Internet, however, which undergoes substantial changes in very short periods of time, it is essential to take into account at least those developments that are presently under way. When IPv6 replaces the existing protocol, certain laws may need to undergo a significant change in order to serve their initial scope, and this may also be the case with other Internet technologies that are currently under development.

The examples cited above to indicate the inherent nature of the Internet, as an unremittingly changing environment and the extent to which this nature may erode the effectiveness and necessity of the various regulative efforts, are certainly not the only ones. An all-encompassing and more detailed analysis, however, would demand much better technological and scientific knowledge. These examples bring out a further problem of the current approach of governments towards on-line privacy. Regulators seem to have failed to comprehend (much more to put it into practice) that, if law is to achieve its target, it should influence the way the Internet itself works, in other words the way it is actually designed. Until now many laws regulating or affecting conduct in cyberspace have been drafted around the world. One of their common characteristics (maybe the only one) is that they regulate the Internet by taking the way it works now as a granted. None of them is drafted so as to achieve its scope by influencing, and maybe change the way the Internet itself is designed. This idea of regulating the architecture of the Internet is not new. According to Lessig, cyberspace has an architecture: its code – meaning the software and hardware that defines how cyberspace is.[9] In order to regulate cyberspace in an effective way, one should regulate at its core, targeting this code and not user conduct, commercial practice, the industry or other external factors; in other words, without taking as granted the way cyberspace is designed at present. To use one of the above examples: if governments want to implement their policies in a successful way, (say for example that they decide to promote the protection of on-line privacy by regulation), one of the targets of their regulation could be the new Internet Protocol IPv6. As already described, this Protocol is going to have encryption integrated into the system but will reveal by default the communications data of the user. According to this author's point of view, instead of regulating after IPv6 is in use, governments could implement their policy by regulating how this Protocol should be designed. Instead of drafting laws to prohibit the

available at <http://www.it.kth.se/~aep/publications/phd-proposal/dissertation-proposal-escuderoa.pdf> (visited on 26/04/2002).

[9] See L Lessig, *Code and other laws of cyberspace* (1999), Basic Books.

abuse of the communications data that will be generated by default once IPv6 is in use, they could prevent this generation of information by regulating the design of IPv6 itself.

This idea may be exaggerating for some scholars, and it is certainly true that it is not the simplest answer to the question of how to regulate cyberspace. It presupposes multilateral coordination between countries, and obviously a decision on the basic principles that should be respected. In effect, a very serious question is posed: would regulating the Internet at its core (targeting computer code) be practically achievable at an international level? If we want to be realistic, the answer is that it is extremely difficult, if not impossible. It entails positive will of the international community and close co-operation of all countries in order to achieve global agreement and produce an international treaty that would lay down the principles on which Internet code should be designed and changed when needed. As things stand at present, development of technology in this area is generated mainly from the US, with the EU and some technologically developed countries (such as Japan and maybe China and Russia) to be contributing a small percentage at this progress. These entities have gained this position through effort and persistence; technological development offers power and capacity to influence the global market and politics. It is obvious that reaching an international agreement on regulating Internet code would entail a change of attitude from these entities and a positive will to ignore or degrade state interest for the sake of the international community. In other words, it means giving up a considerable percentage of the strategic advantage gained through being technologically ahead of the vast majority of countries. But even if we accept that there was a way to obtain international will to co-operate for a global regulation of the Internet code, it would still be extremely difficult to agree on the exact rules, taking into account all the different legal traditions and mentalities of the global community. Still, this author wants to believe that there will come a time when an international agreement will be a one-way solution to the issue of protecting privacy and other rights on the Internet.

Overall, it has become obvious that the current approach to governmental interference with on-line privacy is rather problematic. Let us see now what are the positive findings of the thesis that may prove useful in enhancing this approach.

8.2 Enhancing the current approach

As was said at the beginning of the thesis, an understanding of the special nature, features and needs of on-line privacy is an essential starting point before anything else; that is why

chapter 2 was considered indispensable. There is a great gap of comprehension in the current approach towards on-line privacy; governments tend to act without a further study of the needs of on-line privacy. A global study and recognition of its special nature could prove very useful. Chapter 2 tried to explore on-line privacy as such in order to understand its differences and similarities with off-line privacy, and decide what are the special needs of privacy when it is exposed in the on-line environment. It was shown that even though off-line and on-line privacy are the same in terms of the interests they protect, the nature of the latter is considerably affected by the following facts: a) the Internet is an entirely public environment, even though it feels like a private place for the user, b) there is less control over one's communications, information and anonymity, c) private information and communications are much more exposed and threatened than in the real world and d) the burden of preserving one's privacy has shifted towards the user; in other words, it has become an opt-in to privacy rather than an opt-out of it. On-line privacy is vulnerable in a distinctive way: in order to be effectively protected, users have to be well informed of the possible risks and capable of applying measures to avoid them. This procedure is more natural in the off-line environment: any person getting undressed in front of a window would close the curtains to avoid being seen, but not every person visiting a website would read its privacy policy and click on the 'no' button when asked if he wants a cookie to be installed on his computer (provided of course that there is such a choice and the cookie is not installed automatically, in which case he would have to have his browser set up to deny the installation of cookies). So, what we learned in this chapter is that one of the first things that should be taken into consideration is that there is a greater need for information and training on how to protect one's on-line privacy, at least until we reach a point where these things will be considered as a default. Second, since there is greater need of positive steps to protect one's privacy, users should not be deprived of the technology that enhances privacy protection, at least not without a good reason and only to an acceptable extent.

The second positive finding of this thesis derives from chapter 3. This chapter tried to explore the most popular reason that is used by governments as a justification to interfere with on-line privacy: computer-related criminality. Identifying the nature of this phenomenon will help governments realise which is the most effective way to fight it. It is true that computer-related criminality is a growing problem for modern societies, but that does not necessarily mean that there is an overall increase of criminal activity in general. The more people are using information technology for legal purposes, the more it is becoming a facility

attractive for those with criminal intentions. It is difficult to draw definitive conclusions on how big a problem computer crime is, since there are no reliable statistics available. Things, however, are more complicated than simply deciding to implement measures restricting privacy, as a measure to combat this type of criminality. Policy choices should be based on the factor of necessity and proportionality, as already discussed, and any measure should be at least capable of achieving the intended result. This means that governments need to take a closer look at the problem of computer crime before deciding which is the best way to fight it. Criminal activity on the Internet has a special nature of its own. For example, several surveys have suggested that the majority of system intrusions perpetrated by hackers, are committed for the sheer pleasure of breaking into a system. Another interesting statistic indicates that a large number of system intrusions in companies are actually perpetrated by insiders. In other words, the nature of on-line criminality should be closely observed before deciding which measures are best to deal with it. Up to present computer-related criminality has been used as an excuse, rather than a justification for interference with privacy. It is not suggested here that no special measures are needed in order to deal with it, but rather that they should be thought through and planned so as to target the special problems that computer crime causes.

The next positive finding derives from chapter 4. This chapter tried to explore how justifications for interference operate within the context of law. National security, public safety and the economic well-being of a country have been examined as the most popular legal justifications that governments tend to use in order to justify interference with otherwise protected rights. The fact that there is no further definition of these terms leaves a wide margin of interpretation for governments, which can construct them so as to cover many situations. This opens up a possibility of abuse and creates insecurity to citizens as far as their rights' protection is concerned. Since the same reasons are probably going to be used to justify interference with rights in the on-line environment, it is useful to know the drawbacks of their application, and make an effort to avoid them.

However, what is of greater interest in chapter 4 is how the European Court of Human Rights has interpreted and applied the conditions under which interference with privacy can be allowed, under Article 8 of the ECHR. The jurisprudence of the ECHR indicates what tests can be set to assess if governmental interference with on-line privacy is proportionate to the threats posed by on-line criminality, terrorism etc. It is interesting to note that, although the

Court has shown unwillingness to challenge the reasons presented by governments as such, it has been stricter as far as the other conditions are concerned. In order for an interference to be acceptable it has to be based on a law that is clearly drafted, adequately accessible and foreseeable for the citizens. Furthermore, interference should be proportionate to the aim pursued (which means that not any measure would be acceptable) and sufficient guarantees against abuse should exist. Given the fact that the ECHR is one of the most complete and effective documents for protection of human rights, these rules can be a useful starting point for the drafting of a policy or law regulating governmental interference with privacy in the on-line environment.

Following the ECHR formula, this law should be drafted so as to leave no doubt about its content, be easily accessible for users and create a certainty as to what is going to happen in case it is breached. More importantly, however, interference will be allowed only to the extent that is proportionate to the aim pursued, which means *inter alia* that no measure will be adopted if it is proved that it cannot achieve its intended scope or it limits user privacy more than necessary. This way, we make sure that measures whose effectiveness is negatively affected by the way the Internet is designed, as discussed above, will not be chosen. As was seen in chapter 5, export controls on cryptographic products and key-escrow proposals have had a much more profound effect for law-abiding users than for those with criminal intentions; as discussed at pages 137-138, restrictions on the availability and use of strong encryption can have an impact on the mentality of users, who can be easily dissuaded from using it, if obtaining and operating it becomes even more complicated. Similar situations may be avoided by following this formula. Last, following the ECHR formula of interference will make sure that adequate guarantees against abuse are in force, and possibly a form of dispute settlement in case user privacy is interfered with above the acceptable limits.

It is true that applying this formula sounds rather radical for an environment such as cyberspace. There are many practical difficulties in its application such as the need to reach a global solution and implement a multilateral policy, or the problem of enforcing this policy on a global scale. Apart from that, it is very difficult to form rules and norms that could work in cyberspace, due to the fact that the formulation of such rules and norms has not followed (at least not until now) the standard process of the off-line environment.

8.3 Privacy and the rules and norms in cyberspace

Overall, it has become clear that on-line privacy is not a different or lesser right compared to its off-line counterpart. However, cyberspace started and still operates as an independent environment; it is not perceived as an 'extension' of the real world but as an autonomous environment, which operates under its own rules and norms. These rules and norms were not decided and imposed by external factors, but were gradually created within cyberspace through the process of its evolution. Of course, cyberspace is not autonomous from people, since it was created and is operated by them, but is independent (or at least started as such) from the rules and norms that people apply in their real world. This situation, however, is in a process of change; the Internet has evolved from a free unregulated area to a medium of everyday life, encompassing a great deal of both professional and personal activity. In effect, its rules and norms are being transformed in order to accommodate the needs of people who use cyberspace to do things equivalent to their off-line activities. In other words, the rules and norms of the real world are starting to find their way into cyberspace. It has to be pointed out that this is not an automated process, but one that requires the active intervention of people. It is in this context that discussion about on-line privacy becomes relevant. Privacy is a well-recognised and protected human right in the real world, but the respect it deserves has not been automatically transferred to cyberspace. Some people have even suggested that there is no such thing as privacy in the on-line environment. Needless to say that this author is not in agreement with this position; the respect it is afforded in the real world should be transferred to cyberspace as well, accommodating the special needs that the new environment creates.

The process of transferring the rules and norms of the real world to cyberspace is not as simple as it seems, however. We cannot just implement in cyberspace whatever is in force for the real world, because not everything is equivalent. The inexhaustible possibilities and immense capabilities offered in the on-line environment render it a field not very susceptible to regulation. The speed at which facts change and new alternatives develop tends to undermine the effectiveness of measures adopted, if not render them rather useless in the long run, as already discussed above (pages 220-222). On the other hand, as more and more people move towards the on-line environment, the safeguard of fundamental rights such as privacy becomes all the more important. There is no doubt that a certain degree of compromise is indispensable in order to protect other vital interests as well, such as national

security, public safety or the ability to investigate and prosecute crime. The measures adopted, however, should be at least *capable* (if not necessary or proportionate) of achieving the intended result. It is this *capability* that the above-described nature of the on-line environment mostly affects. A big question mark is posed on the ability of adopted policies and laws to achieve the target for which they were initially drafted.

Overall, it seems to me that, as far as the Internet is concerned, there is a lack of basic rules and norms. Up to the present, the procedure of regulating cyberspace has followed an opposite route: legislation is drafted on the base of the particular needs of a given time or problem, while there is a complete lack of theoretical principles on which the regulation is based. Privacy may be considered as a human right deserving protection in the off-line world, but there is not an equivalent recognition of its value when we move to cyberspace. There are laws that, one way or another, affect on-line privacy as a right, but there is no uniform basis on which they are based. For example, the Data Protection Directive has a great impact on the protection of on-line privacy, but it has no effect outside the European Union. The evolution of export controls and other measures that affect the dissemination and use of strong encryption has not been based on its use as a tool protecting on-line privacy, but rather on political will and industry needs, as was seen in chapter 5. The result of regulating this way is that there is no uniform protection for on-line privacy in cyberspace. In effect, users find their privacy exposed in a medium they use in their everyday life, where there is a complete lack of norms that would offer them the security of a minimum protection. Given also the fact that there are no physical borders in cyberspace, this exposure has a worldwide dimension. So, what cyberspace lacks are the principles of on-line privacy protection on which specific legislation about interference is going to be drafted.

Technology is a factor that should play a vital role in the future of rules and norms in cyberspace. For the time being, the rapidly changing nature of the Internet has been almost neglected. For example, the way cryptography has been handled (through export controls and proposals allowing governmental access to keys) suggests that the existence of techniques that allow the circumvention of these measures has not been taken into serious consideration. Until now the attitude has been to regulate for the present and leave the future for the future. But the future in cyberspace (in terms of technological developments) comes much quicker than in the off-line world. It is neither in the interest of governments nor citizens to draft legislation with a limited period of validity and a narrow space of effectiveness.

What I am proposing here (the adoption of principles for on-line privacy protection) might be radical for the Internet environment, since one of its initial characteristics was the lack of rules and norms that would regulate its operation. However, since the nature of the Internet has changed and it is not anymore a space cut off from the real world, the need for rules and norms has been created; it cannot operate correctly without them just as a society cannot operate without rules and norms. This point of view comes in complete contrast with a widely disseminated position supporting that rules and norms of cyberspace are created by the medium itself and there should be no intervention by external factors. To avoid misunderstandings, many commentators speak of 'self-regulation' of the medium, but this term refers to the mechanism of adoption rather than the substance of the rules; it can include a broad principled approach but it focuses on the mechanism. What is meant here is the creation (consolidation in the minds of users) of substantive rules and principles through lasting practice. However, this does not seem to be the case any more. First of all, the market itself is imposing its own rules, by guiding user practice. This is not free creation of rules and principles in the medium, because the strongest part of the market is the industry rather than the user. It is the industry that imposes the rules that best serve its interests, rather than users and awareness of their needs. Second, government regulation is another external factor that affects the operation of cyberspace. As we saw throughout the thesis, governments impose rules that do not always take users' rights as their first priority; these laws are very much influenced by industry lobbies and tend to address specific problems that are hindering the operation of law enforcement agencies and other governmental institutions. Of course, these rules are not completely arbitrary, but there is no specific guarantee that a minimum of rights will be respected.

In effect, the optimum way to decide how far governmental interference with on-line privacy can go is by deciding the principles of on-line privacy protection and create laws that would respect the minimum field of protection laid down by these principles. It is difficult to suggest what exactly these principles should be. The first step, according to this author's point of view, is to recognise on-line privacy as a right deserving protection. Then, it has to be decided how far this protection should go when other rights or collective interests are at stake. The special nature of the Internet and how it affects on-line privacy should play a prominent role in the formation of these principles; for example, the fact that users are less aware of the dangers to which their on-line privacy is being exposed can be taken to suggest that a positive effort to inform users of these dangers is always essential. The changing nature

of the Internet and how it affects the effectiveness of adopted measures should also play a major role. A 'humble' example of such principles could be the following:

- On-line privacy is a recognised right deserving protection. It includes personal information spread in or through cyberspace, on-line communications of all kinds (such as e-mail, Internet telephone, video contact etc.) and on-line behaviour.
- Interference with (this also means regulating technology that affects on-line privacy, such as cryptography etc.) or compromise of on-line privacy is allowed only when done for an acceptable reason, there is proven connection between this reason and the compromise of the right, it goes so far as necessary for the needs of each situation, the measures adopted are proven to be effective, and there are adequate safeguards against abuse.
- Users should be constantly informed that their on-line privacy is being compromised and how.
- When positive steps need to be followed by users in order to protect their on-line privacy, these should be addressed to the average user and be as simple as needed to avoid discouraging users from protecting their right.
- On-line privacy should be kept an opt-out rather than an opt-in right; meaning that it should be the default, a right that the user might decide to give away in certain circumstances, rather than an option that users need to take many steps in order to acquire.
- Simplicity should be the target in user interface.
- The private factor/ market should also abide by the principles of protecting on-line privacy.
- When Internet code is changed, it should be designed so as to respect and promote the vested protection of on-line privacy.
- The design of new technological applications in cyberspace, affecting on-line privacy, should respect the protection of on-line privacy as laid down by these principles.
- Internal legislation of a country affecting on-line privacy should take into account the global nature of cyberspace (that may have as a result either possible ineffectiveness of a measure, or unwanted effect outside the country's territory).

The principles that are being suggested here do not include a catalogue of the exact reasons

that will allow interference with on-line privacy, even though this issue has been greatly extended in Chapter 4 of this thesis. That is because such a catalogue will probably include the usual national security, public safety, economic well-being of a country and the detection of crime. The only suggestion this author would like to make is that these vague terms should be escorted by well-thought and clear definitions so as to limit the possibility of being interpreted so as to cover any possible situation.

What I am suggesting here (the adoption of principles in an international level that every country should respect and implement in its internal law) is a solution that would probably be more familiar to countries with a Continental tradition, in a sense that it requires positive regulation of a right as the first step. Common law is very much based on the creation of legal rules through practice and Court decisions, law usually follows; whereas in the Continental tradition law comes first. However, one way or another, both traditions are familiar with the adoption of principles at an international forum. Especially for the UK, the EU experience has made it follow exactly that: implement by internal law legal principles that are adopted in this wider forum. The reason why I reached this conclusion is that it seems to be the only viable way to implement a minimum of protection for on-line privacy. The ECHR can also work as an example of what I mean by basic principles of protection, although, as far as privacy is concerned, it covers a rather limited sphere compared to the one I suggest should be covered in cyberspace.

The questions are, of course, who is going to decide these principles and how are they going to be implemented? The most obvious idea that comes to mind is that, since an international agreement is needed, these principles should be decided in an international forum and maybe take the form of a treaty. I know that this idea sounds exaggerated, especially for a jurisdiction such as the UK, where it is only very recently that a Human Rights Act implementing the ECHR was finally adopted. One could even argue that, even if there were a viable way to draft these principles, it would be almost impossible to implement them. Admittedly, the Internet is an area not very susceptible to regulation and control, since it is 'open' for everyone and from everywhere. No rules or principles can be implemented unilaterally. Additionally, the events of 11 September 2001 have made this possibility even more elusive. As discussed in the previous chapter (page 212), the international community, with the US and UK in a leading role, has turned its focus on combating international terrorism with any cost. Under these circumstances, in striking the balance between

protecting on-line privacy and combating terrorism, the scale is for the time being bending towards the latter irrespective of the cost to the former. Even though the perspectives of the near future remain gloomy, this author wants to believe that there is still hope for an international agreement on on-line privacy, an outcome that might become a one-way solution in the future if we want the Internet community to be viable.

References

A. Books

1) J Adams, *The financing of terror*, New English Library 1986

2) P E Agre and M Rotenberg (editors), *Technology and Privacy: The New Landscape* (1998), MIT Press

3) Y Akdeniz, C Walker and D Wall (editors), *The Internet Law and Society*, Pearson Education Limited - Harlow 2000

4) D Bainbridge, *Introduction to Computer Law* (2000), Longman 4th ed

5) D Ball and R Richelson, *The Ties That Bind: Intelligence Co-operation Between the UKUSA Countries*, Boston: Allen & Unwin, 1985

6) H Barnett (editor), *Constitutional and Administrative Law* (1998), Cavendish Publishing Ltd / London-Sydney L Lustgarten and I Leigh, *In from the Cold: National Security and Parliamentary Democracy* (1994), Clarendon Press / Oxford

7) N Barrett, *Digital Crime - Policing the Cybernation* (1997), Kogan Page Editions

8) P Birks (editor), *Privacy and Loyalty* (1997), Clarendon Press - Oxford

9) C Bowden and Y Akdeniz, *Liberating Cyberspace: Civil Liberties, Human Rights and the Internet* (1999), Pluto Press, Liberty Editions

10) Bradley and Ewing (editors), *Constitutional and Administrative Law* (1997), 12th edition, Longman / London and New York

11) S A Brands, *Rethinking Public Key Infrastructures and Digital Certificates*, The MIT Press 2000

12) I Cameron, *National Security and the European Convention of Human Rights* (2000), Kluwer Law International

13) E Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet,* Academic Press, San Diego 2000

14) R Clarke and J Cameron (editors), *Managing Information Technology's Organisational Impact* (1991), North-Holland

15) R Clayton and H Tomlinson, *Privacy and Freedom of Expression* (2001), Oxford University Press

16) B Clough and P Mungo, *Approaching Zero: Data Crime and Computer Underworld*, Faber and Faber, London 1992

17) Lord Clyde, P.C. and D J Edwards, *Judicial Review*, Scottish Universities Law Institute Ltd, Edinburgh/ W. Green 2000

18) F B Cohen, *Protection and Security on the Information Superhighway* (1995), New York: Wiley

19) J DeCew, *In Pursuit of Privacy. Law, Ethics, and the Rise of Technology* (1997), Ithaca: Cornell University

20) D Denning, *Information Warfare and Security*, ACM Press, Addison-Wesley (New York 1999

21) D E Denning and P J Denning, *Internet Besieged - Countering Cyberspace Scofflaws*, ACM Press 1998

22) W Diffie and S Landau, *Privacy on the Line*, The MIT Press 1999

23) R Dworkin, *Taking Rights Seriously*, London: Duckworth, 1977

24) E Dyson, *Release 2.0: A Design for Living in the Digital Age* (1997), Viking/Penguin Group

25) L Edwards and C Waelde (editors), *Law and the Internet: Regulating Cyberspace* (1997), Hart Publishers / Oxford

26) L Edwards and C Waelde (editors), *Law & the Internet - A Framework for electronic commerce*, 2nd edition, Hart Publishing 2000

27) A Etzioni, *Limits of Privacy* (1999), Basic Books US

28) D Feldman, *Civil Liberties and Human Rights in England and Wales,* Oxford University Press 2002, 2nd edition

29) S Furnell, *Cybercrime – Vandalizing the Information Society*, Addison – Wesley, Boston 2002

30) A Gauntlett, *Net Spies - Who's Watching you on the Web?* (1999), VISION Paperbacks

31) P N Grabosky and R Smith, *Crime in the Digital Age (Controlling telecommunications and cyberspace illegalities)* (1998), Transaction Publishers / The Federation Press

32) P N Grabosky, R G Smith and G Dempsey, *Electronic Theft – Unlawful Acquisition in Cyberspace*, Cambridge University Press 2001

33) K W Grewlich, *Governance in Cyberspace - Access and Public Interest in Global Communications*, Kluwer Law International, 1999

34) N N Gringras, *The Laws of the Internet* (1997), Butterworths London / Edinburgh / Dublin

35) N Hager, *Secret Power: New Zealand's Role in the International Spy Network*, Nelson, New Zealand: Craig Potton Publishing, 1996

36) D J Harris, M O'Boyle and C Warbrick, *Law of the European Convention of Human Rights* (1995), Butterworths – London

37) M Henry (editor), *International Privacy, Publicity & Personality Laws* (2001), Butterworths

38) T E Hill Jr, *Autonomy and Self-Respect,* Cambridge: Cambridge University Press, 1991

39) B Hoffman, *Inside Terrorism* (1999), London: Indigo

40) B Kahin and C Nesson (editors), *Borders in Cyberspace - Information Policy and the Global Information Infrastructure* (1997), MIT Press

41) C E A Karnow, *Future Codes: Essays in Advanced Computer Technology and the Law*, Artech House, Boston 1997

42) M E Katsh, *Law in a Digital World* (1995), New York: Oxford University Press

43) B J Koops, *The Crypto Controversy - A Key Conflict in the Information Society*, Kluwer Law International 1998

44) H Kushner (editor) *The Future of Terrorism: Violence in the New Millennium* (London: Sage Publication 1998

45) L Lessig, *Code, and other laws of cyberspace* (1999), Basic Books

46) S Levy, *Hackers: Heroes of the Computer Revolution*, Anchor Press – Doubleday 1984

47) B Loader (editor), *The Governance of Cyberspace*, Routledge London and New York 1997

48) S Lukes, *Individualism,* Oxford: Basil Blackwell, 1973

49) V Markesinis, *Protecting Privacy* (1999), Oxford University Press

50) J Michael, *Privacy and Human Rights (An International and comparative study, with special reference to developments in information technology)* (1994), UNESCO

51) P Newman, *Computer Related Risks* (Reading: Addison Wesley 1994

52) Norris, C. and Armstrong, G., *The Maximum Surveillance Society – The Rise of CCTV*, Berg Oxford 1999

53) Norris, C., Moran, J. and Armstrong, G. (editors) *Surveillance, Closed Circuit Television and Social Control*, Ashgate - Aldershot 1998

54) T A Peters, *Computerised monitoring and on-line privacy* (1999), McFarland & Company Inc., Publishers

55) B Schneider, *Applied Cryptography*, edited by John Wiley, 1996

56) S Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, 1999 Fourth Estate – London

57) A D Soafer and S E Goodman (editors), *The Transnational Dimension of Cyber Crime and Terrorism,* Hoover Institution Press - Stanford, 2001

58) D Thomas and B D Loader, *Cybercrime –Law Enforcement, Security and Surveillance in the Information Age,* London: Routledge 2000

59) J Wadham and H Mountfield, *Blackstone's Guide to the Human Rights Act 1998* (2000), Blackstone Press Ltd

60) D S Wall, *Crime and the Internet: Cybercrimes and Cyberfears*, London: Routledge 2001

61) J R White, *Terrorism: An Introduction* (1998), 2nd ed., Belmont, CA; London: West / Wadsworth

62) P Wilkinson (editor), *Technology and Terrorism* (1993), London: Frank Class

B. Articles

1) S Aftergood, "Intelligence versus the Rule of Law", (2000) 84 *Secrecy & Government Bulletin*

2) Y Akdeniz, "No Chance for Key Recovery: Encryption and International Principles of Human and Political Rights", (1998) Web Journal of Current Legal Issues 1, available at <http://webjcli.ncl.ac.uk/1998/issue1/akdeniz1.html>

3) Y Akdeniz, N Taylor and C Walker, "Regulation of Investigatory Powers Act 2000 (1): BigBrother.gov.uk: State Surveillance in the age of information and rights", (2001) *Criminal Law Review* (February)

4) R Anderson and others, "The Risks of Key Recovery, Key Escrow & Trusted Third Party Encryption", A Report by an ad hoc Group of Cryptographers and Computer Scientists, at <http://www.cdt.org/crypto/risks98/>

5) R Anderson, R Needham and A Shamir,"The Steganographic File system", available at <http://www.cl.cam.ac.uk/ftp/users/rja14/sfs3.ps.gz>

6) S Andrews, "Who Holds the Key? - A Comparative Study of US and European Encryption Policies", (2000) *Journal of Information Law and Technology*, issue 2

7) T A Baloch, "What Price for Privacy?", (2001) *New Law Journal* 50

8) D Banisar,"Big Brother Goes High-Tech", (1996) *Covert Action Quarterly* 56 (Issue of Spring 1996), available at <http://www.media-awareness.ca/eng/issues/priv/reso.../brother.htm>

9) M H Barrera and J M Okai, "Digital Correspondence: Recreating Privacy Paradigms", (1999) 3 *International Journal of Communications Law and Policy*, available at <http://www.digitallaw.net/IJCLP/3_1999/pdf/ijclp_webdoc_4_3_1999.pdf>

10) T E Black, "Taking Account of the World as it will be: The Shifting Course of US encryption Policy", (2001) 53 *Federal Communications Law Journal* 289

11) N Bogonikolos, "The Perception of Economic Risks Arising from the Potential Vulnerability of Electronic Commercial Media to Interception", part 1 of A Scientific and Technological Options Assessment conducted by STOA for the European Parliament ("Development of Surveillance Technology and Risk of Economic Information" an appraisal of technologies of political control), available at <http://cryptome.org/dst-1.htm>

12) L D Brandeis and S D Warren, "The Right to Privacy", (1890) 4 *Harvard Law Review* 193

13) I Brown and B Gladman, "The Regulation of Investigatory Powers Bill - Technically inept: ineffective against criminals while undermining the privacy, safety and security of honest citizens and businesses", available at http://www.fipr.org/rip/R/Pcountermeasures.pdf

14) K Brunnstein, S Fischer-Hübner and M Swimmer, "Classification of Computer Anomalies," Proceedings of the 13th National Computer Security Conference, Washington D.C., 1-4 October 1990

15) A J Campbell, "Self-Regulation and the Media", at <http://www.law.indiana.edu/fclj/pubs/v51/no3/CAMMAC15.PDF>

16) D Campbell, "How the plotters slipped US net", The Guardian / September 27, 2001, available at <http://www.guardian.co.uk/archive/0,3858,4264719,00>

17) D Campbell, "Interception Capabilities 2000", part 4 of A Scientific and Technological Options Assessment conducted by STOA for the European Parliament ("Development of Surveillance Technology and Risk of Economic Information" an appraisal of technologies of political control), at <http://www.iptvreports.mcmail.com/ic2kreport.htmReport>

18) D Campbell, "Somebody's listening", New Statesman 12 August 1988, pp.10-12, available at <http://jya.com/echelon-dc.htm>

19) R Calleja, "The Regulation of Investigatory Powers Act 2000", (2000) *Computers and Law* 21 (August/September)

20) D Carter, "Computer Crime Categories: How Techno-Criminals Operate", (1995) 64 *FBI Law Enforcement Bulletin*

21) R Chandrani, "R.I.P. E-Commerce?", (2000) *Computers and Law* 30 (June/July)

22) H Cleaver, Jr, "The Zapatista Effect: The Internet and the Rise of an Alternative Political Fabric", [Spring 1998] *Journal of International Affairs* 51/2, pp. 20-39

23) P A Collier and B J Spaul, "Problems in Policing Computer Crime", (1992) 2 *Policing & Society* 307

24) P M Dane, "The Spycatcher Cases", (1989) 50 *Ohio State Law Journal* 405

25) D E Denning, "Cyberterrorism" - Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, US House of Representatives, 23 May 2000, at <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

26) D E Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a tool for influencing foreign policy", Internet and International Systems: Information Technology and American Foreign Policy Decision-making Workshop, at <http://www.nautilus.org/info-policy/workshop/papers/denning.html>

27) M Devost, B K Houghton and N A Pollard, "Information Terrorism: Can you trust your toaster?", at <http://www.terrorism.com/documents/suntzu.pdf>

28) M G Devost, "The Digital Threat: United States National Security and Computers", (Paper prepared for presentation at the 1994 Annual meeting of the New England Political Science Association, April 1994), available at <http://www.oss.net/Proceedings/ossaaa/aaa3/aaa3ae.htm>

29) K Di Gregory, "Fighting Cybercrime - What are the challenges facing Europe?"(Meeting before the European Parliament), 19 September 2000, at <http://www.cybercrime.gov/EUremarks.htm>

30) J C Dombrow, "Electronic Communications and the Law: Help or Hindrance to Telecommuting?", at <http://www.law.indiana.edu/fclj/pubs/v50/no3/dombrow.html>

31) M Elliott, "Privacy, Confidentiality and Horizontality: the Case of the Celebrity Wedding Photographs", (2001) 60/2 *The Cambridge Law Journal* 231

32) D Feldman, "Secrecy, Dignity, or Autonomy? Views of Privacy as a Civil Liberty", in *Current Legal Problems* 1994 – Volume 47, Part 2: Collected Papers, edited by M D A Freeman

33) M Figueroa, "Carnivore - Diagnostic Tool or Invasion of Privacy?", 1 September 2000, available at <http://www.sans.org/infosecFAQ/legal/carnivore.htm>

34) A M Froomkin, "Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases", (1996) 15 *U. Pittsburgh Journal of Law and Commerce* 395, available at <http://www.law.miami.edu/~froomkin/articles/ocean1.html>

35) A M Froomkin, "The Death of Privacy?", (2000) 52/5 *Stanford Law Review* 1461

36) W S Galkin, "Privacy issues in the Digital Age", (1996) 29(5) *Maryland Bar Journal* 46

37) R Gavison, "Privacy and the limits of the law", (1980) 89 *Yale Law Journal* 421

38) R M Gellman, "Can Privacy be regulated effectively on a National Level? Thoughts on the Possible Need for International Privacy Rules", (1996) 41 *Vill. Law Review* 129

39) B Gladman, "Wassenaar Controls, Cyber-Crime and Information Terrorism" (A Report by Cyber-Rights and Cyber-Liberties UK, September 1998), available at <http://www.cyber-rights.org/crypto/wassenaar.htm>

40) B Gladman (for the FIPR), "The Regulation of Investigatory Powers Bill - The Provisions for Government Access to Keys", available at <http://www.fipr.org/rip/RIPGAKBG.pdf>

41) B Gladman, "Comments on Preliminary Draft of the Draft Code of Practice on the Investigation of Electronic Data protected by encryption etc", 11th July 2000, available at <http://www.fipr.org/rip/BG_p3copcom.pdf>

42) M D Goodman, "Why the Police Don't Care About Computer Crime", (1997) 10 *Harvard Journal of Law and Technology* 465, at <http://jolt.law.harvard.edu/text/articles/10jolt465.html>

43) P N Grabosky, "Computer Crime: A Criminological Overview", (A Paper prepared for presentation at the workshop on Crimes related to the Computer Network, Tenth United Nations Congress on the prevention of Crime and the Treatment of Offenders, Vienna, 15 April 2000) at http://www.aic.gov.au/conferences/other/compcrime/

44) Graham, S., Brookins, J. and Heery, D., "Towns on Television: Closed Circuit Television in British Towns and Cities" [1996] 22 *Local Governmental Studies* 3

45) T Haershman, "Israel's Seminar on Cyberwar", 10/01/2001 InfoSec News, available at <http://www.securityfocus.com/frames/?content=/templates/archive.pike%Flist%3D12%26mid%3D155550>

46) N Hager, "Exposing the Global surveillance system", *Covert Action Quarterly*, available at <http://public.scre.hr/~mprofaca/echelon01.html>

47) M A Hogg, "The Very Private Life of the Right to Privacy", in H L MacQueen (editor) *Privacy and Property* (1994), 2/3 Hume Papers on Public Policy, Edinburgh University Press

48) T Honess and E Charman, (1992) *Closed Circuit Television in public places*, Crime Prevention Unit paper no. 35. London: HMSO

49) N F Johnson, *"Steganography"*, available at <http://ise.gmu.edu/~njohnson/stegdoc/>

50) D Kelsey, (Newspaper Article) "Survey-Cybercrime Concern Outweighs Precautions", 29 June 2000 Newsbytes, at <http://www.infowar.com/survey/00/survey_062900a_j.shtml>

51) D B Kopel, "Hearings on Wiretapping and other Terrorism Proposals - Testimony", Cato Institute - Committee on the Judiciary US Senate, 24 May 1995, at <http://www.cato.org/testimony/ct5-24-5.html>

52) I Leigh and L Lustgarten, "The Security Services Act 1989", (1989) 52 *Modern Law Review* 801

53) K Lenaerts and E E De Smijter, "A 'Bill of Rights' for the European Union", (2001) *Common Market Law Review* 273

54) C H Lindsey, "Regulation of Investigatory Powers Bill - Some Scenarios", available at <http://www.cs.man.ac.uk/~chl/scenarios.html>

55) B Livesey, "Trolling for Secrets - Economic Espionage is the new niche for government spies", 28 February 1998, at <http://www.infowar.com/class_3/class3_030698a_s.html-ssi>

56) M Maher, "International Protection of US Law Enforcement Interests in Cryptography", (1999) 5 *Richmond Journal of Law and Technology* 13, at http://www.richmond.edu/jolt/v5i3/maher.html

57) D Mahoney and Dr N Faulkner, "A Brief Overview of Paedophiles on the Web", submitted to the Child Advocacy Task Force on *The Internet On-line Summit: Focus on Children*, Washington DC December 1997

58) C Mitchell, "Cryptography: Key Distribution, TTPs and Warranted Interception", (An Occasional Paper published by the Global Transformation Research Group) 1999 Series, 2 / Jan. 1999

59) V Mitliaga "Regulation of Investigatory Powers Act 2000 and the Truth about the Disclosure of Keys" (2001) *E-Law Review* 6, Issue 2/December 2001

60) E A Mohammed, "An Examination of Surveillance Technology and their Implications for Privacy and Related Issues - The Philosophical Legal Perspective", (1999) 2 *Journal of Information Law and Technology*, available at <http://www.law.warwick.ac.uk/jilt/99-2/mohammed.html>

61) M M Mostyn, "The Need for Regulating Anonymous Remailers", (2000) 14/1 *International Review of Law Computers & Technology* 79

62) T Nguyen, "Cryptography, Export Controls, and the first Amendment in Bernstein v. United States Department of State", (1997) 10 *Harvard Journal of Law & Technology* 667

63) H H Perritt Jr and M G Stewart, "False Alarm?", available at <http://www.law.indiana.edu/fclj/pubs/v51/no3/stemac7.PDF>. S Perry, "Economic Espionage - The corporate threat", (Newspaper Article) September 1995, at <http://www.the-south.com/USInternational/econ.html>

64) S Perry, "Economic Espionage - The corporate threat", (Newspaper Article) September 1995, at <http://www.the-south.com/USInternational/econ.html>

65) P S Poole, "Echelon: America's Secret Global Surveillance Network", 1999-2000, available at http://fly.hiway.net/~pspoole/echelon.html

66) J M Post, K G Ruby and E D Shaw, "From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism", [2000] 12(2) *Terrorism and Political Violence* 97

67) W L Prosser, "Privacy", [1960] 48 *California Law Review* 383-423

68) A S Reid & N Ryder, "The Case of Richard Tomlinson: The Spy who E-mailed Me", (2000) 9 *Information & Communications Technology Law* 61

69) T Regan, "When Terrorists Turn to the Internet", 07/04/1999 Infowar.com, available at <http://www.infowar.com/class_3/99/class3_070499a_j.shtml>

70) J B Richards, "Hearing on Cybercrime" (Written Testimony before the US Senate Committee on Appropriations Subcommittee on Commerce, Justice, State and Judiciary) 16 February 2000, at <http://www.internetalliance.org/policy/000216_testimony.html>

71) J Richelson, "Desperately Seeking Signals", (2000) *Bulletin of the Atomic Scientists* March/April 2000, Vol. 56, No. 2, pp. 47-51, available at <http://www.bullatomsci.org/issues/2000/ma00/ma00richelson.html

72) J K Robinson, "Internet as the Scene of Crime", Remarks presented at the International Computer Crime Conference, Oslo - Norway, 29-31 May 2000, at <http://www.cybercrime.gov/roboslo.htm>

73) M Rogers, "Modern-day Robin Hood or Moral Disengagement: Understanding the Justification for Criminal Computer Activity", 1 July 2000, at <http://www.infowar.com/articles/00/article_010700a_j.shtml>

74) J I Rosenbaum, "Privacy on the Internet: Whose Information is it Anyway?", (1998) 38 *Jurimetrics Journal* 565

75) A Rogers, "You Got Mail but Your Employer Does Too: Electronic Communication and Privacy in the 21st Century", (2000) 5/1 *Journal of Technology Law and Policy* 1, available at <http://grove.ufl.edu/~techlaw/vol5/emailfinal.htm>

76) M Savage, "Surveys Shows Growing Losses from Cybercrime", Newspaper Article on the annual survey conducted by the CSI (Computer Security Institution), TechWeb News 5 August 2000 at <http://www.techweb.com/wire/story/TWB20000323S0010>

77) F Schauer, "Internet Privacy and the Public-Private Distinction", (1998) 38 *Jurimetrics Journal* 555

78) E J Sinrod and B D Jolish, "Controlling Chaos: The Emerging Law of Privacy and Speech in Cyberspace", (1999) *Stanford Technology Law Review* 1, at http://stlr.stanford.edu/STLR/Articles/99_STLR_1/

79) G Skok, "Establishing a Legitimate Expectation of Privacy in Clickstream Data", (2000) 6 *Michigan Telecommunications Technology Law Review*, available at <http://www.mttlr.org/volsix/skok.html>

80) W Stallings, "IPv6. The New Internet Protocol", available at <http://www.cs-ipv6.lancs.ac.uk/ipv6/documents/papers/stallings/>

81) B Sullivan, "International Organised Crime: A Growing National Security Threat", (1996) 74 *Strategic Forum* 2

82) N Taylor, "Closed Circuit Television: The British Experience", [1999] *Stanford Technology Law Review* 11

83) A Tomkins, "Public Interest Immunity after Matrix Churchill", (1993) *Public Law* 650

84) S M Thompson, "The Digital Explosion comes with a Cost: The Loss of Privacy", (1999) 4 *Journal of Technology Law & Policy* 3, available at <http://journal.law.ufl.edu/~techlaw/4/Thompson.html>

85) R C Thomsen and A D Paytas, "US To EU: Me Too", available at http://www.t-b.com/cryptoarticle.htm

86) L Valeri and M Knights, "Affecting Trust: Terrorism, Internet and Offensive Information Warfare", [2000] 12(1) *Terrorism and Political Violence* 15

87) J Wadham, "The Intelligence Services Act 1994", (1994) 57 *Modern Law Review* 916

88) G G Yerkey, "Special Report: Export Controls: US Controls on Encryption Software Have Hurt Exporters, Government Finds", (1996) *International Trade Report*, Jan. 17, at 85

89) "The Constitutional Right to Anonymity, Free Speech, Disclosure and the Devil" by anonymous, (1961) 70 *The Yale Law Journal* 1084

90) Testimony of Marc Rotenberg, executive director of the Electronic Privacy Information Centre, Hearing on Privacy in the Commercial World, March 2001, available at <http://www.epic.org/testimony_0301.html>

91) Andrew Shen, on behalf of the Electronic Privacy Information Centre (EPIC), *Online Profiling Project - Comment, P994809 / Docket No. 990811219-9219-01*, available at <http://www.epic.org/privacy/internet/profiling_reply-comment.PDF>

92) TheElectronic Privacy Information Centre (EPIC) survey conducted in 1999, "Surfer Beware III: Privacy Policies without Privacy Protection", available at http://www.epic.org/Reports/surfer-beware3.html

93) Better Regulation Task Force, "Principles of Good Regulation" 2000, (available at <http://www.cabinet-office.gov.uk/regulation/taskforce/2000/PrinciplesLeaflet.pdf>

94) NCIS (National Criminal Intelligence Service), "Year 2000 Report on Organised Crime in the UK", available at <http://www.ncis.co.uk/PDFS/SmallThreatPages1-14.pdf > (15-39.pdf) (40-52.pdf)

95) NCIS (National Criminal Intelligence Service), "NCIS Submission on Communications Data Retention Law", available at <http://cryptome.org/ncis-carnivore>

96) "The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet", A report of the US President Working Group on Unlawful Conduct on the Internet, February 2000 at <http://www.politechbot.com/docs/unlawfulconduct.txt>

97) "Threat from International Organised Crime and Terrorism Before the House of Commons, on International Relations", 105th Cong. 94 (1997) available in 1997 WL 615544 (F.D.C.H.)

98) "United Nations Manual on the Prevention and Control of Computer-Related Crime", available at http://www.hinduja.org/cj.htm

99) Home Affairs Committee, Third Report, Organised Crime (1994-95 HC 978)

100) House of Commons, Northern Ireland Affairs Committee, "The Financing of Terrorism in Northern Ireland", Fourth Report of Session 2001-2, HC 978-1

101) House of Commons, Second Reading of Terrorism Act 2000, 14 December 1999, Hansard Reference Vol 341

102) House of Commons, Northern Ireland Affairs Committee, "The Financing of Terrorism in Northern Ireland", Fourth Report of Session 2001-2, HC 978-1

103) "The UK Threat Assessment 2002", The Threat from Serious and Organised Crime, National Criminal Intelligence Service 2002

104) Rand Report 1999, (prepared by I O Lesser, B Hoffman, J Arquilla, D F Ronfeldt, M Zanini, B M Jenkins), "Countering the New Terrorism", available at <http://www.rand.org/publications/MR/MR989/MR989.pdf/>

105) Cato Institute - Committee on the Judiciary US Senate, 24 May 1995, Testimony of David B. Kopel, "Hearings on Wiretapping and other Terrorism Proposals", available at <http://www.cato.org/testimony/ct5-24-5.html>

106) "*e*Europe 2002", Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*, (available at <http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeCommEN.html>

107) Computer Security Institute (CSI) / FBI, "2001 Computer Crime and Security Survey", available at <http://www.gocsi.com/prelea/000321.html>

108) "2001 Industry Survey", Information Security Magazine - October 2001, available at <http://www.infosecuritymg.com/articles/october01/images/survey.pdf>

109) Computer Crime Survey conducted by Michael G. Kessler & Associates Ltd., see news article at <http://www.ethailand.com/IT/Columns/Siamrelay/computer_crime.html>

110) InterGOV: Latest Web Statistics (2001), available at <http://www.intergov.org/public_information/general_information/latest_web_stats.html>

111) Centre for Democracy and Technology (CDT), "Comments of the CDT on the Council of Europe Draft Convention on Cybercrime", available at <http://www.cdt.org/international/cybercrime/010206cdt.shtml>

112) Electronic Privacy Information Centre, Washington DC, "Cryptography and Liberty 1999 - An International Survey of Encryption Policy", available at <http://www.gilc.org/crypto/crypto-survey-99.htm>

113) Department of Commerce, Bureau of Export Administration, Office of Strategic Trade & Foreign Policy Controls, Inf. Tech. Controls Division, "Commercial Encryption Export Controls - Questions and Answers", available at <http://www.bxa.doc.gov/Encryption/qanda.htm>

114) "Open Letter by Amnesty International to Members of the House of Lords on the RIP Bill", available at <http://www.fipr.org/rip/AmnestyRIPletter.htm>

115) "STAND's Guide to the RIP v1.0", available at <http://www.stand.org.uk/ripnotes/>

116) "Response of the Data Protection Commissioner to the Government's Regulation of Investigatory Powers Bill", available at <http://www.fipr.org/rip/DPCparlRIP.htm>

117) "Advice Paper on the RIP Bill (In the Matter of a Human Rights Audit for Justice and FIPR)", by Justice Tim Eicke of the Essex Court Chambers, available at <http://www.fipr.org/rip/ripaud3.html>

118) "A Further Open Letter to the House of Lords from Cyber-Rights and Cyber-Liberties (UK) concerning the Regulation of Investigatory Powers Bill" (29 June, 2000), available at <http://www.cyber-rights.org/reports/hl-let2.htm>

119) JUSTICE, "Regulation of Investigatory Powers Bill - Secondary Reading Briefing", available at <http://www.fipr.org/rip/Justice%20RIP%20Bill%202nd%20reading%brief.pdf>

120) *"The Economic Impact of the Regulation of Investigatory Powers Bill" (An independent report prepared for the British Chambers of Commerce)*, edited by I Brown, S Davis and G Hosein, available at http://www.britishchambers.org.uk/newsandpolicy/downloads/lsereport.pdf

121) Explanatory Notes to the Anti-terrorism, Crime and Security Act 2001, available at <http://www.hmso.gov.uk>

122) "Your Privacy Ends Here", June 4 2000 The Observer, available at <http://www.observer.co.uk/focus/story/0,6903,328071,00.htm>

123) The Home Office, "Myths and Misunderstandings (Mass surveillance?)", available at <http://www.homeoffice.gov.uk/ripa/mass.htm>

124) Justice's Response to the Government Consultation Paper "Interception of Communications in the United Kingdom", available at <http://www.fipr.org/ioca/justice.pdf>

125) "Draft Report on the existence of a global system for the interception of private and commercial communications (Echelon)", prepared by the Temporary Committee on the Echelon Interception System, 18 May 2001, available at <http://www.bof.nl/docs/echelon_draft.html>

126) "Echelon Furor Ends in a Whimper", (news article by S Ketmann), Wired News 3 July 2001, available at <http://www.wired.com/news/politics/0,1283,44984,00.html>

127) "The Spy in your Server", (news article by D Campbell), The Guardian 10 August 2000, available at <http://www.guardianunlimited.co.uk/online/story/0,3605,352394,00.html>

128) "Frenchelon - France has nothing to envy in Echelon", (news article by J Thorel), ZDNet France 30 June 2000, available at <http://www.zdnet.co.uk/story/printer/0,,s2079875,00.html>

129) "Cybercops Police China", (news article by K Platt), The Christian Science Monitor 17 November 1999, available at <http://more.abcnews.go.com/sections/.../chinacybercops991117.htm>

130) "China Plans to Build Internet Monitoring System", (news article), CND 20 March 2001, available at <http://www.cnd.org/Global/01/03/20/010320-3.html>

131) "Echelon's Counterparts" (last updated and verified on June 28, 2001) in Echelon Watch web page, at <http://www.aclu.org/echelonwatch/networks.html>

C. European Human Rights Court Cases

1) Case *Amann v.Switzerland* (2000) 30 EHRR 843

2) Case *Andersson (M and R) v.Sweden* (1992) 24 EHRR 615

3) Case *Barthold v.Germany* (1985) 7 EHRR 383

4) Case *Berrehab v.The Netherlands* (1988) 11 EHRR 322

5) Case *Buckley v.UK* (1997) 23 EHRR 101

6) Case *Dudgeon v.UK* (1981) 4 EHRR 149

7) Case *Halford v.UK* (1997) 24 EHRR 523

8) Case *Huvig v.France* (1990) 12 EHRR 528

9) Case *Jasper v.UK* (16 February 2000) Appl. No. 27052/95

10) Case *Khan v.UK* (2000) 31 EHRR 45

11) Case *Klass and Others v.Federal Republic Germany* (1979-80) 2 EHRR 214

12) Case *Kopp v.Switzerland* (1998) 27 EHRR 91

13) Case *Kruslin v.France* (1990) 12 EHRR 547

14) Case *Kroon v. Netherlands*, A 297-C 1994

15) Case *Leander v.Sweden* (1987) 9 EHRR 433

16) Case *Lustig-Prean and Becket v.UK* (1999) 29 EHRR 548

17) Case *Malone v.UK* (1985) 7 EHRR 14

18) Case *Marckx v.Belgium* A 31 (13/6/1979)

19) Case *Niemietz v.Germany* (1992) 16 EHRR 97

20) Case *Rees v UK* A 106 (17/10/1986)

21) Case *Rekvenyi v.Hungary* (Appl. no 25390/94) 20/05/1999

22) Case *Rowe and Davis v UK* (16 February 2000) Appl. No. 28901/95

23) Case *Sener v.Turkey* (Appl. no 26680/95) 18/07/2000

24) Case *Smith and Grady v.UK* (1999) 29 EHRR 493

25) Case *Sunday Times v.UK* (1979-80) 2 EHRR 245

26) Case *The Sunday Times v.UK* (1991) 14 EHRR 229

27) Case *Valenzuela Contreras v.Spain* (1999) 28 EHRR 483

28) Case *Vereinigung Demokratischer Soldaten Osterreichs and Gubi v.Austria* (1995) 20 EHRR 56

D. UK and US Court Cases

1) Case *A v B plc* [2002] 2 All ER 545

2) Case *Attorney-General v. Guardian Newspapers Ltd.* [1987] 1 W.L.R. 1248

3) Case *Attorney-General v. Guardian Newspapers Ltd. (No. 2)* [1988] 2 W.L.R. 805

4) Case *Attorney-General v. Newspapers Publishing Plc.* [1987] 3 W.L.R. 942

5) Case *Attorney-General v Blake and Jonathan Cape Ltd*, [2000] 4 All ER 385

6) Case *Balfour v Foreign and Commonwealth Office*, [1994] 2 All ER 588

7) Case *Barasch v. Bell Telephone* 605 A.2d 1198 (Pa. 1992)

8) Case *Bernstein v. United States Department of State,* 922 F. Supp. (1996)

9) Case *Bernstein v. United States Department of State*, 945 F. Supp. (1996)

10) Case *Naomi Campbell v Mirror Group Newspapers Ltd* [2002] EWCA Civ 1373

11) Case *Naomi Campbell v Mirror Group Newspapers Ltd* [2002] EWHC 499 (QB)

12) Case *Gary Flitcroft v MGN Ltd* (2002) 2 All ER 545

13) Case *Katz v United States*, 1967, 389 US 347

14) Case *McDougall v. Dochree*, The Scots Law Times 1992, issue 25, p. 624

15) Case *MacIntyre v. Ohio Elections Commission* 514 U.S. 334 (1995)

16) Case *Messrrs Bindam and Partners, on behalf of Ms Anna Ford and Mr David Scott*, PCC No. 52, 15/09/00

17) Case *R (on the application of Anna Ford) v The Press complaints Commission* [2001] EWHC Admin 683, CO/1143/2001

18) Case *R. v Brentwood Borough Council ex parte Peck* [1998] EMLR 697

19) Case *R v Shayler* [2002] UKHL 11

20) Case *Raffaelli v. Heatly*, The Scots Law Times 1949, p. 284

21) Case *JK Rowling v OK! Magazine* PCC Report No. 56, 17/08/01

22) Case *Jamie Theakston v MGN Ltd* [2002] EWHC 137 (QB)

23) Case *Venables and another v News Group Newspapers* [2001] 1 All ER 908, [2001] 2 WLR 1038.

Appendix A
Publications

The following papers have been either published or submitted to conferences or journals.

Varvara Mitliaga "Privacy in Cyberspace: Identifying the limits of governmental intervention in electronic communications," won the postgraduate Lord Lloyd of Kilgerran essay prize (BILETA 2001). *Submitted for publication to the Journal of Information and Technology Law.*

Varvara Mitliaga "Cyber-terrorism: A call for governmental action?," *Working Paper for the British and Irish Legal Technology Association (BILETA) 16th Annual Conference,* Edinburgh, 9-10 April 2001.

Varvara Mitliaga "Regulation of Investigatory Powers Act 2000 and the truth about the disclosure of keys," *E-Law Review*, Issue 2, December 2001, pp. 6 – 7.

Varvara Mitliaga "Cyberterrorism: a beginner's guide – on the convergence of cyberspace and terrorist activity," *The Legal Executive*, February 2002, pp. 4 – 5.

Varvara Mitliaga "Book review on: *Networks and Netwars: The Future of Terror, Crime, and Militancy* by John Arquilla, David Ronfeldt (editors), RAND Publications 2001," *International Journal of Law and Information*, Volume 10, Issue 2, Summer 2002, pp. 238-9.