Gothenburg Studies in Informatics, Report 36, October 2006
ISBN 91-628-6937-X, ISSN 1400-741x (print), ISSN 1651-8225 (online)

Disruptive Technology

Effects of Technology Regulation on Democracy

Doctoral Dissertation

Mathias Klang

Barba non facit philosophum,
neque vile gerere pallium

GÖTEBORG UNIVERSITY
Department of Applied Information Technology
Box 8718, SE-402 75 Göteborg, Sweden

Abstract

This work develops the thesis that there is a strong relationship between the regulation of disruptive technology and the Internet-based participatory democracy. In other words, attempts to regulate disruptive technology have an impact upon the citizen's participation in democracy. This work will show what this relationship is and its effects on democratic participation.

Taking its starting point from the recent theoretical developments in regulation, disruptive technology and role of ICT in participatory democracy, this work is the application of theoretical discussions on the field of the Internet-based participatory democracy. These theoretical discussions are used in the empirical exploration of six areas: virus writing and dissemination, civil disobedience in online environments, privacy and the role of spyware, the re-interpretation of property in online environments, software as infrastructure and finally state censorship of online information. The purpose of these studies is to explore the effects of these social and technical innovations upon the core democratic values of *Participation*, *Communication*, *Integrity*, *Property*, *Access* and *Autonomy*. The overall research question for this thesis is therefore:

How do attempts to regulate disruptive technology affect Internet-based participatory democracy?

The specific contribution of this thesis is the development of extended understanding of the way in which we regulate disruptive technology. This understanding helps us to better regulate that which is new and threatens that which is established. Additionally, the extended understanding in this field can then be applied to all domains where regulation of technology may occur. This thesis contributes towards a richer understanding in the research areas of e-democracy, technology regulation and disruptive technology.

Keywords: technology regulation, disruptive technology, participatory democracy, e-democracy

Language: English
Number of pages: 265
Gothenburg Studies in Informatics, Report 36, October 2006
ISBN 91-628-6937-X, ISSN 1400-741x (print), ISSN 1651-8225 (online)

About the cover

As I slowly began to realise that the writing process was coming to an end and the result would be printed a whole new problem arose. What should, would or could the cover of this book look like? After attempting to design a few covers of my own I came to the realisation that I needed help.

By posting my request for a cover on my blog and emailing others to place this information on their websites the call for a book cover design appeared online in at least five languages (Chinese, English, Finnish, Spanish and Swedish). The information was online at (amongst other places) Boing Boing, Lessig's Blog, Foreword, Patrik's Sprawl, Perfekta Tomrummet, Free the Mind and Cyberlaw. The results of this call generated 21 covers from 16 designers.

The covers were put on my blog so that visitors could be allowed to comment and pick their favourite. This created a wide discussion on the merits of different book cover designs. The cover on this book was chosen by a clear majority of visitors to my blog. It has been designed by Max Vähling (aka Jähling), a German comics artist and author. He is an editor of the comic web zine "PANEL online" as well as a small press self-publisher and contributor to various fanzines. His activities, both in comics and, occasionally, as a sociological author, are usually documented online at http://www.dreadful-gate.de. Thanks, Max.

Table of Contents

ABSTRACT II
ABOUT THE COVER III
TABLE OF CONTENTS IV
ACKNOWLEDGEMENTS VI

1. INTRODUCTION 1

DISRUPTIVE TECHNOLOGY 7
INFORMATION TECHNOLOGY AND DEMOCRACY 11
THESIS STRUCTURE 20

2. THEORY 22

REGULATION 26
REGULATING TECHNOLOGY 30
THEORETICAL FOCUS 38

3. METHOD 45

RESEARCH PROCESS 45
RESEARCH ACTIVITY 53
EMPIRICAL DATA 55
DATA ANALYSIS 59
METHOD SUMMARY 61

4. PARTICIPATION 64

INTRODUCTION 64
THEORY 66
ANALYSIS: ACTORS 71
ANALYSIS: STRUCTURES 77
DISCUSSION 81
CONCLUSION 87

5. COMMUNICATION 89

INTRODUCTION 89
THEORY 91
ANALYSIS: ACTORS 97
ANALYSIS: STRUCTURES 102
DISCUSSION 110
CONCLUSION 113

6. **INTEGRITY** ... **115**

INTRODUCTION ... 115
THEORY ... 117
ANALYSIS: ACTORS ... 125
ANALYSIS: STRUCTURES ... 127
DISCUSSION ... 133
CONCLUSION ... 135

7. **PROPERTY** ... **138**

INTRODUCTION ... 138
THEORY ... 140
ANALYSIS: ACTORS ... 145
ANALYSIS: STRUCTURES ... 152
DISCUSSION ... 156
CONCLUSION ... 159

8. **ACCESS** ... **161**

INTRODUCTION ... 161
THEORY ... 163
ANALYSIS: ACTORS ... 169
ANALYSIS: STRUCTURES ... 175
DISCUSSION ... 179
CONCLUSION ... 182

9. **AUTONOMY** ... **184**

INTRODUCTION ... 184
THEORY ... 185
ANALYSIS: ACTORS ... 189
ANALYSIS: STRUCTURES ... 193
DISCUSSION ... 200
CONCLUSION ... 202

10. **DISCUSSION** ... **204**

THE CASES ... 209
UNDERSTANDING DISRUPTIVE TECHNOLOGY ... 220
DISRUPTIVE TECHNOLOGY REGULATION ... 222

11. **CONCLUSION** ... **233**

12. **BIBLIOGRAPHY** ... **237**

Acknowledgements

I'D LIKE TO INTRODUCE YOU TO BETH, AN ANTHROPOLOGY P.H.D. STUDENT.
HI, HOW IS YOUR RESEARCH GOING?
WHAT'S THE MATTER WITH YOU?
SMACK!
WHY I NEVER...
DON'T YOU KNOW IT'S BAD MANNERS TO ASK A P.H.D. STUDENT THAT?
I-I'M SORRY. UH, SO... HOW LONG BEFORE YOU FINISH YOUR THESIS?
GEEZ, WHY DON'T YOU ASK HER FOR HER WEIGHT OR HER AGE WHILE YOU'RE AT IT?
SMACK!
THANKS TO MIGUEL...

"Piled Higher and Deeper" by Jorge Cham - www.phdcomics.com

So, when are you finished?

This is among the most stressful questions anyone can ask a PhD student. It misses the point by focusing on the destination rather than the journey. Despite this, every long journey must reach a point when the tourist becomes a traveler. Where one lets go of the familiar and boldly goes where one has not gone before.

It is at this stage (hopefully) that the thesis as text is written, delivered and evaluated. Like travel, the PhD period is marked with clarity and confusion, plans and reality, missed connections and strange dishes. The purpose of study is intellectual growth, the by-products include developing eccentric habits, learning to appreciate theory discussions and jokes about Foucault.

As with travel, it is the serendipitous encounters that make it memorable, so at this point I would like to thank my fellow travelers for all their help, shared experiences, horror-stories and tips. I also want to thank the border guards, customs officers and surly waiters for ensuring that I did not have an easy ride. Thank you all for making my journey as memorable and important as it could be.

Some people are more responsible than others for making sure that this journey did not end up in the middle of nowhere. Mentioning them here is a small recognition of the debt I owe them.

My supervisor, Rikard Lindgren, has patiently read, discussed and questioned so much text and ensured that, at least most of it, has been re-written and improved. Without him this project would have remained stranded, unfocused, and ultimately, incomplete. Here is a debt that cannot be repaid.

For encouragement, diversion and discussions on everything from the price of socks to the meaning of life, technology, politics, programming, rights, regulation, law and this text I would like to thank Bela Chatterjee, Marie Eneman, Örjan Hägglund, Karl Jonsson, Andrew Murray, Lennart Petersson, Henrik Sandklef, Joseph Savirimuthu, Rebecca Wong and Jonas Öberg.

Thanks to Antonio Cordella for our discussions on the academia game, to Douglas Hibbs for initiating me into university politics, to Christina Ramberg for enthusiastically demanding that I think independently and express myself academically, and to Harry Reichert for getting me passed security.

On a personal note: Thank you Marie, for our past, present and future. And to Ludwig for making sure I remember that the important stuff in life requires no footnotes.

Oh, and the answer to the question? *Never. This is just the beginning.*

Asperö 2006

Now that I understand this right
Let me take it to the mike
This revolution has just begun
- Tricky

1

Introduction

The blade itself incites to violence.
Homer

When bombs damaged the House of Commons Chamber in 1941 it was rebuilt exactly as it was. This was despite the fact that even then there were many flaws in the design of the Chamber, which is unsurprising since it had been the home of English Parliament since the 16th century. Churchill was well aware of the importance of the decision not to take the opportunity to renew the design. Maintaining the oblong shape of the Chamber, as opposed to the more modern semicircle was a political as well as an architectural choice.

> Here is a very potent factor in our political life. The semicircular assembly, which appeals to political theorists, enables every individual or every group to move round the centre, adopting various shades of pink according as the weather changes…The party system is much favoured by the oblong form of chamber. It is easy for an individual to move through those insensible gradations from Left to Right, but the act of crossing the Floor is one which requires serious attention. (Churchill 1952, p 150).

This quote shows that Churchill recognized the connection between physical space and human behaviour and, in extension, the potential regulatory effects obtained by controlling or regulating the physical environment. To Churchill, the reconstruction of the Chamber was not one of architecture alone. The reconstruction of the Chamber affected the applied politics of the United Kingdom and its empire. If technology is to be understood as the teleological activity of transformation or manipulation of natural resources and environments in order to satisfy human needs or goals (Kroes 1998) then this 500 year old Chamber is an example of technology which, in addition, illustrates the main point of this thesis: The regulation of technology is the regulation of democracy.

The regulation of British politics through the seemingly innocuous control of the physical space of the Chamber shows the importance of the relationship between technology and democracy. In this case the regulation of the physical space of the Chamber enhances and supports the traditional party system. This example should be understood as an analogy for this work. This work studies the regulation of information and communications technology (ICT) with a focus on the democratic effects of the regulation.

While this work could apply to all forms of ICT in particular to the area of information systems design since in these cases the designer becomes the regulator of the system by formulating rules that guide, control and regulate user behaviour.

> A system which delivers a strong and consistent symbolic message…may have the effect of creating or reinforcing norms, strengthening belief in them, and making it harder for people to disengage their self-controls from these norms. By contrast, a system which removes all personal choice may tend to weaken self-controls, for a variety of reasons. If people are denied any autonomy, then they perceive that the moral responsibility lies entirely with the system, and they no longer retain any obligations themselves. (Smith 2000, p 170).

Despite this more general applicability the focus of this work is the exemplification, discussion and analysis of the democratic effects of the regulation of ICT in relation to Internet-based activity. The importance of ICT in a democracy has been succinctly stated by Feenberg (2002, p ix) "Computer design is now political design." Therefore, in extension, the regulation of technology is not only a technological matter but also a political one.

The locus of concern for this work is the technological base, the cluster of technological innovations, groups of infrastructure(s), applications and social organizations commonly referred to as the Internet. It is important to keep in mind that the Internet is not one innovation but a rapid series of steps, innovations and collaboration within the field of communications technology. In addition to this the Internet as a phenomena is constantly technically evolving.

The regulation of Internet-based activity has become an area of increased discussion and study with a particular focus on adequate forms of regulation, while avoiding cases of overregulation. Overregulation occurs when the regulation implemented tends to not only regulate undesirable behaviour but additionally criminalizes or frustrates many types of legitimate behaviour. The impact of this undesirable side effect of legal regulation on democratic participation is the focal point of this thesis. Such an analysis must take its starting point in a definition of overregulation (intended or unintended) and proceed to discuss the effects of overregulation (positive/negative).

Since the Internet is more than one technological system, artefact or innovation, that has come to be employed in a multitude of social settings, the lack of coordinated development is unsurprising (Castells 1996, 2001). The haphazard manner in which this information infrastructure (Hanseth 1996) has evolved plays a significant role, as we shall see later in this work, in the way it is used, controlled and developed. In addition to this, their open nature and unplanned development (Ciborra 1992, Dahlbom & Janlert 1996, Hanseth 1996), lead to a haphazard development of a so-called autonomous technology (Winner 1978). In other words the development of technology through open standards leads to a technology that lacks, or seems to lack, conscious control and definition. Therefore when we talk about the Internet we are indulging in simplification, or convenient fiction (Kling 2005), since we reduce the different complexities until we have a manageable subject matter.

The fundamental idea of the Internet Infrastructure is the creation of a non-discriminatory mode of transportation. This is defined as the end-to-end principle of the Internet Protocol (IP). It states that, whenever possible, communications protocol operations should be defined to occur at the end-points of a communications system (Saltzer *et al* 1984). The development of this idea led to the creation of the communications system which was not concerned with the content of what was being transported as long that which was transported followed the correct transportation procedure. This has as its effect that the social interaction that is conducted via the Internet is in some sense freer than many alternatives since it is not constrained by the technology. Or, to put it another way, the constraints and enabling factors of the technology are non-discriminatory to the designs of the user (Lessig 1999).

Since the Internet provides an open undiscriminating transportation of data it has the ability to be used as a platform for a seemingly endless array of content. With the addition of speed, the passing of content becomes more or less instantaneous and this brings with it the appearance of computer supported simultaneous interaction.

To understand how regulation is carried out within the mediated world of the Internet we need to understand its context and its purpose. This entails defining parts of the whole in the hope of understanding the whole. The development of understanding of the way in which we regulate disruptive technology helps us to understand the regulation of that which is new and which threatens that which is established. The results of such a study can then be applied to all domains where regulation of disruptive technology may occur.

This work is concerned with the democratic effects of the overregulation of Internet-based activity. The regulation of Internet-based activity and technology is rapidly becoming a case of overregulation (Benkler 2006, Lessig 1999, Reidenberg 1998). In other words the regulation which is implemented tends to not only regulate undesirable behaviour but regularly criminalizes or frustrates many types of legitimate behaviour. To better understand these processes it is necessary to look at the way in which technology can be seen as a disruptive force and the way in which technology and democracy are being linked together in rhetoric and practice.

Therefore the research question of this thesis is: **How do attempts to regulate disruptive technology affect Internet-based participatory democracy?**

The specific contribution of this thesis is the development of understanding of the way in which we regulate disruptive technology. This understanding helps us to better regulate that which is new and which threatens that which is established. The results of such a thesis can then be applied to all domains where regulation of technology may occur. Specifically this thesis contributes towards a richer understanding in the research areas of e-democracy, regulation and disruptive technology.

The misalignments of technology and social thought become disruptive when the adherence to a certain social solution or concept remains in place during a period of technological change. Or, to state this in simpler terms, when the physical realities change while social arrangements remain static. At present the debate over the power of information and communication technology is an adequate example of a disruptive technology. This thesis will examine the technological challenges to six core democratic values (*Participation*, *Communication*, *Integrity*, *Property*, *Access* and *Autonomy*) and show that the technological change has far outpaced the evolution of social concepts in these areas and as a result the technology can be viewed as being a disruptive force in society.

The six core democratic values that have been explored in this work are not intended to be an exclusive list of such values. Other authors may choose to include other core values for a democracy. However the core values presented in this work perform a normative function. Without these values a socio-technical system cannot claim to be an IT-based participatory democracy. The latter concept is complicated by the fact that these values may be present in varying degrees.

Therefore, for the purposes of this thesis, the literature in this field helps us arrive at an understanding of disruptive technology. This can be summarised as: technology can be viewed as being disruptive when the technological developments affect social behavioural norms[1]. These technological developments push users to adapt their lives and behaviour to create new social interactional codes of behaviour in keeping with the new technology in their lives.

Since this thesis studies the effects of technology regulation upon the participatory democracy the concept of disruptive technology, within the framework of this thesis, is understood as: A technology becomes disruptive when it begins to affect a core value in the society or organization where the technology is implemented. With this definition we can at once see that technologies have long been disrupting society. While it is hard to choose a greatest, or most disruptive, technology it is relatively easy to find examples upon which we can build a common understanding of the issue. The steam engine, and with it the social, economic and technological changes it brought about must be seen as a disruptive technology. While it is not the purpose of this thesis to enter into the discussion on the role of technology on the industrialization of the world it is enough to point to the steam engine and the following industrial boom that it brought about. In addition it is also important to recognize that the development of technology, as well as the attempts to regulate, bring unintended consequences (Beck 1992, Kallinikos 2005, Rolland 2002, Tenner 1997).

The study of social institutions and organization in history tends to largely downplay technology and the effect of technology (Mitcham 1994, White

[1] Social behavioural norms in this work should be understood as patterns of behaviour that are adopted and followed by members of groups. Individuals confirm to such norms partly due to pressure experienced (real or imagined) from other members of the group. Norms are not only descriptive in that they illustrate how people within groups behave but they are also normative in that they dictate how group members should behave (Strahilevitz 2000, 2002).

1962). The social history of man is often viewed as the history of thought where the development of technology seems to play a small part in this evolution of mind (Latour 1999, Mitcham 1994). However to ignore the role of technology would not present a fair picture of social interaction since social relations are dependent upon a changing technological infrastructure.

Changes in the technological infrastructure enable the users to carry out their activities in new ways at the same time these technologies also bring with them challenges to established social conventions and practices. Activities, which previously did not need to be regulated because they were technically impossible, become the subject of regulatory interest once they become technically possible. For example discussions on the regulatory prevention of human cloning did not take place in earnest before it became technically possible to clone living organisms (Beyleveld & Brownsword 2001). This does not necessarily mean that our social values in relation to cloning have changed but rather that due to technological developments it is deemed necessary to attempt to regulate possible behaviour. In this way technology can provide an opportunity for revising established social structures through its implementation and use (Orlikowski & Robey 1991, Orlikowski 1992).

Dahl (1989) lists criteria that mark the democratic process, such as voting equality, effective participation, enlightened understanding, control of the agenda, and inclusion of all adult members in collective decisions. For Dahl (1989), the violation of any of these criteria makes the whole process undemocratic and incompatible with the logic of political equality. For example, as he writes on the topic of participation:

> …to deny any citizen adequate opportunities for effective participation means that because their preferences are unknown or incorrectly perceived, they cannot be taken into account. But to not take their preferences toward the final outcome equally into account is to reject the principle of equal consideration of interests. (Dahl 1989, p 109).

Barnett (1997) takes a different approach when attempting to assess the potential contribution of new media to an effective democracy, chooses four components:

> …a more knowledgeable citizenry, whose understanding of issues and arguments is fostered by the availability of relevant, undistorted information; access to collective rational debate in which citizens can deliberate and develop their own arguments; participation in democratic institutions, whether through voting, membership of a party, trade union or pressure group, attendance at political events or through some other national or local political activity; and making use of the representative process by communicating with and holding accountable

> elected representatives (at local, national or international levels). (Barnett 1997, p 195).

In his discussion on political activities taking place in society, apart from active deliberative democracy, Waltzer (1999) offers a list of twelve key activities such as political education, debate, voting, campaigning, corruption and bargaining. The purpose of Waltzer's list is to show that the activities within a democracy are not only those formally defined but also, the process of democracy involves many forms of interaction, some less noble than others.

The core democratic values studied[2] within this thesis have been identified[3] from the data collected in the case studies and a synthesis of works of mainstream theory of political scientists focusing on the concept of democracy. They will be defined and studied in greater detail in their individual chapters and case.

The theories of structuration and regulation are to be considered to be the foundations and domain within which the continued work on this thesis will be carried out. After the theoretical overview the thesis turns to a more analytical approach of the problem domain. This analytical approach consists of six studies of particular problem areas where the conflict between regulatory method and human actor is exposed and illustrated. To be able to analyse these six cases further specific theories will be required to obtain a more clear understanding of the specific domain in which the discussion is being carried out. Therefore each case study, represented in individual chapters, will include specific theories to better acquaint the reader of the specific domain. This is followed by a connection to the more general discussion of theory on the regulation of technology.

Disruptive Technology

Life is organized around technology. Despite our desire to maintain control over our lives, the bulk of what we do with our lives has been coordinated and adapted by and to the technology that surrounds us (Cowan Schwartz 1983, Norman 1990, White 1962). Therefore it should come as no surprise that when existing technology evolves or old technology is made obsolete that the phase where new technology enters our lives could be seen as being

[2] See *Theoretical Focus* page 38 *et seq.*

[3] The method with which these particular core values were chosen is discussed further in Chapter three below.

disruptive. The disruption occurs when the technology, which is introduced effects the social arrangements around which we build our lives (Lyytinen & Rose 2003a, 2003b).

While, in many cases, a disruptive technology can be seen as a technology that replaces the incumbent technology one must not forget that this replacement also displaces the social organization around the displaced technology (White 1962, 1972). Printing presses replaced the scriptoria and also change the role of the scribe (Eisenstein 1979). Railways replaced canals and also changed the way in which the social organization around the canals functioned. Railroads did not only make an impact on the barge pilot but also on the bargeman, lock keeper, canal owners, canal-side innkeepers, barge builders, waterway engineers and the horse trade (most barges were horse drawn) (Hadfield 1959). This process is not only one of historical interest. Examples of disruptive technologies are all around us. It is, in fact, a continual process. Digital cameras are replacing photographic film, flash drives replace floppy disks, DVD players replace VHS players. Each change brings social and economic effects to a larger or smaller degree. This disruption brings with it new possibilities of communication and control as well as disruption (Beniger 1986, Yates 1989).

The result of this disruption of social behavioural norms leads people to adapt their lives and behaviour to create new social interactional codes of behaviour in keeping with the new technology in their lives (Cowan Schwartz 1983, White 1962, 1972). At the same time (or more often later) the disruption caused by the new technology causes the regulator to react. The latter is not necessarily the state legislator but can also be any entity with the power to act (there may also be several such entities acting concurrently).

Disruption is often seen as being a negative force. In a sense it is. Disruption affects the status quo and therefore those who profit from the status quo see the force as a negative. Even those who do not profit from the status quo may view disruption as a negative force since change is a movement from the known to the new, or unknown. This thesis views disruption as an inevitable agent of change and sees change as playing an important role in society.

In recent work the concept of disruption is being used to explain organizational change and innovation. Undoubtedly the most popular use of the term disruptive technology has been presented by Christensen (1997) in his book *The Innovator's Dilemma*. Christensen defines a disruptive technology as a new technological innovation (product or service) that will eventually overturn the dominant technology in the market sector. While this description has been effective in bringing the concept of disruptive technologies into the more general debate of the role of technology it has also changed our concept of technology, since it limits our general view of disruptive technologies to being one of a less economically viable technology. The role of Christensen (1997) is therefore a double-edged sword since he brings the concept or term of technology as a disruptive force into our consciousness but he also manages to limit the discussion to a very specific concept. Christensen does this knowingly and openly and this is reflected in the sub-title, which refers to the failure of great firms. By taking this position Christensen affirms his position as being situated within the study of theories of industrial innovation (Christensen & Bower 1996, Foster 1986, Teece 1986, Utterback 1996, von Hippel 2005).

Within the information systems (IS) field there has been a growing interest in the concept of disruptive technology which can in part be explained by the rapid changes in technology which have occurred in the IS discipline. Among those working to develop a theoretical framework of understanding for the concept of disruptive technology are Lyytinen and Rose (2003a, 2003b). One of their observations is that the traditional form of innovation has been developer driven (push) as opposed to market demand (pull). On the effect of this they write:

> While theories that lean solely on push-side explanations are simplified versions of technological determinism, IS research to date has been flawed in terms of being dominantly engaged with the pull-side analysis. This has lead IS researchers to largely neglect the importance of push-side forces in continued IS innovation and in understanding waves of IS innovation. (Lyytinen & Rose 2003a, p 308).

The goal of Lyytinen and Rose is to build a theoretical framework to help understand the idea of disruptive IT innovation. Their view of the disruptive effect is like an "earthquake" (Lyytinen & Rose 2003a), which strikes with little warning and cannot be ignored. The long-term effects are radical and force those affected to alter their lives. To Lyytinen and Rose (2003a) the effects of disruptive technology are both radical and pervasive. In this way they are comparable to the paradigm shifts as described by Kuhn (1962).

Disruptive technology is a difficult concept. It is something that occurs and re-occurs. The technological infrastructural base in society does not remain the same and one of the important aspects of this change is that society must be aware that it takes place. This awareness is not always pleasant. Kontio (2004) posits in his work that through an adaptation of the theories of Lyytinen and Rose a model can be built to understand the internal organizational effects of a technology. Once this is done the company has a choice of whether to adopt the technology or not depending upon the effects. To a degree Kontio may be right but it is important to understand that due to the complexity involved, any understanding the future effects of a technology is illusory. The idea that a disruptive technology can be chosen or rejected is to fail to understand the nature of disruptive technology. Lyytinen & Rose (2003b) offer this definition:

> We define a disruptive IT innovation as a necessary but not sufficient architectural innovation originating in the IT base that radically and pervasively impacts systems development processes and services. To avoid technological determinism we use the terms necessary and not sufficient in the definition to clarify the conditions under which specific changes in the technology base can become disruptive. (Lyytinen & Rose 2003b, p 563).

Certain elements of a technological change can be more or less disruptive. The level of disruption may effect to a greater or lesser degree different areas in society (organizations, academic disciplines etc). However within the IS discipline disruption is described as an occurrence which can be said to occur "...when a constellation of linear growths in computing capability…eventually overwhelm current computing metaphors." (Lyytinen & Rose 2003a, p 310). That which is overwhelmed is the metaphor[4] with which we understand the discipline; it is in other words the overwhelming of our understanding of our surroundings and basis of knowledge.

Therefore the idea of disruptive technology that can be drawn from these sources adequately matches the use of the terminology in this work. The metaphor of the earthquake is dramatic, and yet poignant in the sense that everything changes for those who are involved. The innovative effects of Internet technology since the mid 1990s have created a technology of disruption and its effects are being felt in the whole digitalized world.

As previously stated, the purpose of this work is to study how the attempts to regulate disruptive technology affect Internet-based participatory democracy. This work will expand upon the concept of disruptive technology by exemplifying the manner in which such technology drive subtle but important social change in the manner of the earthquake metaphor. This is to say that the effects of technical change and its

[4] Lakoff and Johnsson (1980) have eloquently shown the importance of metaphors as going beyond mere language tropes and being the basis of our knowledge and understanding of the world.

regulation tend to disrupt the, previously established, social norms that make large parts of our democratic social interaction.

This work studies the social interaction which takes place via Internet technologies. These technologies are, as we shall see, viewed positively as being potentially valuable for the participatory democracy. The basic, or simplified, discourse concerning the technology in relation to democracy claims that the potential for increased interaction provides a greater level of democratic participation. However, as this thesis will show, occasions of overregulation occur when attempts to regulate the abuses are made.

Besides the practical applications of disruptive technology as a critical lens upon social change and its regulation this work will contribute both to the understanding of the term, its implementation and its development in the field of IS theory. These goals are achieved by the case studies and their analysis collected in this work.

Information Technology and Democracy

All forms of government depend ultimately upon their legitimacy among the population they are set to rule (Dahl 1989, Harrison 1993, Pateman 1970, Sartori 1987). Democracy depends upon a high level of acceptance among the population since democracy is the rule of the people. In real terms today this means that democracy is a form of government where policies are directly or indirectly decided upon by the will of the majority of the population. Besides being a form of government the concept is in itself an ideology and the choice of democracy or the comparison between states on the level of democracy and democratization is political (Dahl 1989, Harrison 1993). The origins of the democracy lie in the form of government practiced by the Athenians in the fifth century BCE where the process of direct democracy was called *demokratia* or rule of the people. This Athenian practice gave Athenians the right (and duty) to participate[5] in the processes of the state (this included, but was not limited to legislation, judicial activity and foreign policy). This participation was direct and therefore not through representatives. The understanding of democracy we have today is based upon interpretation of Athenian democracy and the subsequent developments (theoretical and practical) that have taken place largely in the 18th century (Dahl 1989, Harrison 1993, Sartori 1987).

[5] Since participation was limited to free (non-slave), adult males, whose both parents were Athenian born, political participation remained in the hands of a minority (Harrison 1993).

According to Mill (1965 [1848]) in an efficient democracy it is not enough for the government to be structured democratically but even large parts of the social system must be similarly organized for democracy to be effective.

> A democratic constitution, not supported by democratic institutions in detail, but confined to the central government, not only is not political freedom, but often creates a spirit precisely the reverse. (Mill 1965 [1848], p 944).

One method of achieving this goal is to attempt to a large degree create a participatory democracy. The goal of participatory democracy is to go beyond universal suffrage, the right to select leaders and influence the state. Its goal is to achieve a self-managing society. The goal of participatory democratic theory includes maximum input (participation) from the public. The result of this participation is not limited to policies (decisions) but also the development of the social and political capacities of the individuals involved in the process (Pateman 1970).

Participatory democratic theory takes its starting point from two important assumptions. Firstly that people are capable of understanding, expressing and finding solutions for their problems. Secondly, effective solutions require the participation of the people who will be affected by them, without necessarily being dependent on authorities and experts (Oppenheimer 1971). Participation can be given many meanings. In the context of participatory democratic theory, participation refers to the normative process of shared decision-making and governance between government (decision-makers) and citizens (Dahl *et al* 2003). Cook and Morgan (1971) observe that participatory democracy implies two broad features in patterns of decision-making: (i) decentralization or dispersion of authoritative decision-making whereby authority to make certain decisions is displaced such that authority is brought closer to those affected by it, and (ii) direct involvement of amateurs in the making of decisions. They clarify that amateurs in this setting are individuals who do not carry credentials as formally trained experts; they are laymen and not professional participants (Cook & Morgan 1971).

It is important to recognize that in-group decision-making a social "ranking" is formed within the groups where non-experts tend to defer to experts even in questions concerning topics where the experts are not expert. (Beck 1992, O'Neil Lane 2005). This form of referral to experts is also visible in a participatory democracy where experts (often assumed to be society's scientific and technical elites) play an increasingly influential role in the decision-making process (Fiorino 1990). Expert perceptions of technical problems (such as the potential for risk associated with a human subjects research protocol) are judged to be more rational than the "subjective" perceptions of the less technically sophisticated public (Fiorino 1990).

An underlying assumption of participatory democratic theory is that citizens are not isolated beings, and that social organizations play an important "educative" role in teaching them how to interact and work together and how to act socially as well as politically. Citizens are socialized to learn democratic norms by participation in social groups, workplaces, and other forums (Coke Ellington 2004, Pateman 1970). Therefore the right to participate in the democracy brings with it several advantages. Rosenbaum (1978) goes so far as to argue that public participation is necessary for democratic functionality through its role in ensuring political equality and popular sovereignty. Others argue that the importance of participation lies in the knowledge that such participation is a requirement to uncover the public will (Dienel 1989, Gauthier 1986). Participation is also an important factor in ensuring that the citizens have a possibility to protect their interests and influence the outcome of decisions and policy (Rosenbaum 1978, Van Valey & Petersen 1987) In addition to this, participation plays an important role in the enhancement and development of personal and social life (Daneke *et al* 1983, Rosenbaum 1978).

One of the major stumbling blocks for developing a larger participation in the democratic process has been one of logistics (Dahl 1989, Pateman 1970). The communications required for large-scale participation have not been in place and therefore the present day processes of democracy can be seen as a compromise between theory and technological limitations. The technological limitations have been the difficulties in building a public sphere were two-way communication can take place (Castells 1996, Dahl 1989, Pateman 1970). Habermas' (1989) concept of the public sphere was to allow the participants (citizens) to discover the general will or common interest. The society that supports such a public sphere will require of its citizens to participate in it. The purpose of this participation is both to enable the uncovering of the general will and the civic education of the citizens (Barber 1984). This approach to government, therefore, does not solely concern itself with resource allocation but is also concerned with the uncovering, communicating and addressing the interests of the public (Barber 1984). In order to activate the citizen to participate to such a degree the institutions must be designed to facilitate individual autonomy and participation in the common cause (Barber 1984, Habermas 1989).

The role of user participation has a long-standing tradition within Scandinavian information systems development (Bjerknes *et al* 1987) at an early stage technology was understood to be important in the role of empowering the worker. Workplace development projects such as the UTOPIA project (Ehn 1989) were early examples of the belief of the potential empowerment inherent in technology. While the goal of the UTOPIA project was the democratic organization of work (Bjerknes & Bratteteig 1995), the dissemination of technology within society was to change the way in which our democratic participation was undertaken. The basic concept can be simplified with the idea: Once the infrastructure of empowerment is in place the users will use it (Norris & Curtice 2004).

It is important to be clear that the Internet is not an inherently democratic technology. Technology itself is neutral and therefore can be used both for democratic and non-democratic purposes. The desire to equate communications technology with democracy is not unique to the Internet (Winner 2005). Many communications technologies have been celebrated as being democratic but it is important to remember that communication alone is not enough of a base for a democracy. Winner (1986) writes:

> But democracy is not founded solely (or even primarily) upon conditions that effect the availability of information. What distinguishes it from other political forms is a recognition that the people as a whole are capable of self government and they have a rightful claim to rule. As a consequence, political society ought to build institutions that allow or even encourage a great latitude of democratic participation. How far a society must go in making political authority and public roles available to ordinary people is a matter of dispute among political theorists. But no serious student of the question would give much credence to the idea that creating a universal gridwork to spread electronic information is, by itself, a democratizing step. (Winner 1986, p. 110).

From the mid 1990s the diffusion of Internet technology has presented the technological infrastructure necessary to conduct experiments with cost-efficient large-scale participatory democratic projects. The study of such systems has grown in parallel with the technology. Grönlund (1994) presents his study of public computer systems were he blends traditional arguments from Rousseau and Mill and contemporary sources such as Pateman and argues for traditional participatory democracy supported by computer and network technology. His arguments concern public computer systems, which he defines as systems designed to act as an interface between organizations and their clients. Grönlund (1994) recognizes that such systems are more than simply technological innovations but must also be seen as being valuable components in the communicative process between the organization and the client. Grönlund's systems impact upon what he defines as the societal dialogue. He notices that this is particularly true of public agencies.

Grönlund was early in Swedish academia in pointing out that public computer systems would play an important role in public dialogue and that this use would also change the way in which this dialogue would be conducted. This change would not only be based upon technical change but would also involve social and organizational changes. These changes in communication will also place demands on the designers of the computer systems that mediate the communication to ensure that democratic participation is supported (Grönlund 1994).

For the Internet the year 1994 may be considered to be early. This is not so much in relation to the technological maturity but rather in relation to the technological dissemination in society. Up until this point the results of studies of the democratic effects of Internet technology could only be representative of a limited number of users and these users should be considered to be early adopters of technology. Such constraints limit the universality of the results of the democratic effects being studied. The technological roots of Internet stretch back to the ARPANET project launched in the 1960s. It gained popular appeal in 1991 with the development of the World Wide Web (WWW) application and the opening of the Internet for commercial purpose in 1994/1995 (Castells 1996). Therefore discussions on the social impact of this technology prior to 1995 can be considered to be early studies.

These technical developments led many to predict positive or negative impacts on democracy. Up until the mid 1990s the work was mainly positive techno-optimism as the authors presented little grounds for their stance, the position towards the impacts of technology on democracy during the later half of the 1990s was that it would have little effect or that it may even cause harm to democracy (DiMaggio *et al* 2001). In a review of the literature of the time Bimber (1998) writes that there are two positions being taken (i) populistic predictions about the empowerment of technology, and (ii) proposals for improving the community building role of technology. Bimber (1998) argues that neither position had an objective basis for the views they put forward. In an effort to revisit this study Johnsson and Bimber (2004) are more optimistic towards the ability of technology to empower citizens and user groups. While they do not see Internet technology as revolutionizing politics they do maintain that it has the effect of reinforcing individual groups in fragmented, hyperpluralistic societies.

E-government and E-democracy

There is a fundamental difference between electronic government and electronic democracy even if the terms have a substantial overlap. Electronic government is the ability of the state to achieve savings by automating decision-making processes, preferring online information and allowing certain forms of citizen-state communication to take new forms. An example of a technology that has been harnessed to facilitate the latter is the mobile telephone text messaging (SMS). In Sweden citizens who file simple tax returns can do so via SMS while in the UK experiments have been conducted in voting for local government elections via SMS (Norris 2004). Ciborra (2005) maintained that electronic government in practice entailed applying ICT to the transactions between state and citizen and re-defining the boundaries between state and market. Electronic democracy is not about streamlining or economizing the state by alternative forms of communication. It is about empowering the user in her ability to directly participate in the general democratic process (Kahn & Kellner 2004).

Democracy supported by information technology has many names, the most common are "e-democracy", "digital democracy", "cyber democracy" and the curious term "virtual democracy". These terms presuppose a positive connection between technology and democracy. Information technology is expected to have a positive effect on democracy by providing a greater degree of citizen insight and participation. This will be achieved by an expansion of the public sphere through the use of technology. This vision is also reflected in political manifestos, policy documents scientific texts and the public debate (Beckman 1995, Ilshammar 2002). Techno-optimism is not a new feature. Ilshammar (2002) has shown that the gap between technology and rhetoric is not particular to Internet technology.

In attempting to clarify the terminological confusion which sometimes seems to exist in this field the article by Chadwick and May (2003) have analysed the forms of interaction between state and citizen in the United States, Great Britain and the European Union and arrived at three models of interaction (managerial, consultative and participatory). According to Chadwick and May (2003) an e-government regime can be identified by a high level of "managerialism" which is the focus on the effectivisation and rationalization of government services (both within government and communication between citizens – government) through the implementation of ICT. This view focuses on the development and application of ICT services and the development of technology in society. The e-government approach also entails "… a general absence of user resource issues, such as ability to receive and interpret information." (p 272) Therefore the e-government, or "Managerial Model", is the use of ICT to improve on previously existing technologies either by reducing transaction costs or increasing communications speed (Chadwick & May 2003). This e-government model is a potentially dramatic shift in state – citizen interaction, however Chadwick and May (2003, p 273) point out:

> Though we argue that change is not likely to enhance democracy, even if taken on its own rather limited terms, it is still clear that the public sector is being altered by e-government innovations.

The "Consultative Model" is, in contrast to the previous model, a pull technology where ICT is used to facilitate the communication of citizen opinions to the government. In this model the citizen's opinions are seen as being the basis of a more informed public policy. The infrastructure provided by ICT creates the possibility of citizen involvement in government policy beyond the established voting system where representatives are chosen.

Chadwick and May's (2003) third model is the participatory model. This model goes beyond the "vertical flows of state-citizen communication" (p 280) and provides based upon "…complex, horizontal, and multidirectional interactivity" (p 280). This model accepts that, while states are heavily involved in facilitating political discussion and interaction they are not alone in this role. There are many other organizations with a role in political interaction within a civil society.

For the purpose of this work the term e-democracy will refer to the process of democratic communication between stakeholders (e.g. citizens, government bodies, NGOs, corporations) for the purpose of participating in society. The term e-government will refer to the use of technology by government to make governmental communication (whether inter-departmental or government-citizen) more efficient. This division between e-government and e-democracy is reflected in government policies (as discussed below) and European Union information technology initiatives.

The eEurope 2002 Action Plan (eEurope 2000) was geared at creating a larger degree of participation; its express goal was the "…participation for all in the knowledge based society" (p 18). A key objective in this goal was that the European Union should become the most competitive and dynamic knowledge-based economy with improved employment and social cohesion by 2010. The plan focuses on areas such as cheaper Internet access, e-commerce, e-services, online government and intelligent transportation.

Though very little is said of actual IT-based participatory democracy (Anttiroiko 2001).

> To put it bluntly, the EU refers to "access" as critical mass, "participation" to consumption processes, "dialogue" to opportunity to make inquiries via Internet, and "transparency" to official documents available in e-format on the Internet. This suggests how eEurope and the entire Union deal with democracy. The techno-economic message is usually surprisingly explicit, though sometimes it is bundled with expressions suggestive of genuine democracy and participation. (Anttiroiko 2001, p 34).

These goals have been reiterated in the eEurope 2005 action plan (eEurope 2002) "An information society for all" which stated among other things that access to public information implies addressing the specific requirements of "people with special needs, such as persons with disabilities or the elderly" (p 11). These European Union goals are also reflected in the Swedish national goals presented in the Proposition 1999/2000:86 entitled "Ett informationssamhälle för alla" (An information society for all) (Proposition 1999). While there is a focus on user competence the main thrust of these governmental documents focus on the development of a robust information infrastructure. The goal of achieving participatory democracy is translated into the development of technological infrastructure.

The new millennium brought with it a certain amount of disenchantment since the differences between the promises and the realities of information technology supported democracy were becoming clearer (DiMaggio *et al* 2001). A governmental investigation could state that information technology democracy projects thus far had been focused upon increasing information supply. Projects aimed at supporting active participation and influence in democratic processes are few and far between and have thus far have had limited content. Many of the democratic projects also lacked a long-term concerted effort aimed at increasing democracy (Demokratiutredningen 2000). The report goes on to state that while there is a great deal of interest in technology and democracy in Sweden, the projects, which have been conducted, have neither problematised between conflicting democracy ideals nor analyzed the results (Demokratiutredningen 2000). The report continues by warning that all too routine uses of information technology will not provide for an increased participation in the democratic process. The report recommends the development of information technology so that it is developed into a tool for democracy and not remain a routine tool of governmental organization (Demokratiutredningen 2000).

The stated goal is to achieve a participatory democracy. This goal regularly loses something in implementation, where it becomes the creation of electronic government, or the transfer of organizational forms and technology into the process of public administration. The general view seems to be one where this transfer will not require policy changes or a more fundamental approach to participation in society. Most experiments in digital participation have arrived at the realization that it is a complex affair requiring many competencies and financial support (Ranerup 1999, 2001).

Since this work is more interested in what it defines as the participatory democracy as opposed to the processes of electronic government it is important to understand the role of technology in the participatory democracy. While some scholars argue that the presence of Internet technology is enough to motivate the user to become politically active (Norris 2001, 2004) others argue that the technology alone will not create the politically active user (Bimber 2001). This thesis argues neither view. The argument in this thesis concerns the way in which the use of technology is affected by the regulation of technology and therefore the argument of whether technology creates participation or not falls outside the scope of this work at the same time it is important to recognize that this is a closely related topic to thesis. Additionally many e-democracy theorists focus relationship the individual and the state or conceptions of deliberative democracy (Noveck 2005) in doing so they forget about the needs of the users or groups of users who are actively using the technology to participate with each other in IT-based participatory democracy.

Therefore if studying the amount of technology available to the users tells us very little about the state of IT-based participatory democracy, then what shall one study? Watson and Mundy (2001) suggest that the implementation of e-democracy requires a careful plan. This stance is re-iterated by Grönlund *et al* (2003) who argue that the way ahead in developing a viable democracy where active participation is supported by technology depends upon development in two main strategies. The first strategy concerns the need for an overall governmental approach to IT democracy. This involves a change where separate governmental offices taking decisions based upon economic incentives cannot define the development of IT democracy. The second strategy involves a concerted effort in the development of technology to enable participation in democratic processes and decisions. It must be stressed (Grönlund *et al* 2003) that simply choosing one of these two strategies is insufficient in that it will not move the situation forward towards the desired goal.

While not wanting to enter into a nominalist debate there is a need to additionally clarify the position of this thesis towards that which is being studied. The object being studied is the IT-based participatory democracy this should be understood as the use of ICT for democratic processes such as for deliberative and participatory aims. Implementations of e-democracy projects include virtual town hall meetings or citizen consultations and the use of discussion boards on party websites and in municipalities (Chadwick & May 2003). Rather than study the democratic effects of a particular organized technology in this manner this thesis chooses to arrange the work around six core democratic values, namely: *Participation*, *Communication*, *Integrity*, *Property*, *Access* and *Autonomy*.

Central to the understanding of the nature of the IT-based participatory democracy is its interconnectedness. This entails that when something occurs in one part of the IT-based participatory democracy it can potentially become an experience shared by all. The novelty with this level of interconnectedness is that conventional methods of control by isolating the problem are no longer available (Kallinikos 2005). This is not to say that all events will affect all users equally but rather that the potential of containing problems to certain geographic areas, ICT artefacts, user groups, ethnic groups etc is shrinking. Another view of the issue of interconnectedness (Kallinikos 2005) is the largely conceptual inability to separate technical and ideological choices carried out in situations that typically have been understood to be design choices. Therefore technical design choices should not be seen as being solely technical in nature since they have real repercussions on the implementation and experience of the IT-based participatory democracy.

The focus in this work is on the use of Internet as an integral part of the creation of an IT-based participatory democracy. As examples in this work will show, the use of the Internet in supporting this goal challenges established conventions and therefore the technology becomes a disruptive force. One reaction demonstrated in this thesis is the impulse to control this disruption by attempting to regulate it. However, as this work will show, this regulation often results in the suppressing of applications of technology that would have been beneficial and fundamental to the participatory democracy.

Thesis Structure

This section brings the introduction of this work to a close. With the next section, the theory, the main work of this thesis begins by explaining both the theoretical foundations and starting point of this work. This section is followed by an overview of the fundamental methodology applied during the course of this thesis. The purpose of this has been to bring forward the case studies, which are both the empirical foundations of this work and the practical examinations of theory in practice.

The case studies, which are the main empirical foundation of the entire research project presented here, have been carried out between 1999-2005. The main bulk of the results have been published in academic journals during 2003-2005. These articles have been substantially reworked to become the chapters of this book.

Core Democratic Value	Published
Participation (Expanded in Case 1)	Klang, M. (2004) "Civil Disobedience Online", Journal of Information, Communication & Ethics in Society, Volume 2: Issue 2: Paper 2, Troubador Publishing.
Communication (Expanded in Case 2)	Klang, M. (2003) "A Critical Look at the Regulation of Computer Viruses" International Journal of Law and Information Technology, Vol 11 No 2, Oxford University Press.
Integrity (Expanded in Case 3)	Klang, M. (2004) "Spyware – the ethics of covert software", Ethics and Information Technology, Issue 3, September 2004 pp. 193-202, Kluwer.
Property (Expanded in Case 4)	Klang, M. (2004) "Avatar: From Deity to Corporate Property", Information, Communication & Society, Volume 7, Number 3 pp 389- 402, Routledge.
Access (Expanded in Case 5)	Klang, M. (2005) Free Software & Open Source: The Freedom Debate and its Consequences, First Monday, volume 10, number 3 (March 2005)
Autonomy (Expanded in Case 6)	Klang, M. (2006) "Virtual Censorship: Controlling the Public Sphere", IFIP-TC9 HCC7 Social Informatics: An Information Society for All?, Nova Gorica (Slovenia), Gorizia (Italy), September 21-23.

Table 1: Previously Published Studies

To be able to draw wider conclusions from the individual cases, which are represented in the empirical work, the main theoretical foundations will be applied and discussed in relation to the specific results of each of the cases. This analysis will provide the material from which conclusions can be drawn about the effects of the regulation of disruptive technology and its unintended democratic side effects. This analytic section will provide the material from which the implications of the regulation of disruptive technology can be drawn. This work will then be summarized with a focus on the salient details in the final section of this thesis, which will present the reader with the conclusions of this project.

2

Theory

Pray for the welfare of the government, since if not for the fear of it, a person would swallow his fellow man alive.

Rabbi Chanina

This section will provide an overview of theories of structuration, regulation and technology regulation. The choice of structuration theory is intended to provide a context within which regulatory activity takes place. It is also meant to provide the reader with the image that the researcher views the actions and reactions between the regulator and the regulated as a constant discussion and movement between the structure (represented by the regulator) and the actor (represented by the regulated). However it is important that this is understood as an image, a metaphor, a simplification. The actor is not passively regulated and nor is the structure behaving autonomously. The actors form and define the structure in the same way as the regulated create the regulator. Without the regulated there could be no regulator. Structuration theory is used in this work as an analytical tool. This work does not intend to primarily contribute to the development of structuration theory. The primary contribution of this work is towards the e-democracy field and to the discussions and development of technology regulation and the implications of disruptive technology.

The view, stated above, that there could be no regulator without the regulated reveals the researchers position on regulation. The simple command and control structure posited by the early regulatory theorists is too much of a simplification to be able to provide academic research with a meaningful basis from which to develop our understanding. The position of this work is that regulation is every force or external controls exerted upon those to be regulated (Fuller 1964). Therefore regulation can be state or non-state, intended or unintended, legal or economic and so on.

The purpose of this thesis is to look at and understand the democratic effects of the regulation of Internet-based activity. The regulation of Internet-based activity and technology is rapidly becoming a case of overregulation (Benkler 2006, Lessig 1999, Reidenberg 1998). In other words the regulation which is implemented tends to not only regulate undesirable behaviour but regularly criminalises or frustrates many types of behaviour which, from a democratic point of view, are legitimate. To be able to meaningfully discuss this issue we must first come to understand what regulation is and how it is carried out. To arrive at an understanding of these issues we must therefore carry out a theoretical exploration of the role of regulation within society. Therefore, this section begins by showing the role of structuration theory in forming the way in which individuals interact with the structures that surround them prior to looking at theories on regulation, from the classical to present day regulatory theory. This brief look at the theory of regulation will be concluded with the theories employed in the regulation of the Internet.

The main ideas in the theory of structuration have been developed by Anthony Giddens (most pointedly in 1984). The theory in itself is not a specific information systems (IS) theory but rather a general theory of social organization. The theory has been widely and successfully adapted and used within the IS field (DeSanctis & Poole 1994, Orlikowski 2000). The theory of structuration is mainly an attempt to reconcile a theoretical dichotomy of social systems that views the individual either as being acted upon or as an autonomous agent. It is an attempt therefore to combine the objective understanding of society as an objectively definable structure and the objective viewpoint of the autonomous actor. This is done not by seeing these two views as conflicting but rather as two halves of a duality both effecting and being effected by each other. Therefore adopting the theory of structuration involved taking a balanced position and attempting to treat structure and agency equally.

Structuration is a theory of social organization that explains change and stability in a social system over time. Since the theory originally presented by Giddens does not deal with power relationships it does not show in detail how technology regulates us – it has been necessary to apply the theory in manner beyond its original form.

Structuration theory has been further developed and adapted in research fields such as the IS research field. The approach of IS scholars has been to argue that structuration provide an analytical tool needed to explain regulation (Monteiro & Hanseth 1995) while focusing on and theorizing the IT artefact (Orlikowski & Iacono 2001). The advantage to structuration is that it moves beyond technological determinism and social constructivism. This adapted IS structuration theory argues that an individual's actions are neither determined by technology, nor are they capable of constructing technology. Technology constrains and enables individual action while also being a product of individual action. Technology is developed and also affects our activities. Structuration theory recognizes that individuals design technologies that enable action – these same technologies also constrain action.

The structure of which the theory speaks consists of the "Rule-resource sets, implicated in institutional articulation of social systems" (Giddens 1984, p 377). Giddens envisioned the structures as being virtual or "memory traces" rather than physical representations social agreements. In a development of Giddens' theories (Orlikowski 1992, Orlikowski & Robey 1991) adaptations to the theory have been made in order to encompass more than these memory traces by studying the role of technology in social interaction. In so doing the theory becomes "…well-suited for the understanding of information technology and its interaction with organizations (Orlikowski & Robey 1991, p 164).

In line with these adaptations to structuration theory the structure becomes many of the normative elements within a society. These normative elements can be clear rules or laws. They may be physical barriers such as walls, bollards or doors however they may also consist of more virtual norms such as social rules which we adhere to as a group. It is however important to note that these structures are fixed over periods of time and can be identified outside the individual actor. These normative elements are part of Giddens (1984) duality of structure in that they are both created by human action and regulate future action.

Within these structures we find reflexive social actors monitoring, evolving understandings of and adapting to structural conditions. Despite this evolution, actors tend to develop routines, which provide a sense of continuity and security and an ability to plan and carry our social activities. Giddens (1984) maintains that the actors have the power with which to shape their own actions however the complexity of social interaction makes it difficult to predict unintended consequences.

> The flow of action continually produces consequences which are unintended by actors, and these unintended consequences also may form unacknowledged conditions of actions in a feedback fashion. Human history is created by intentional activities but is not an intended project; it persistently eludes efforts to bring it under conscious direction. (Giddens 1984, p 27).

The duality pointed out by Giddens (1984) is that the structures are created by actors and the structures are what give similar social practices a systematic form. Once in place the structure constrains the actors, Giddens (1984) downplays the limiting power of structural constraints and points to both the fact that structures are actor-controlled and that the structures also may enable actors to carry out practices, which they otherwise would be unable to do. This therefore is what is known as the duality of structure and agency. There can be no agency without structures and yet there can be no structures without the agents which create them.

In this thesis the theory of structuration launched by Giddens (1984) and later developed and adapted (DeSanctis & Poole 1994, Orlikowski 1992, Orlikowski 2000, Orlikowski & Robey 1991) is used as an outer framework with which to study the role of power within social systems.

This adapted structuration theory understands that technology enables, forms and limits the actors' choices and actions. This should not be seen as a one-way relationship. It is the actors themselves who constitute the structures. The particular focus of the thesis will be the way in which the regulatory bodies use their power to regulate technology use. In addition to this the studies within this thesis will also look at how Internet technology is used to augment communicative interaction. The focus on regulation is important since it shows the way in which the formalized structures of law and regulation are adapted to the change in human behaviour vis-à-vis new technology. The enabling aspect of the new technology shows actor empowerment, which creates and invigorates interaction between human actors. The actions of the regulator contain a well-defined pattern of problem identification, analysis and attempts to control actors' behaviour through changes in legislation.

The reaction of the regulator towards the new forms of interaction among human actors which is provided by technology is particularly interesting since the behaviour clearly shows attempts by the legislative body to control what is, de facto, an increasingly difficult situation to control. The difficulties of control, however, do not deter the states from exercising the control mechanisms they maintain. Giddens (1984) felt that the study of power should not be carried out half-heartedly. He writes that the study of

"Power cannot be tacked on, as it were, after the more basic concepts of social science have been formulated. There is no more elemental concept than that of power." Giddens (1984, p 283) did not mean that the study of power was more important than other social considerations however it should not be given a secondary position within an analysis.

This thesis looks at the regulators use of power through the regulatory structures. The study of the creation and adaptation of regulation shows the interaction within structures and between structures and actors. The reactions towards regulation shows the human actors desire to adapt and negotiate the new social orders being created. This creation is the expression of power, it is the way in which the state attempts to achieve goals and, in the best scenario, guide society toward certain well-defined goals.

Despite its forceful role power is not "inherently divisive" however due to the way in which power is divided in society there will naturally be decisions and actions by the regulator that are inherently forceful in the way in which they define and sanction actions of groups within society. These can be seen as social power struggles were groups act in ways to either mitigate the negative effects of regulation or attempt to create a strong enough powerbase from where unwanted regulation (in other words undesirable structures) may be altered. A focus in this thesis will therefore be on the modalities of control between actors-actors and actors-structures in society.

Regulation

The concept of regulation may currently be narrowed down to three accepted theories or descriptions of the phenomenon (Baldwin *et al* 1998). These are presented in the current literature of the field as (i) regulation is the presentation of rules and their subsequent enforcement usually by the state, (ii) regulation is any form of state intervention in the economic activity of social actors, and (iii) regulation is any form of social control whether initiated by a central actor such as the state or not. This latter description includes all forms of acts whether they are intended to be regulatory or not.

Often discussions on regulation will bring together both formal procedural methods of regulation and include them together with strategies of regulation (cf. Braithwaite & Drahos 2000). This approach tends to be more pragmatic to its nature but has the difficulty in that the more complexity it involves in presenting a true representation of regulation in a given time and place the less likely any such representation can be considered to be useful as generalisable theory to be applied anywhere outside the specific arena.

The modern regulatory debate begins with the work of John Austin, in particular *The Province of Jurisprudence Determined* (1998 [1832]), which is an attempt to free the concept of law from the precepts of religion and morality. He does this by taking an analytical approach to the law (as opposed to, for example, historical or sociological). Austin's project was an attempt to define law in a morally neutral descriptive manner. This approach to law enabled Austin to present the foundations of what has become the command (and control) theory of law.

Law was basically, according to Austin, a command issued by a sovereign. Austin makes the focus of regulation an expression of desire from the sovereign backed up by a credible threat, or use, of force. Therefore regulation becomes the command and control structure. The sovereign issues commands (expresses desires) and the subjects must obey if they are not to be subjected to the control mechanisms available to the sovereign.

As Austin was concerned with removing value judgments from the concept of regulation he does not attempt to discuss the sovereign or the legitimacy of the sovereigns use of force. For Austin the sovereign was an individual or an entity with control over a geographical space and the people within that territory. Austin makes one qualification in that the sovereign is the "unobeying obeyed", this refers to the fact that the sovereign is supreme and has no superiors that command him/her/them. Aside from this qualification the sovereign need not be legitimized in any form, it is enough that the sovereign has the power to make credible threats. If the threat of punishment is convincing then the subjects will obey.

Since Austin's presentation of the command and control structure of regulation devoid of legitimacy, morality and the concept of good and bad regulation the discussion has been active. The main thrusts of these discussions have been fundamentally in agreement with each other and represent an incremental growth in our understanding of the process of regulation. In *The Concept of Law*, Hart (1994) writes about the concept of regulation:

> In any large group general rules, standards and principles must be the main instrument of social control, and not particular directions given to each individual separately. If it were not possible to communicate general standards of conduct, which multitudes of individuals could understand, without further direction, as requiring from them certain conduct when occasion arose, nothing that we now recognize as law could exist. (p 124).

Therefore Hart posits that the fundamental building blocks of any regulatory regime are the communicable rules, standards and principles in society. This therefore entails a communication between the sovereign and the subjects. The focus of the discussion has become a question of how rules are to be made as to facilitate their understanding, enforcement and compliance. The main focus of this body of work has been on the concept associated with *command and control regulation*, which can be best described as a system of statutory rules backed by sanctions (Black 1997). The fundamental idea is to create regulation which is "compliance oriented" (Baldwin 1995) these rules would be designed in such a manner as to promote the ease in which they could be adhered to. However it must be understood that the creation of regulatory rules is a process of simplification. The rule must take a simplified understanding of reality to enable large groups of regulated subjects to fall within the scope of its purpose. The rule is not only by its nature a simplification of an existing understanding of reality it is also "hostage to future developments" (Black 1997) which may utterly change the meaning and purpose of the rule. These latter problems become very obvious in times of rapid technological change when rules based upon one presupposition of technology are suddenly being applied to a new technological infrastructure with very different results.

An example of this process can be seen in the Swedish data protection legislation prior to 1997. The Data Act (*Datalagen*) was introduced in 1973 and required everyone who wished to store other people's personal data to apply for permission from the Data Inspection Board (*Datainspektionen*). The Data Act was in force up until 1998. Technological advances between 1973-1998 saw the advance not only of personal computers but also of mobile telephones. If the law were to be slavishly enforced every mobile telephone with an address book would have required advance permission from the Data Inspection Board. The regulation become unenforceable through the sheer development of technology since enforcement would have required an inordinate level of administration.

Recently there has been a growth in the questioning of the straightforward command and control structure of regulation (Baldwin 1995, Black 1997, 2002, Braithwaite & Drahos 2000, Ellickson 1991, Maher 2002). This has opened up the discussion to include a more decentred perspective of regulation that includes more than the established rules enforced by sanctions approach. Black (2002) identifies five core concepts: (i) complexity, (ii) fragmentation, (iii) interdependencies, (iv) ungovernability and (v) the rejection between a clear distinction between private and public.

Adopting a decentralized view of regulation takes into consideration the complexity of interactions between social actors and social structures. Admitting to complexity entails a recognition that everything cannot be understood and that social interaction between actors and between actors and structures is in a state of constant development. Black's fragmentation refers to the fragmentation of control. In traditional regulatory theory the control element of command and control was taken for granted. However this is too great a simplification for the model to hold true. There exists a great knowledge and power asymmetry between the regulator and the regulated. The regulator cannot be knowledgeable in all fields and all things. The decentred approach therefore takes as its starting point that no one actor has the information necessary to resolve complex problems. This can be further problematised by the understanding that there can be no social objective knowledge since information is socially constructed (Berger & Luckman 1967). Within regulation this therefore means that social subgroups and systems such as law, administration or technology create their views of other systems through the distorting lens of their own reality. Therefore the information/knowledge understanding one subsystem (such as law) has of another subsystem (such as technology) is the result of what the former system (law) has created with their own tools, experience and knowledge (Teubner 1993).

The multiplicity of subsystems also provides another vision of fragmentation and this is the fragmentation of power/knowledge (Foucault 1980). Since there are many different subsystems that are unable to obtain the dominant truth, also unable to regulate and enforce alone (Foucault, 1991) the subsystems then become interdependent upon each other.

The realization that there is no one great system but rather a complex interaction of many subsystems leads to the inevitable conclusion of system of ungovernability (Foucault 1991). To be able to govern the regulator must obtain legitimacy and support from a large number of the subgroups within and without of the regulatory sphere. Upon understanding the interplay of dependencies between actors within and between subsystems there occurs what Black (2002) terms "the collapse of the public/private distinction". This is a re-evaluating of the formal authority of government. The decentered view understands regulation as something that "happens". Not dependant upon formal legal sanctions being in place. Black (1997) describes the rule making process as:

> …contextual, stressing the significance of the market and political context, the institutional and legal structure, and of the dynamics of the system itself, its

> history, the norms and perceptions of the regulators and their awareness of the potential uses of rules, and the stage that their system is at in its own evolution. These factors interact, shaping both each other and the rule making decision. The rule making process is characterized by a high degree of casual complexity, involving the interaction and confluence of these different factors. The influence of some may be constant and structural, others ephemeral; some may act as catalysts, reacting with another to exert a particular type of influence or pressure at a particular time; some may always dominate, others only at particular points. (Black 1997, p 215).

Therefore regulation is the product of the complex, fragmented interactions and dependencies of many social subsystems. Naturally the legal, administrative, political subsystems play an important role in the production but they do not dominate the regulatory discourse. We should understand regulation not as a hierarchical process in the hands of one elite but rather the product of the interactions and the webs of influence of the many subsystems involved in the process (Black 2002, Braithwaite & Drahos 2000, Rhodes 1997).

Regulating Technology

Technology has only recently become to be seen as a separate subset deserving specific regulatory norms. The large-scale discussion on the role of regulation of technology use can be seen to have developed from the widespread use of information technology in general and the Internet in particular.

The early beginnings of the regulation of Internet-based activity began to form in the early 1990s. At the time the United States Secret Service was attempting to prevent the spread of the so-called E911 document. The latter was an illegally copied document that described how the emergency 911 systems worked. The Secret Service executed a warrant against a game publisher called Steve Jackson Games, a suspected recipient of the E911 document, and removed among other things, all their computer equipment. Once the computers were returned, Jackson's employees realized that all of the electronic mail that had been stored on the company's electronic bulletin board computer, where non-employee users had sent personal messages to one another, had been individually accessed and deleted. Jackson believed his rights as a publisher had been violated and the free speech and privacy rights of his users had been violated. Upon hearing what had happened a group of technologists, realizing the implications technology has on civil liberties, founded the Electronic Freedom Frontier in 1990 and represented Jackson in a lawsuit against the United States Secret Service. The Steve

Jackson Games case was important since for the first time a court held that electronic mail deserves at least as much protection as telephone calls (Sterling 1994).

Events such as these were bringing the discussion of the regulation of Internet-based activity into focus. The groups defending civil liberties came to be known as cyberlibertarianists (Winner 1997) while an alternative school of thought, which has come to be known generally under the name of cyber-paternalists (Murray 2002). A basic foundation of the Cyberlibertarian understanding of technology is that the communications protocols and online social communities of networked information technology create a new form of politics. Based mainly in the belief that Internet technology blurs our understanding of place, the cyberlibertarians argue that with the disappearance of the locus of action the state no longer has the legitimacy to either command or control. This makes both established institutions of power, political influence or protest groups obsolete. The cyberlibertarian ideal is portrayed through early writings entitled *Cyberspace and the American Dream: A Magna Carta for the Knowledge Age* (Dyson *et al* 1994), *A Declaration of the Independence of Cyberspace* (Barlow 1996) and *Birth of a Digital Nation* (Katz 1997). In his declaration Barlow (1996) writes:

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather…We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different.

Both through their titles and their content these early documents attempt to establish the domain of Cyberspace as being beyond the control of traditional government. Additionally, by attempting to emulate and echo traditional, historical rights documents the authors attempt to connect to established praxis whereby the absolute state power is curtailed, thereby granting online activity special privileges.

During this period it seemed that the information environment was heralding the decline and fall of the State. Removing territorial limitations to interaction between actors the technology challenged the states claim to legal use of force within its territorial boundaries. The lack of centralized control and ungovernability led many commentators to stress the importance of alternative private ordering schemes (Lessig 1999), and view the technology as a post-national state-of-being (Johnson & Post 1996).

The cyberlibertarian school combines an enthusiasm for electronically mediated forms of living with right wing libertarian ideas on freedom, society and markets. From a regulatory point of view, the cyberlibertarian position was originally set out by Johnson and Post (1996) in their seminal paper entitled *Law and Borders - The Rise of Law in Cyberspace*. The paper posits the cyberlibertarian contention that traditional state sovereignty, based as it is upon notions with physical borders cannot function in cyberspace. People move seamlessly from regulatory regime to another. In some cases this movement is not evident to the user.

This ability to move allows individuals to choose the regulatory regime which best suits their requirements. A system of regulatory arbitrage (Froomkin 1997) quickly develops and is seen as proof for the cyberlibertarians, that cyberspace is inherently unregulable by established hierarchical control systems (Murray 2002). The only alternative system of regulation is a grassroots approach relying on the consensus of the users of these virtual spaces (Johnson & Post 1998). Therefore the cyberlibertarian approach is that regulators appearing in cyberspace will act as the agents for individual or group interests (Murray 2002). Regulators will therefore be unable to regulate against the will, and tacit consent, of the regulated since such regulation will entail the movement or exit to alternative regulatory regimes.

This early libertarian position was not without its critics. Among these we find Langdon Winner, who criticizes the highly individualistic approach the cyberlibertarians take. Winner (1997) writes:

> In sum, my suggestion is not that we need a cyber-communitarian philosophy to counter the excesses of today's cyberlibertarian obsessions. Instead is a recommendation to take complex communitarian concerns into account when faced with personal choices and social policies about technological innovation. Superficially appealing uses of new technology become much more problematic when regarded as seeds of evolving, long term practices. Such practices, we know, eventually become parts of consequential social relationships. Those relationships eventually solidify as lasting institutions. And, of course, such institutions are what provide much of the actual framework for how we live together. That suggests that even the most seemingly inconsequential applications and uses of innovations in networked computing be scrutinized and judged in the light of what could be important moral and political consequences.

Another critic of the cyberlibertarian school was Joel Reidenberg (1996, 1998) who introduced the concept of *Lex Informatica*. Reidenberg argues that policy-makers can resolve conflicting policy problems by understanding, recognizing and applying the theory of *Lex Informatica*. According to the theory of *Lex Informatica*, technological capabilities and system design choices, as well as user preferences, impose overarching default rules on users of cyberspace technology. Reidenberg's work on *Lex Informatica* was to have a strong influence on the future debate of technology regulation and the Cyber-Paternalist position.

While cyberlibertarians such as Perrit (1998) argued for a revised position taking into consideration the growing criticism of the libertarian approach to online regulation. Perritt (1998) argued for a relativistic position where the effect of the Internet on the state depended very much upon the state in question. Liberal democracies, for example, would be improved by the Internet since the freedoms of the press and speech within these states would be enhanced. While autocratic states would be threatened by the technology since it provided an element of uncontrollability. This middle way approach was attacked from both sides. From the cyberlibertarians Post (1998, p 527) argued, "…Liberal theory itself contains a set of often unacknowledged normative premises that pose a deeper peril for the institution of statehood than Perritt suggests. These premises require us to ask not whether a world of Realist or Liberal states comports better with the new realities of the Internet, but rather how these new conditions affect our normative justifications for the existence of the state itself." The Cyber-paternalists quickly pointed out that, "there is no single monolithic concept of sovereignty to be threatened - we already live in a world of multiple, overlapping, contradictory and oftentimes intensely contested sovereignties." (Aoki 1998, p 443).

Eventually the cyberpaternalist view that would come to dominate this young discussion, mainly in the form of the book *Code and Other Laws of Cyberspace* by Lawrence Lessig (1999). In this work Lessig (1999) challenges the presumption that technology has created an inherently free environment will remain so if governments leave it alone. Lessig observes that cyberspace is susceptible to control by other means and the greatest threat is the control of the computer code that constitutes the environment.

Therefore when cyberlibertarians argue that the design of the Internet leads to regulatory arbitrage and makes established hierarchical regulation impossible, Cyber-paternalists argue to the contrary. They argue that the design is a form of hierarchical regulatory control (Lessig 1999). The underlying code of Cyberspace, the software it requires and even the protocols constituting the network act as a constitution setting out the limits of behaviour. In his words, "Code is Law." Instead of finding inherent freedoms in the technology the paternalist sees a multitude of regulatory possibilities. The question is never “if” regulation is possible, but only “who” regulates and “how”? The lack of state regulation leads the cyberlibertarian to erroneously think that Cyberspace is unregulated and unregulatable. This is erroneous since this presupposes a very limited view of regulation as one of the established state control through command and control mechanisms. In response to the “who” question Lessig (1999) replies that since code is a form of regulation then the proprietors of code set regulatory standards. Software developers who control code play a central role in the regulation of the Internet. This is not a position of absolute power. Those developing and controlling the software are part of a wider network or regulators. This network is tentatively described by Aoki (1998), and includes a greater role for the private sector. This private/public hybrid model of regulation is now clearly being applied to Cyberspace.

Recent legislation has however re-enforced the role of the state as a fundamental player. Legislation such as the USA PATRIOT Act (2001) and the Homeland Security Act (2002), the UK Antiterrorism Act (2001), and the Convention on Cybercrime, clearly mark the ability and intention of the state to take an active part in legislating the digital domain. The Cyberpaternalist writers are today claiming victory showing that the state has never left the arena of regulation. They show that the states ability to regulate today proves that the state was never in danger of becoming a secondary actor on the regulatory scene (Birnhack & Elkin-Koren 2003, Bowrey 2005).

Lessig (1999) writes on the relationship between technology and law, particularly in relation to digital environments. Lessig observes that the there are four modalities of regulation: laws, norms, markets, and architecture. Simply stated, law regulates through the threat of punishment, norms regulate through the threat of social sanctions or exclusion, markets regulate through price-setting mechanisms and architecture may regulate by physically limiting behaviour. Each of these modalities works directly or indirectly in combinations to regulate behaviour. By introducing the four modalities Lessig recognizes that the changes in any of the modalities have an effect on the behaviour of the regulated. Therefore this must be understood to mean that changes to the architecture have a direct effect upon our behaviour. The importance of regulation through architecture has been previously recognized and implemented. For example speed bumps are used to regulate traffic flows or in a more ominous example: the use of low bridges to prevent buses to certain areas of cities, which increases the segregation between rich (car owners) and poor (dependant upon busses)

(Winner 1986). Architecture takes upon a whole new importance in cyberspace since the environment is highly susceptible to environmental change.

Lessig's (1999) four modalities of regulation (law, markets, norms and architecture) act as effective regulators since they all work in a way to constrain certain actions. Law constrains through the threat of punishment, markets use pricing and price related signals to constrain, norms constrain through social sanctions such as exclusion or ostracism and architecture uses physical constraints (such as a locked door).

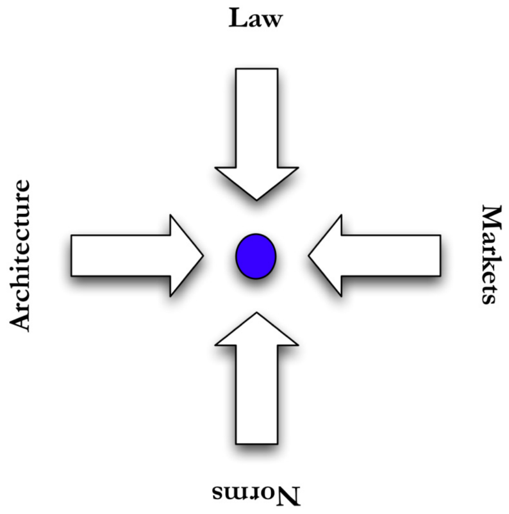

Figure 1: Lessig (1999) Modalities of Regulation

These modalities of regulation may effectively explain systems of regulation both in the physical world and in Cyberspace. The labels used by Lessig to explain regulation have not gone without criticism (Murray & Scott 2001). Murray and Scott (2001) show that Lessig's description needs further development to better understand the underlying elements, which generate the regulatory system.

> This development of the analysis provides a clearer descriptive framework for understanding how control is or can be achieved and opens up the possibility for identifying the wide range of control systems which appear as hybrids of two or more modalities of regulation. (Murray & Scott 2001, p 502).

The advantage of the developed model is that it goes beyond the simpler command and control understanding of regulation and approaches method by which a more complex analysis can be made. The developments in the analysis model include the study of three functional dimensions: (i) standard-setting, (ii) information gathering and (iii) behaviour modification involved in each of Lessig's (1999) modalities.

Elements of a Control System	Hierarchical Control	Community-Based Control	Competition-Based Control	Design-Based Control
Standard Setting	Law or Other Formalized Rules	Social Norms	Price/Quality Ratio	Inbuilt design features and social and administrative control
Information Gathering	Monitoring (by agencies or third parties)	Social Interaction	Monitoring by dispersed buyers, clients etc	Interaction of design features with environment
Behaviour Modification	Enforcement	Social Sanctions (eg ostracism, disapproval)	Aggregate of decisions by buyers, clients etc	As for information gathering (self-executing)

Table 2: Elements of Control System (Murray & Scott 2001)

Terms such as "Law" and "Norms" are far too over-inclusive. Both "Law" and "Norms" refer only to a standard or director and is therefore missing the other essential elements of a control system (Murray 2002). These two modalities of control should rather be referred to as "hierarchical control" and "community-based controls" (Murray & Scott 2001). The remaining modalities are considered to be under-inclusive and should be re-labelled. Markets would be better entitled "competition-based control" while architecture should be referred to as "design-based" control (Murray & Scott 2001).

This is not a simple re-labeling of terms but an attempt to create a theory that will encompass the largest range of regulatory strategies and instruments (Brownsword 2005). The analysis of regulation within this work is based upon the work of Murray and Scott (2001), which has since been further developed by Murray (2006). This choice is motivated by the latter's more nuanced understanding of regulation and its effects. This understanding is critical when attempting to bring together multiple case studies to draw conclusions on the effects of the attempts to regulate disruptive technology on Internet-based participatory democracy.

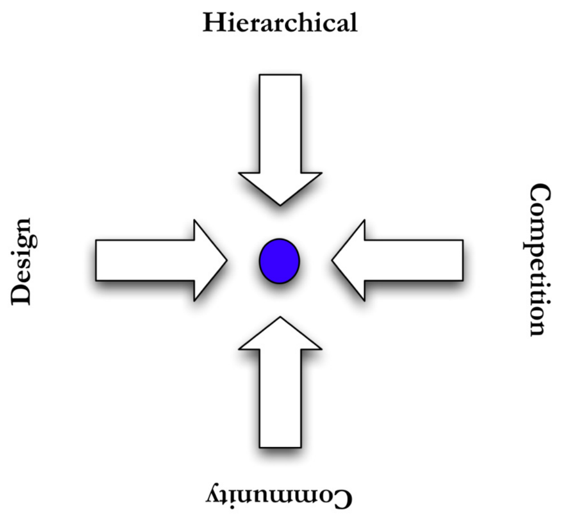

Figure 2: Murray & Scott (2001) Modalities of Regulation

The criticism of cyber-paternalism does not remain on the level of critiquing the labels used in the theory. Through the critique of the cyber-paternalists we can see the rise of the neo-cyberlibertarian school. The proponents of this idea (Murray 2006) are moving towards a more complex understanding of the role and nature of the regulation of disruptive technologies such as the Internet. The domain of cyber-regulation becomes complex largely due to the difficulty in controlling the "physical" environment. In addition to this there is the complex problem of decentred or polycentred regulation (Fuller 1964). These latter concepts refer to the idea that regulation does not come from a single source. A more nuanced understanding of regulation must include the understanding that regulation consists of competing regulators, even within the same regulatory body. Therefore once we begin with a mature understanding of regulation to mean the enterprise of subjecting human conduct to the governance of external controls whether state or non-state, intended or unintended (Baldwin *et al* 1998) the advantage of this inclusive definition of regulation is that its takes into account the Law as "the enterprise of subjecting human conduct to the governance of rules". (Fuller 1964, p 106). These definitions provide the regulatory theorists with the manoeuvrability necessary to discuss regulation even when it appears as conflicting systems (Fuller 1964). As Fuller himself noted, "A possible . . . objection to the view [of law] taken here is that it permits the existence of more than one legal system governing the same population. The answer is, of course, that such multiple systems do exist and have in history been more common than unitary systems." (p 123). Viewing regulation as polycentric legal systems (Fuller 1964) entails a moving away from the traditional regulatory model of state monopoly (Murray 2006). This is necessary if we are to understand the complexity involved in the regulation of global information technologies such as the Internet.

Theoretical Focus

In the beginning of the chapter on theory the position of this work in relation to the theory was laid out. This began with a view of structuration theory being a theory used to show the social interaction between the regulator and the regulated. This theoretical starting point has also been chosen to show that regulation is a continuum, albeit which can be broken down into specific cases or legislative acts, that deals with the interaction of the actor and structure.

In relation to regulation as a discipline this work is not dependent upon the formalized understanding of legal regulation in the form of laws and court actions. Regulation must be understood to be the exercise of power within social interaction. In this case regulation can take the form of inanimate objects. Objects do regulate social behaviour. Both Winner (1985) and Latour (1992) have problematised the social role of technology as regulator. Winner provides examples of low bridges in New York being used as physical barriers to class interaction. The latter example has been questioned more recently (Joerges 1999) however even the questioning of Winner's example does not diminish the power of his conclusions. Latour (1992) provides us with an example of regulation by heavy doors which discriminate against the weak and therefore act as limitations on what we are capable of doing. Lessig provides several examples in his attempt to show that computer code *regulates* or acts as a *modality of regulation*. These are expanded views on the understanding of regulation and they are fundamental to the understanding of regulation described in this work. Objects do regulate our actions in the sense that they guide and control what we should and can do. Social actors are conditioned to obey the guidance of these objects (Norman 1990).

However it is important to differentiate between the object regulating behaviour, in the sense of guiding, controlling or enabling, and the object becoming a modality of regulation. Whether it is a computer code or barbed wire that guides and regulates behaviour the object in itself is not regulating through its own will. The inanimate objects of our regulation cannot react to the actor's reactions. The inanimate objects are simply tools of the regulator. Therefore when Lessig (1999) introduces his four modalities of regulation (market, law, norms, architecture) he defines them as modalities, which have an effect on online liberty (in the sense of Mill 1980 [1859]). In doing this he is using the definition of regulation in the widest sense (Baldwin *et al* 1998) as described above and can be summarised by the formula: all manner of control, state or non-state, intended or unintended.

However, there is an important distinction to be made in the four regulatory norms provided by Lessig. Laws, markets and norms are socially mediated modalities while architecture is environmental modality (Murray 2006). The Internet creates an environment that, due to the malleability of code, becomes sensitive to regulatory intervention. However, since code is an inanimate regulator and does not react to the actor it is extremely difficult to predict the effects of code-based regulation. In addition to this the fact that the online environment is, in some important senses, beyond regulation due to the fact that code regulation can be circumvented and obfuscated by other implementations of code, it is highly unlikely any regulatory intervention will successfully bring to an end any ongoing regulatory conflict. Simply stated: Using legal rules to attempt to control a volatile changeable environment is virtually impossible since the rules can only with difficulty define what they are set to regulate and, as this work will show, without clarity of definition regulation is severely frustrated.

In attempting to grapple with the issue of regulating disruptive technology it is inevitable that comparisons with other regulation be made. This inevitable comparison leads to the question of whether technology is different? In other words is the phenomenon of disruptive technology so different that it should be treated as a special form of social interaction and no follow ordinary regulatory theory? This question is more often dealt with in public or political debate. The concept of new technological communication being something that requires special consideration is often repeated for new technologies (Kern 1983, Ilshammar 2002).

This point of view usually recedes and new technology becomes common technology and is treated no differently than any other common technology. This development can be understood as the functional equivalency (Di Lello 1993, Posner 1996) approach to technology regulation. This approach is an attempt to avoid discriminating any form of technological interaction by showing preferences towards a particular form of technology or technological standard.

The functional equivalency approach is based on an analysis of the purposes, requirements and functions of the activities with a view to determining how those purposes or functions could be conducted within an online environment. The basic premise is that the adoption of the functional-equivalent approach should not result in imposing on users of online communication more stringent standards than in an offline communication.

The concept of functional equivalency came from a concern with how to deal with the disruptive effects of ICT. This concern was voiced by Tribe (1991) when he wrote that modern computer technology was changing established social relationships and, in particular, facilitated new forms of social interaction between individuals, government, and institutions. The disruptive effects of ICT created problems for the courts, since they are unable or unwilling to apply constitutional principles to these new social relationships (Tribe 1991). The method of applying the functional equivalency approach was first used in regulatory procedure by Judge Leisure in the case of *Cubby, Inc. v CompuServe, Inc.*[6] CompuServe provided access to an online information service with access to hundreds of specialised databases. The question of concern to the court was whether CompuServe could be held criminally liable for the content in these databases. Stated in another way – was CompuServe a publisher (and therefore legally liable) or a distributor (and therefore not legally liable) for any criminal content in the databases? In attempting to answer this question Judge Leisure wrote:

> …a computerized database is the functional equivalent of a more traditional news vendor, and the inconsistent application of a lower standard of liability to an electronic news distributor . . . than that which is applied to a public library, bookstore or newsstand would impose an undue burden on the free flow of information. (Judge Leisure, Cubby v Compuserve).

Here we can see an application of the method of functional equivalency. The idea is to be technology neutral and not place onerous burdens on any technology simply because it is not the most used technology. The goal is to allow the adoption of new technology without demanding that it fulfils more demands than its older alternatives. To put it bluntly: we live in an imperfect world therefore we should not expect perfection in our Internet-based interactions.

Therefore in implementing the functional equivalency approach we must analyse the online and offline to see their effects and side-effects in relation to the right of political participation in a democracy. This participation demands the freedom to communicate for without communication there is

[6] 776 F. Supp. 135, 140 (S.D.N.Y.1991)

no participation. The ability to communicate consists of several parts such as the physical or technical ability to communicate, the political right to communicate, the economic ability to communicate (McQuail 1984).

Core Democratic Value	Empirical Focus	Regulatory Discourse	Democratic Effects
Participation (Case 1)	Online Disobedience	Online communication	Discriminates against online participation
Communication (Case 2)	Virus	Protection of property	Discriminates against online communication
Integrity (Case 3)	Spyware	Protection of contracts	Failure to defend user integrity
Property (Case 4)	MMORPG	Protection of contracts	Disincentive for online participation
Access (Case 5)	Software	Ideological lock-in	Discrimination against non-commercial production
Autonomy (Case 6)	Online Censorship	Protection of cultural values and norms	Patrimony

Table 3: Core Democratic Value, Regulation and its effects

While it is important to use the functional equivalency approach to ensure that technology is not being overregulated and that there is no loss of the right to communicate and participate in a democracy via technological mediums it is important also to recognize that even regulation brings with it unintended consequences. Unintended consequences do not only occur within the domain of new technologies but are frequently present in regulatory decisions (Beck 1992, Kallinikos 2005, Rolland 2002, Tenner 1997). This work will strive to exemplify and analyze the effects of regulatory intervention and show the effects of such intervention.

Table three shows the core democratic values addressed in each of the cases in this study. Each of these values is identified as being parts of the foundation of the modern participatory democracy. The regulatory discourse can be seen as both the discussion and the cause of the discussion concerning the core democratic values. The effects listed here are those effects that the discourse has brought about to date. These are not to be understood to be an exhaustive list but are the most salient feature of the specific discourse.

Case 1 Participation/Disobedience

Attempts to apply Internet-based communication for the purpose of democratic *participation* (Pateman 1970) have occasionally caused some alarm. In cases where the Internet has been used for political protest have motivated regulators to limit the ability of politically activated users to use Internet-based communications as an infrastructure for civil disobedience (Castells 1997, Pickerill 2003). The underlying regulation of such activities has been efficient since the ability for individuals to connect to the Internet is governed by contractual relations. The communication via Internet technology based on contractual relations is easily monitored and regulated. Individual access points to the Internet can be regulated through the contract between the user and the service provider. This creates additional difficulties for the creation of the Internet as a public sphere (Habermas 1989) as will be discussed further in this work. Internet communications are not treated as being functionally equivalent to offline communication. The effect of this weak position of the user is that the ability to conduct civil disobedience activities online is threatened, which leads to the discrimination of online activities in the sense that these are not tolerated to the same degree as offline activities.

Case 2 Communication/Virus

A basic premise of participatory democracy is the ability to *communicate* freely (Schauer 1982). Case two in this work deals with the issue of computer viruses. Due in a large part to the simplified media discourse (Kling *et al* 2005) the concept of virus is almost universally vilified. Regulatory structures in most areas affect an almost unified approach towards viruses and prohibit their creation and dissemination. However, while the concept of virus may easily be regulated against the definition of what has been regulated is insufficiently described. This causes several non-harmful virus-like applications of software to potentially fall under this regulation. The reliance on the simplified view of viruses creates an inability for certain forms of communication thus creating a democratic deficit. The role of freedom of expression is vital within a participatory democracy. The purpose of such a right is to protect controversial expressions – uncontroversial expression needs no protection.

Case 3 Integrity/Spyware

Case three involves the examination of the role of *integrity* in a participatory democracy (Sundström 2001). In this case study we can see the effect of when users experience a lack of integrity through spyware. The perceived lack of integrity caused concern among users. This case will discuss the negative effects of the lack of integrity protection for a participatory democracy in terms of the regulatory powers inherent in the internalisation of surveillance (Foucault 1979). This concern was however met with a regulatory inertia since the apparent legal position of the software in question could be disputed. This lack of concern for the users opinions vis-à-vis integrity resulted in the creation of a market based regulatory solutions. These solutions came in the form of integrity protecting, spyware removal software.

Case 4 Property/MMORPG

Case four deals with the core democratic value of *property* (Harris 1996). This case examines the frontiers of intellectual property in that it looks at the conflict that appears in the creation of intellectual property in online environments. The basic disagreement surrounds the ownership of artefacts within massively multiplayer online role playing games (MMORPG). From the traditional point of view these environments are created and controlled by private organisations and the users are regulated by contractual agreement with the private organisation. Among the users there has been a growing belief in that they own their online characters and any artefacts they find within the world. This opinion is widespread among the players but is contrary to the contract. This case shows that there is a growing re-appraisal or negotiation on the way in which intellectual property originating in online environments should be understood. This entails that there is a re-evaluation of the role and concept of property being driven by the users of MMORPG. This is tantamount to a grassroots revolution to see a user-driven re-appraisal of one of the core values in democracy being negotiated in this manner.

Case 5 Access/Software

Another core value in a democracy is the right of *access* to the general infrastructure (Åström 2004). The study in case five demonstrates the way in which this right can be problematised within the digital environment. The case concerns the present day distinction between the development rationales for software. The traditional form of software (erroneously referred to as proprietary software) production is based upon an economic rationale. In other words the motivation to make software is to make economic profit from the activity. The last 25 years have seen the growth of politically motivated software development. The latter is an attempt to build a digital infrastructure that grants the user a greater amount of freedom. Through policy documents and technological decisions there is a state bias towards the use of economically developed software. This bias discriminates against the ideologically motivated software developed in society and in certain cases this bias can result in state subvention of individual products, to the detriment of others.

Case 6 Autonomy/Censorship

The final core democratic value studied in this work is *autonomy* (Harrison 1995). In case study six the control and censorship of online information is studied. The study looks at the more blatant forms of information control carried out by government who use technical and social means to openly limit information flows. In addition to this the case study also looks at the more subtle forms of controlling online information. The latter are more commonly implemented within democratic governments and can be seen as a delegation of regulatory practices to the service provider. The rationale for the limitation of online communications can be seen in the re-occurring moral panics (Thompson 1998) surrounding technology. Structural regulation of communications through the persistence of paternalistic information policies results in the loss of user autonomy in relation to the online environment. This in turn results in the discrimination of the online communications medium.

As this brief overview has shown the cases in this work all reflect individual core values of a participatory democracy. The choice to include these core values has been to demonstrate the role of technological regulation. Such regulation can be conducted in many forms. In case one we see a direct legislative approach to regulation while in case five the regulation is mainly by technical policy. What is important to recognise is, irrespective of the regulatory approach, the regulation of technology is the regulation of democracy.

3

Method

I have come to believe that the whole world is an enigma, a harmless enigma that is made terrible by our own mad attempt to interpret it as though it had an underlying truth.

Umberto Eco

Research Process

The research presented within this thesis began in early 1999 when the author began participating in studies concerning virtual online communities. These studies revolved around the new form of interaction dubbed the virtual community (Rheingold 1993, Kollock & Smith 1998). Much of the focus of these studies surrounded the concept of community and whether such a thing could exist in a technologically mediated world. At the same time there was a growing understanding amongst regulatory theorists that this technology created an interaction that did not fit easily amongst the established theories. The cyberlawyers (at the time names such as these were desirable amongst those wishing to show that they understood that the technology created a new form of law) argued that cyberlaw was a growing and important discipline. While those who disagreed at best ignored the topic at worst argued that this was academic dilettantism (Easterbrook 1996).

From these earlier studies the basic idea of looking towards regulatory attempts to resolve "problems" in online environments arose. The fundamental idea was to collect data on attempts to identify and regulation problems in online environments. The result of this work became the six studies that make up the bulk of this thesis. All these studies are studies of how Internet technology impacts our society in different ways. In addition to this end the studies also illustrate how such technology is being regulated within society. This regulation is carried out both by formal structures such as law but even by the more ephemeral negotiations carried out by the actors touched by the technology.

The data collected in these studies include the formalized structures of legal regulations. These are analysed both in the light of what that regulation claims to achieve and contrasted with the arguments of groups who feel that such regulation either does not achieve the desired goal, or while reaching the desired goal creates undesirable side-effects which negate its beneficial action.

The purpose of chapter three is to explain both the general development of this work in the sense of which topics were explored, in what manner and in what order. The case studies in this thesis are presented in the chronological order in which the research was undertaken.

Methods Applied Case 1: Participation

The first case (*Participation*) was initiated by the Convention on Cybercrime in 2001 and the work was conducted during 2002. The actions of the structure are represented through legislative documents and preliminary materials. The response to the Convention is represented by the actions and texts of primarily two groups who conduct actions defined, by their own publicity, as civil disobedience. The conflict in this case study is to analyse the legitimate needs of the regulator with the desire of the actors to conduct activities of civil disobedience in online environments.

The event that triggered the research into this area was the development of an online discussion which took place mainly between two groups of activists: *The Electrohippies* and *The Cult of the Dead Cow*. The main thrust of this online discussion was the attempt to define and delineate what was, and what could be, acceptable online political activism. The debate mainly took place through email discussion lists, web pages and presentations of ideologies in print media. The two organisations argued on the legitimacy of the use of denial of service as a legitimate form of online civil disobedience. The debate itself may be seen as a way in which different actors attempt to create meaning and order by arguing for the legitimacy of their actions. This debate was subsequently interrupted by the presentation of the Cybercrime Convention. As an act of regulation the Convention criminalised the act of denial of service, in addition to many other acts of online political activism that were seen as less controversial by the two groups.

The documentary sources provided by the discussions and printed documents of the two groups provide the official views of the actors. This material is supplemented by additional material in the form of email interviews carried out with representatives of the groups. Due to the nature of email interviews the material is less forthcoming than face-to-face interviews. This is due in part to the loss of additional information, such as the physical actions of the interviewee during the interview. Additionally written question and answer sessions tend to be less spontaneous which may have the effect that the replies tend to be more structured and thought through. However the interviews provide an additional richness with which to complement the more formal written material.

The main source of this chapter remains the formal written sources. We are provided with the organised presentation of the arguments used by the actors involved in online political activism. This is then followed by the structural regulation by the Convention and the documents that surround it, and provide it with an environment. The main empirical work of this chapter has been conducted between 2000-2002. The results were originally published in 2004 (Klang 2004a). This work was then re-visited in 2004 to obtain a deeper understanding of the effects of the implementation of the Cybercrime Convention and the reactions of the actors involved. This reworked version was published in 2005 (Klang 2005a). The reworking of the published material to form part of this thesis entailed additional empirical work during 2005. The formation of this work in this manner can be seen as a process of validation (Hammersley 1990) since the data collection and analysis took place in three complete and independent cycles. Each cycle was informed by the proceeding cycle and the iterative effect can be seen as a form of triangulation of results (Silverman 2005).

Methods Applied Case 2: Communication

The second case appearing in this work (*Communication*) deals with the development of harsher legal regulation against the threat of damage caused by computer viruses. The original work in this chapter was carried out primarily in 2001-2002 following the raised awareness on the importance of defining and discussing online criminal activities due to the presentation of the Council of Europe's (CoE) Convention on Cybercrime in Budapest in November 2001. The latter convention created a great deal of interest and discussion. The key conflict came from the increased demand of criminalisation created, amongst other reasons, by this convention. This increased demand of criminalisation conflicted with the lack of substantial definition (either technical or legal) on the nature of viruses. The foundational material used in this case study is mainly the regulatory attempts of governments to control (in this case to limit) the use of viruses.

The actors' negotiation is represented by alternative approaches to the harmful virus. The conflict within this case is exemplified by the constraining effects on legislation upon legitimate uses of viruses.

The original empirical work in this chapter was carried out primarily in 2001-2002 following the raised awareness on the importance of defining and discussing online criminal activities due to the presentation Convention on Cybercrime. The latter convention created a great deal of interest and discussion. The key conflict came from the increased demand of criminalisation created, amongst other reasons, by this convention. This increased demand of criminalisation conflicted with the lack of substantial definition (either technical or legal) on the nature of viruses. The foundational material used in this case study is mainly the regulatory attempts of governments to control (in this case to limit) the use of viruses. The actors' negotiation is represented by alternative approaches to the harmful virus. The conflict within this case is exemplified by the constraining effects on legislation upon legitimate uses of viruses.

In this chapter two different approaches to viruses are presented within the framework of three jurisdictions (Sweden, United Kingdom & United States). In addition to this the approach put forward by the Convention on Cybercrime is explained. These are presentations of the attempts of the regulatory structure to control the phenomenon of viruses. One of the fundamental problems with virus legislation presented within this chapter is a lack of coherent definition of what it is that is being legislated.

To enable a fruitful discussion on the role of virus regulation the chapter presents the views of actors who wish to develop virus-like software. It is important here to clarify that none of these actors present their actions as being harmful and therefore they believe that their actions are morally legitimate.

The studied artefacts that are the basis of this chapter are the regulative documents that provide the legal foundations for virus regulation in three jurisdictions and the Cybercrime convention. These artefacts provide the documentary foundation and creation of the structural regulatory view of viruses in society. To contrast this, the chapter performs a literature review with the express purposes of generating alternative interpretations of the various roles that viruses may occupy in society. The goal with this approach is to provide a critical foundation upon which to interpret and study the actions of the regulatory structure.

The main sources of this chapter are the analysis of national and international regulation compared with the practical implementation of beneficial or harmless uses of virus-like code. This work was initially conducted in 2001-2002, published in 2003 (Klang 2003a) updated and subsequently reworked to form part of this thesis in an independent research cycle to ensure the validity of the findings (Hammersley 1990, Silverman 2005).

Methods Applied Case 3: Integrity

The empirical work on the third case (*Integrity*) was conducted during 2002-2003. In this case study the actions of the structure are represented by the texts of the manufacturers of spyware and the scant legal opinions being delivered. The activities of the actors may be seen in the private initiatives to produce anti-spyware software and to maintain forums that discuss whether certain software contains spyware. In a sense these actions of the actors can be seen as private regulatory behaviour.

The main issue being studied here is the lack of reaction by the regulatory structure to the perceived privacy threat of spyware. This however does not mean that spyware exists in a regulatory void. There is no specific regulation of the spyware phenomenon but there is a legal position on spyware. This position can be found in the analysis of the legal principles of contract law. Therefore to be able to exemplify the regulatory position towards spyware, this chapter examines the basic legal principles, which provide the foundation for the legality of spyware.

The controversy of spyware is that many users protest its existence and the method of its implementation. The actors who are against the use of spyware also put forward legal arguments, which courts and regulators could use to prevent or curb the phenomenon. However no such regulatory action has been taken. These anti-spyware arguments will also be presented in this chapter.

While these two positions, for and against spyware, provide the background theories of this chapter, the main focus is on the growing solution to the threat perceived in spyware. The development and implementation of spyware discussion forums and later the development of anti-spyware software provide excellent examples of market based solutions. These market-based solutions are a form of regulatory system that each user can choose to implement. Therefore the example of spyware with its element of regulatory choice provides an interesting example of how actors may control and regulate their own technology in an attempt to gain control over their disruptive technology.

This case study is based upon empirical work conducted during 2002-2003. It contains the study of regulatory artefacts in the form of case law and fundamental legal principles, the study of online forums discussing the development of concern against spyware and also the study of the growth of anti-spyware systems and their impact on the perceived threat to privacy caused by the technology of spyware. The results have been initially published in 2003 (Klang 2003b) then further reworked and for subsequent publication in 2004 (Klang 2004b). The case presented here is a development of these two publications.

Methods Applied Case 4: Property

The fourth case (*Property*), concerns the legitimate claim to ownership in online virtual environments. These online virtual environments are created by private initiatives and are developed as private property. The research work, which forms the basis of this case, harkens back to the original studies carried out in 1999 which were then revisited in 2003. The activities of the users of these environments may create virtual commodities of value for the members of these environments. These commodities are claimed to be both the property of their online creators and the property of the creators of the online environments. The regulatory structure is represented in this case study by the licensing agreements and the negotiations of the actors can be seen by the different discussions being carried out in online forums and the academic field of game studies. This chapter takes its starting point by reviewing the position of the regulatory structure as created by the actual virtual environment and the regulatory environment that is created by the legal documentation that surrounds the massively multiplayer online role-playing game (MMORPG). This starting point is achieved by studying the fundamental legal position and applying it to specific position as created by contract law.

This position is then juxtaposed by the views of the actors. The actors are the players who oppose the legal position of the regulatory structure and attempt to claim property rights in the avatars and artefacts that they create within the virtual environment. In addition to the legal documentation, case law and contracts, which form the regulatory structure, this case study takes into consideration the points of views put forward by players in online forums, academic publications and carries out online interviews within the MMORPG in addition to hosting group discussions with active players. These latter activities are conducted in an attempt to bring forward the views of the active players who otherwise may not be heard. The research activities were conducted between 1999-2003 and published in 2001 (Klang & Roos 2001) and in 2004 (Klang 2004c). The chapter in this work is a revision of these early findings and the earlier publications enable a level of reliability and validity in the results (Hammersley 1990, Silverman 2005).

Methods Applied Case 5: Access

The fifth case (*Access*) grew from the researcher's participation in discussions on the ownership of software and software standards. These discussions were initiated in 2003 as a part of a project on the nature of property standards. The purpose of this project is to compare and contrast the foundations of property in computer software by comparing licenses from proprietary software, open source and Free Software. Since the incumbent norm is one of proprietary software the actions of the regulator and courts have reflect the acts of the social structures while the activities of the Open Source and Free Software movements can be seen as the negotiations of the actors in relation to this regulation. The empirical material available in this area is large and the choices have been made to find representative data from the different positions.

Among those against the introduction of software patents is the Free Software Foundation. The purpose of this chapter is to develop a greater understanding of the role of software in society in relation to its proprietary form and its distribution. Within this work the regulatory structure can be understood to be the established norm of software manufacture and delivery often known as proprietary software while the point-of-view of the actors is best presented by the ideology espoused by the Free Software Foundation.

This work aims to explore the alternatives to proprietary software in general and in particular explore the differences between the approaches taken by those groups attempting to present alternatives to traditional proprietary software.

The main part of the empirical work was conducted during 2003-2005 and consists of both a study of the basis of software as a form of property. This is then followed by a study of the alternatives to proprietary software in the form of Open Source software and Free Software. The study of these two movements is conducted both by studying their formative texts and their licences, which create the regulatory environment within which they exist. This is followed by a deeper exploration intended to better understand the differences between the two different movements.

In addition to studying the founding documents and the formative canon texts which surround these movements in-depth interviews were conducted with Free Software Foundation European representatives. Several in-depth interviews were conducted with the Vice-President of the Free Software Foundation Europe and one of the Team Members of the Free Software Foundation Europe. The research activities within this chapter have been conducted between 2003-2005 and have been published in 2005 (Klang 2005b). These results have been revisited and subsequently reworked for publication in this work.

Methods Applied Case 6: Autonomy

The empirical work on the final case (*Autonomy*) included in this work has been carried out during 2004. This sixth case deals with the control of access to online information. The structural regulatory actions can be seen as the manner in which states attempt to control the flows of information to the citizens. The manner in which certain groups attempt to circumvent these control mechanisms is the way in which certain groups of actors attempt to negotiate such technological regulation in the attempt to obtain and disseminate information.

To understand the structural regulation of online information through censorship it has been necessary to understand the manner in which censorship is conducted in practice among nations. This work is based upon the study of second hand sources in the form of regulations on censorship and studies of national censorship technologies. Among the different ad hoc studies (Deibert 2002, Zittrain & Edelman 2003) and the organisations who observe online censorship as a peripheral activity (e.g. Reporters without borders, Amnesty International). There has been a growing interest in online censorship studies. One such project is the Open Net Initiative, which is a collaboration between the University of Toronto, Harvard Law School, and the University of Cambridge. They have recently published reports on censorship activities in Saudi Arabia (2004), United Arab Emirates (2005), Bahrain (2005), China (2005), Burma (2005), Iran (2005) and Singapore (2005). The growth of these studies shows that the field is maturing and that a long-term field of research is being developed.

Once the behaviour of the regulatory structure has been established through the studies of technological censorship systems this work then studies the methods available for circumventing such systems. This consists of both technical systems for the purpose of censorship circumvention and texts made available on how Internet censorship functions and the methods in which it can be circumvented both through technical and social methods.

The purpose of studying this material is to understand the actor reaction to the regulatory structure of censorship. The research activities have been carried out during 2004-2005 and are due for publication (Klang 2006).

Case	Structures	Actors	Qualitative Base
Participation	Convention on Cybercrime Explanatory text Doctrinal documents	Electrohippies statement Cult statement Discussion lists	Email interviews with ehippies representative Mailing lists
Communication	Convention on Cybercrime Explanatory text Legal Analysis Doctrinal documents	Alternative virus uses in theory and practice	Email interviews with alternative virus creators
Integrity	EULA Documentation Legal Analysis Doctrinal documents	User group definitions of phenomenon. Spyware Classification documentation	Spyware discussion forums
Property	EULA Documentation Legal Analysis Doctrinal documents Policy documentation Case law	Theoretical presentations Research documentation	Online forums Group discussions Online interviews Online survey
Access	EULA Documentation Legal Analysis Doctrinal documents Policy documents	Position statements from FSF representatives and advocates	Interviews with FSF representatives
Autonomy	EULA Documentation Legal Analysis Doctrinal documents Policy documents	Test & evaluations Evasion documentation & manuals	Email interviews with circumventions advocates

Table 4: Data Collection

Research Activity

An efficient way of evaluating research methods is to attempt to discern the usefulness in bringing forth data to be analysed. This usefulness depends on how they fit with the theories in use, hypothesis to be tested and research field being explored (Silverman 1993). Ethnographic research, especially that which is based upon fieldwork in non-literate societies has focused the study of mainly oral cultures (Atkinson & Coffey 2004). The methodologies developed in this tradition have been widely used in the study of "advanced literate societies" where the social actors often practice advanced forms of documentation. While this documentation is not a form of ethnographic work it is important to acknowledge that many actors, organisations and settings studied today are to a large degree self-documenting (Atkinson & Coffey 2004). Despite this recognition, the social sciences have long prioritised the spoken word over the written word and the written word over the nonverbal communication in its attempts to understand human action (Hodder 1994). However this priority does not adequately enable us to study all situations.

Studying Internet interaction often entails the study of highly literate social actors. Therefore it is important to be aware of the fact that the bias towards oral cultures in social sciences may result in incomplete understanding of the social interaction. There is something intuitively wrong in studying highly literate settings based to a high degree upon written and nonverbal communication as if it were an oral culture. When studying these environments the researcher must pay attention to the analysis of documentary realities. The study of documents is important because documents create a version of social reality. This reality is however not "divorced from other levels" of social reality (Atkinson & Coffey 2004).

In studying textually based social interaction in this way it is also important to be mindful of the different roles played by documents. They are manufactured, organized and consumed, not always in the same context (Prior 2004). They can also be affected by the differing intentions of the authors, suppliers and readers (Prior 2004). Therefore it is important to attempt to gain insights into the context within which the text is used. This means that there cannot be absolute truths in the understanding of meanings of texts – only interpretation. While acknowledging the importance of interpretation it is equally important to recognise that the study of artefacts or material traces (such as documents and texts) left by human activity provide not better nor worse understanding of human action – but different.

Therefore to understand how regulation is carried out within the mediated world of the Internet we need to understand its context and its purpose. This entails defining its parts in the hope of understanding the whole. The development of understanding of the way in which we regulate disruptive technology helps us to understand the regulation of that which is new and which threatens that which is established. The results of such a study can then be applied to all domains where regulation of disruptive technology may occur. This may be within an organisation, a family group, a multi-national corporation or a state.

Researching Internet regulation requires a study of both the regulation being practiced on different levels, by different actors and the study of those being regulated online. This latter study requires following activities of online individuals, organisations and groups. The technology under study has the effect of making organisational boundaries increasingly permeable (Dutton 1999) as a result the study of online behaviour by necessity involves the study of computer-mediated communication. Studying these phenomena has both strengths and weaknesses (Pargman 2000, Sveningsson 2001)

Empirical Data

Throughout the studies conducted in this thesis the practice of observation was carried out. To obtain a clearer understanding of the regulated participation in online activities requires an understanding of both the requirements and goals of the human actors involved in the online activities. However it is important to note that while observation and participation provide rich empirical data it is frequently of questionable reliability since information collection is conducted over a limited period of time. In addition to this one must be mindful of Silverman's (1993, p 9) comments on observation that "qualitative researchers also argue that observation is not a very "reliable" data collection method because different observers may record different observations." Despite these weaknesses the value of observation and participation provide such a valuable source of rich information that it cannot be ignored. Therefore it must be included and tempered with other data to ensure that the material we base our analysis on is balanced.

Whenever possible, the interviews conducted in this research were face-to-face interviews (individually or in groups). Other interviews were carried out within the framework of this research in the form of email interviews and interviews carried out in online virtual environments.

These last two forms of interviews differ from the face-to-face interview in the data collection process (Bloor 1997). The data is shaped and formed by the context and circumstances in which it is collected. This factor must be taken into consideration in the analysis of the data since the data gathered in one interview form is not equivalent to the data gathered in another (Bloor 1997). This, however, does not imply that one set of data is inferior to another. As Hammersley and Atkinson (1995) point out:

> What is involved in using different research methods is not the combination of different kinds of data per se, but rather an attempt to relate different sorts of data in such a way as to counteract various possible threats to the validity of analysis. (p 231).

Differences between data collection in the two interview types include the aspects that online interviews are often low-cost and relatively unconstrained by time and/or space. It is however also important to be aware of the information which is not included in interviews which are conducted in other ways than face-to-face. The non face-to-face interview lacks the visual or aural cues that provide additional information and can be used to pursue a line of questioning. However the non face-to-face interview does carry with it some important advantages since they allow the interviewees more time to reflect and to structure their responses. This may improve the accuracy of the responses but it does reduce the spontaneity. Generally speaking, this is more true of the email interview than of the interview conducted in real time within a virtual environment.

Therefore, whenever possible this research has a preference towards the face-to-face interview. The alternative forms appear at first glance to be easier to conduct for both the interviewer and the interviewees. Taking everything into consideration the value of non face-to-face interviews cannot be considered to be less valuable. The different interview approaches have different strengths and weaknesses. In this research all interviews perform the same function, which is to help ensure the validity of the analysis.

As previously mentioned, different methods provide different results and have different strengths and weaknesses. Qualitative methods are more promising in obtaining full answers when investigating what people actually do. However the methods are not without weaknesses as they provide a certain type of data from the subject observed or interviewed. Therefore it is important to remember that to conduct "a full sociological analysis cannot be restricted to interview data, it must also consider the material traces" (Hodder 1994, p 395). The main methodological thrust of this thesis is the study of these material traces.

Hodder (1994) refers to the analysis of material traces as the study of mute evidence. This is because the study of material traces is the study of the artefacts that are created and left in the wake of our existence. The main difference between the study of artefacts and action is that the artefact exists beyond the moment of its creation. This endurance allows it to be transported in space and time. The analysis of such artefacts can therefore be conducted in other locations and in other times from the moment and location of creation and use. This is a great advantage for those wishing to study events without being there to witness them. However it is important to remember that any such study takes place without the active commentary of the creator and/or user of the artefact (Hodder 1994, Markham 2004).

As Hodder (1994, p 395) puts it: "There is often no possibility of interaction with spoken emic "insider" as opposed to etic "outsider" perspectives."

Even when such interaction is possible the motivation for why material traces appear to be the way they are sometimes inadequately explained. This may be explained in part by the theories of Argyris and Schön (1974). They argue that there is a distinction between an individual's espoused theory (what they claim) and their "theory-in-use" (what they actually do). People always behave consistently with their mental models (theories-in-use) even though they often do not act congruently with what they say (espoused theories).

Material traces are often left in online environments. These traces can be both voluntary and involuntary traces. Involuntary traces can be seen by those traces the user of online environments leaves without meaning or intending to. This does not mean that these traces are unwanted but only that they are unintended. The voluntary traces display themselves more clearly as communicative acts intended by the communicator to be received by either specified readers or groups of readers. Examples of these traces within the online environment can be seen in online threaded discussions and asynchronous discussion lists which remain online and available even after the communicator has gone offline.

Material traces add an important dimension to data collection and present important insights not provided by face-to-face empirical data. Material traces allow "new light to be shed on topics…and different facets of problems to be explored" (Bloor 1997, p 1). Analysis of these material traces serves as an important method in research. Material traces cannot be viewed as neutral instruments, whether produced intentionally or as a by-product of other behaviour all material traces should be understood to represent reflections of values and goals of the author[7]. MacDonald (2001, p 196) explains that: "Such creations may be regarded as 'documents' of a society or group which may be 'read', albeit in a metaphorical sense." Research relying on material traces should be capable of acknowledging that "documents which are intended to be read as objective statements of fact are also socially produced" (MacDonald 2001, p 196). It must be recognized that this material is must be understood in the context of its development and use:

> They are produced on the basis of certain ideas, theories or commonly accepted, taken-for-granted principles, which means that while they are perfectly correct –

[7] Author is a misnomer. The producer of material traces can be unaware of such production and therefore cannot be understood to be an author or creator in the traditional sense. The term is used here as a simplification.

> given certain socially accepted norms –they do not have the objectivity of, say, a measure of atmospheric pressure recorded on a barometer. (MacDonald 2001, p 196).

A large number of documents have been used in this work. Their format and origin represent the diversity of the areas being studied. The primary documentation spans from legislation to policy document to individual and standard contracts. These documents are presented in a wide variety of formats from traditional paper to digital online versions accessible via the Internet. The secondary documentation includes everything from first hand accounts and interpretations of action to reports, research and educational literature. Lincoln and Guba (1985) categorise documentary artefacts loosely as documents or records according to their purpose, whether they have been created for a formal transaction (records for example licenses, contracts and legislation) or if they have been formulated for more personal reasons (documents for example diaries and letters). This categorisation, however, lacks the documentation created for semi-formal purposes (for example letters of protest, web page defacements etc). They argue that the less formal documents are comparable to speech and require a more contextualised interpretation. Hodder (1994, p 396) writes that the distinction is important on the basis of power and technology where: "Documents involve a personal technology, and records a full state technology of power."

The designations of primary and secondary should not be understood to be a value judgement. The primary sources are those that reflect the position of the formal structures created by organisations (e.g. legislation or contracts) while the secondary sources to a much higher degree reflect the actions of actors within the formal structures. Naturally this classification into primary and secondary is not absolute. It is intended to help understand the nature of the documents not to be a goal in itself.

When working with documents the researcher must keep in mind that documentation does not represent an absolute or objective position. First it is necessary for the researcher to check the accuracy of the documents then the documents must be interpreted in light of "…the teller's interests, perspectives, and presuppositions" (Hammersley & Atkinson 1995, p 160). Primary documentation such as governmental policy and legislation reflect the interests, perspectives, and presuppositions of the state[8] while the

[8] Who is the state? What does it represent? This term cannot be defined adequately within the scope of this work.

secondary documentation can be said to represent the views of groups and individuals participating in the social debate from a position of less power, or at least less access to more established channels of communication.

To obtain an adequate understanding of the complex reality it is important that the researcher studies a large number of texts from a plurality of sources to attempt to establish an understanding of the meaning of the communication within its context. This plurality of sources provides a picture of general discourse.

Data Analysis

The law is not a natural phenomenon but it is a socially constructed institution. Among socially constructed phenomenon there exists objects that are by their nature more easily studied since they are created in one finite process. Buildings such as the Empire State building are constructed once. When the final stone is laid it is to a large extent finished. Once finished it can be measured and described. Other socially constructed phenomena are constantly being re-interpreted and are never completed. Once such area is regulation. However, the fact that regulation is continuously being constructed and reconstructed does not mean that it is impossible to take a snapshot of the process. Through this the researcher can explain the nature of regulation as defined by a certain point of its development in space and time. The work represented here is an exercise in describing the nature of regulation in present state of Internet technology and its implications upon participatory democracy.

Choice of methodology is not a matter of personal preference.[9] The goal with this work is to see the interaction between structure and actors depends upon an ability to gather data that will reflect the goals, intentions and aspirations of the structures and the actors. This data does not present itself easily by using one methodological approach. Therefore this work has gathered data from several sources, using multiple methods over different time periods. This empirical evidence presented in this work attempts, therefore to define both a situation in place and time together with the regulation taking place within that definition. To make matters more complicated the technological base of this study is extremely malleable since it is made up of software and interconnected computers. The challenge

[9] This is not to say that personal preferences do not play an important part in methodological consideration.

therefore is to present valid and reliable cases upon which an analysis can be based.

The validity of each case can be seen as the accuracy with which the data describes the social phenomenon (Hammersley 1990). To ensure validity of the cases in this work the descriptions of the social phenomenon come from various established sources. As far as can be ascertained much of the descriptive material comes from legal sources or sources which may be considered relatively unbiased. The goal with this is to avoid the pitfall of anecdotalism, a practice that Silverman (2005) describes as describing reality from a limited or biased number of sources. When describing less official activities[10] the material will be selected as to be so close to the source that it aims to describe. In addition to these methods, as far as possible, a triangulation (Silverman 2005) of sources will be made, so as not to rely on single sources of information. By using this approach and attempting to discuss the validity of unofficial sources the validity of the analysis presented herein will be enhanced.

Another issue, related to the once above, is the question of rigour. By basing this work on qualitative data the reliability or rigour of the results may be questioned. Often such mistakes are made by those attempting to judge the rigour of qualitative studies using rules developed to judge quantitative studies. While the quantitative approach to data collection is symbolised by conciseness and objectivity based upon ideals of statistical analysis. The use of rigour in qualitative research must focus on thoroughness in data collection, openness towards the data and theory and a declaration of sources.

To ensure sufficient rigour in the use of case studies the multiple approach has been taken. The multiple case study aggregates data collected from several sources at different times. This work is the result of the aggregation of six case studies collected over a four-year period. This approach provides a method for gathering data of interest for studying a large-scale reality, as is the case when studying the regulation of disruptive technology in relation to its democratic effects. The material gathered demonstrates the actions of the parties involved and enables an analysis of the interactions between the structures and actors (Giddens 1984).

[10] This should be understood to mean when representatives of structures discuss regulation informally or "off the record", for example in explanatory statements or private opinions etc.

Taken together this work therefore relies on the use of multiple methodologies and information sources. The data analysis, undertaken within the framework of this thesis was conducted as part of the research process and cannot be fixed to a specific time-period. Data analysis was conducted during the collection of empirical data for each case. This data was then additionally analysed and presented in the form of research articles, mainly in journals. A second round of analysis was naturally conducted during the compilation of this work. The latter process included both the addition of new data where appropriate due to new developments and the inclusion of feedback gathered from the responses to the publication of the individual studies.

Each study provided the researcher, not only with insights to the specific field, but also a greater understanding of the whole research field. This latter greater understanding was naturally applied to the following study and the results were again applied to the studies that followed in a fruitful development. This work therefore provides the opportunity not only to update with factual information but also to revisit preliminary studies with a new experience of the research field gained from the long-term work.

Method Summary

In table 5 below, *Trigger* refers to the event that identified the topic as an area worthy of research. The cases presented in chapters four and five (*Participation* and *Communication*) were both prompted by the publication of the Cybercrime Convention (2001). Once proposed this convention provoked intense discussions both on its content and on the manner in which it had been produced. Two areas that were of particular interest (for reasons presented in their respective chapters) were acts of civil disobedience online and virus writing and dissemination. The motivations for studying chapters six and seven (*Integrity* and *Property*) grew from a general discussion that was taking place at the time. The rise of interest in spyware may be attributed to its general growth and the awareness created by anti-spyware propagators and software manufacturers.

The rationale for chapter seven grew from the growth in game research and recent case law. The two final chapters eight and nine (*Access* and *Autonomy*) differ from the previous chapters since the researcher was able to follow in the growing political discussions, first in the protest against EU legislation against software patents (chapter eight) and then in the World Summit on the Information Society (chapter nine). Therefore the triggers from these final two chapters can be understood as current political developments.

Democratic Value	Empirical Focus	Trigger	Time	Research Activity	Empirical Material	Regulator
Participation	Online Disobedience	Cybercrime convention	2000-2002	Observation Interviews	Convention, National Regulation	Hierarchical
Communication	Virus	Cybercrime convention	2001-2002	Observation Discussions	Convention, National Regulation	Hierarchical Design
Integrity	Spyware	Rising awareness	2002-2003	Online forums Observation	Legislation, Courts, Contracts, Forums	Design Competition
Property	Online Environments	Caselaw, Rising awareness	1999-2003	Online forums & discussions Seminars	Licensing agreements, Courts, Legislation	Design Hierarchical
Access	Software	EU Software Patents directive	2003-2005	Active participation discussions Seminars	Proposed EU directive, Opposition documents	Design Community
Autonomy	Online Censorship	WSIS process	2004-2005	Discussion Workshops Forums	Technology evaluation, Literature, NGO documents	Design Hierarchical Community

Table 5: Research Progress

The heading *Time* in table five refers to the dates during which the main empirical work for this case was undertaken. It is important to point out that the dates imply only the main timeframe for empirical data collection and is not to be understood as finite dates. The studies can, in most cases, be seen as ongoing something which will be discussed in greater detail in the individual chapters. The label *Research Activity* refers to the main forms of activity that were undertaken in the process of collecting the empirical data during the main timeframe. This will be discussed in more detail in the respective chapters.

During the data collection process documentary output from the parties studied were collected and analysed as part of the research process. The label *Artefacts* in the table refers to the main types of objects studied. These artefacts, together with the other research activities were analysed in an attempt to compare the goals of the regulatory structures with their effects together with the actions and reactions of the actors affected by the regulation studied in this work. The label *Regulator* gives an indication of the modalities of regulation, which will be discussed in greater detail in their respective chapters.

4

Participation

Democracy is not something that you believe in, or something that you hang your hat on. It's something that you do, you participate. Without participation, democracy crumbles and fails.

Abbie Hoffman

Introduction

The Internet is used for every conceivable form of communication and it is therefore only natural that it should be used as an infrastructure for protest and civil disobedience. Special interest groups, such as environmentalists, have been among the early adopters of Internet technology for organisation and protest (Castells 2001, Meikle 2002, Pickerill 2003, Walch 1999). The technology brings with it the ability to carry out new forms of protest, in new environments and also involve changed consequences for those involved. These changes disrupt the way in which protests are traditionally carried out and provide new avenues of democratic discourse for those involved. The use of Internet technology for political purposes is in itself nothing special. The technological infrastructure, as mentioned earlier, does not discriminate content. Therefore, using Internet technology to conduct different forms of political protest is a use of technology that could have been easily anticipated.

The events that triggered research into this field follow online political activism and political repercussions during 2000 and 2001. During this period an active negotiation of the role of online political activism among the actors themselves and the reaction to such activism by the regulatory structure took place. This work takes its starting point from a discussion held, mainly online, in 2000 between two activist groups (*The Electrohippies* and *The Cult of the Dead Cow*) on the role of online activism and civil disobedience. Their common point of view was that both groups were actively involved in such activities and were attempting to negotiate the limits of permissible political activism online. This discussion was followed by the presentation of the Convention on Cybercrime[11] in 2001 that can be seen as a reaction of the regulatory structure. The Convention threatened to make many of the actions carried out by political activists online illegal with severe criminal penalties.

The Cybercrime Convention was developed by the Council of Europe, an organisation whose primary mission to strengthen democracy, human rights, and the rule of law, throughout its member states. Additionally it works to develop continent-wide agreements to standardise member countries' social and legal practices while promoting awareness of a European identity based on shared values and cutting across different cultures. At the time of writing the Council of Europe, which was established in 1949, consists of 49 member states.

The Cybercrime Convention reflects the goals and values of this organisation by stating in the preamble that a proper balance needs to be ensured between the interests of law enforcement and respect for fundamental human rights. However it is agreed that this balance has not been achieved and that the Convention is heavily biased towards meeting the needs of law enforcement (Akdeniz 2005). Following state ratifications, the Cybercrime Convention came into force in July 2004. The next stage in the process is the enactment into national law by the member states of the Council of Europe.

This chapter studies the use of technology regulation of online participation. This is carried out through an analysis of the activities of online political activists in relation to each other (as represented by the two groups) and to the regulatory structure (as represented by the Convention). The analysis is done by studying basic criteria found in tradition civil disobedience discourse and observing their applicability in online environments. *The purpose of this chapter is to better understand the political protest activities carried out online and to see whether traditional civil disobedience theory embraces these new forms of political activism.*

Participation is recognized as a core democratic value (Pateman 1970) however there are disputes about which form such participation can take

[11] Budapest, 23.XI.2001 (ETS No. 185)

(Månsson 2004, Vinthagen 2005). The use of Internet-based communications as an infrastructure for civil disobedience can be seen both as a development of online participation and as a threat to communication (Klang 2004a). To counter this threat there has been an increase in regulatory activity which has led to the discrimination of online participation. Internet-based civil disobedience is not treated as being functionally equivalent[12] to offline civil disobedience since the regulatory structure demands a higher degree of obedience in online environments as compared with offline environments.

Civil disobedience is a disputed concept. It is regularly seen both as undemocratic actions that threaten a democracy and as actions that further democracy (Waldman 1969, Månsson 2004).

It is beyond the scope of this work to attempt to resolve the Gordian knot of civil disobedience in participatory democracies. Therefore this work will limit itself to broadening our understanding of the way in which the regulation of technology regulates democracy. Therefore this chapter will focus on what civil disobedience is and to see if, and how, its practice and regulation differ in online environments.

Theory

Democracy may be seen as a system of self-rule where, in practice, the population of a society controls the government of that society. It is rule by the people. Therefore the concept of democratic government is that it serves the people as opposed to only ruling them (Pateman 1970, Harrison 1995). This is most commonly practiced in the form of a system of indirect representation whereby citizens are able, through a voting system, to choose who will form the government. Seen only in this light the participatory elements of democracy are weak and therefore many theorists show that the voting system is but one form of active participation in a democracy.

Other important elements within a democracy are all forms of communication and control between the government and the citizens (Pateman 1970). One form of communication within society is the regulation, law and policy decisions that make up the everyday regulatory structures within a society. When such examples of regulatory structures are created by the citizen's ruling representatives the default position within democratic theory is that such regulations must be obeyed (Rawls 1963).

[12] See *Theoretical Focus* page 38 *et seq.*

Political participation within a democracy can entail not obeying the structural regulations. As we shall see, actively opposing the rules created within a democratic society is a legitimate form of political participation.

Disobedience is not a behaviour that is encouraged. Despite this, there are many situations where disobedience is praised as a virtue and obedience is punished. An example of the former can be seen in the American civil rights movement. While, an example of the latter can be seen in the German attempts to come to terms with its history. Following the fall of the Berlin Wall, East German border guards have been charged with manslaughter or attempted manslaughter for shooting individuals attempting to defect (Quint 2000). Our relationship to social and legal rules is therefore not as clear and simple as we would like it to be. We praise the actions of those who have undertaken the classical acts of civil disobedience while we attempt to prevent, limit and punish those who would disobey today.

Civil disobedience can be defined as: disobeying the law for a good cause. The reason why this may be a simplistic definition is that the good cause is a very elusive. The political and philosophical traditions of disobedience arise from the actions of Thoreau's refusal to pay poll tax in protest of the federal government's war in Mexico, support of chattel slavery and the violation of the rights of the native Indians. His action was based on his perceived right and obligation to follow his conscience. Thoreau (1993 [1849]) writes that he would not support a government that carries out wrongful acts. While this refusal to be a party to wrongful acts may be an admirable trait; it is not an active attempt to stem injustice, rather a method of keeping ones own hands clean (Singer 1973).

A more precise definition on civil disobedience has been formulated by Bedau (1961) who described it as a public, non-violent political act contrary to law and carried out with the aim of bringing about change in law or policy. Later Bedau (1991) would broaden his definition to refer to illegal acts, "committed openly…non-violently…and conscientiously…within the framework of the rule of law…with the intention of frustrating or protesting some law, policy or decision…of the government." While these definitions are an important basis for further discussion it is important to remember that definitions in this area are to a certain extent arbitrary and therefore it is not the role of the definition to control what disobedience is but rather form the basis for attempting to arrive at a consensus on what disobedience may be.

The developments of civil disobedience are strongly connected with both Tolstoy's writings on pacifist non-resistance (rather die than kill) and

Gandhi's less ideologically clear but more proactive non-violence (Vinthagen 2005). In their most clear form the concepts of practical civil disobedience can be seen in the actions and writings of King (1991 [1963]). In his struggle we see the whole span of possible reactions to the law. From the strictest views that even unjust laws are to be obeyed to the moral obligation to reject immoral laws.

Therefore one can sum up the situation that there is an *a priori* obligation to obey the law. However, this rule may come into direct conflict with moral obligations and have the ability to cause more harm. Or the duty to obey may be overridden in certain cases by other more stringent obligations (Rawls 1963). There are however objections to this view (Suber 1999). These objections claim that there cannot be any form of civil disobedience in a democratic state since the injustice is created in a "just environment" and can therefore be changed by democratic means – thus removing any need for disobedience. Much of civil disobedience has been carried out in democratic environments there is no requirement that disobedience be carried out only in a non-democratic environment. Additionally the use of democratic channels to correct an unjust situation may in itself create a situation which perpetuates the injustice since there are, in theory, no limits to democratic means of action. In a democratic society a minority may be particularly burdened by legislation despite that the majority feels the situation to be equitable. It is important to make the distinction that while the state may be democratic; it does not necessary follow that all the practices therein are just. Singer (1973) has defined the process of disobedience as one method for a minority to appeal to the majority to reconsider an injustice. The need for disobedience in such an appeal is necessary when the democratic process itself prolongs the injustice. Disobedience is therefore not intolerance towards the system but the view that the democratic process being allowed to run its course perpetuates the injustice. King (1991 [1963]) goes further and states that there is an obligation to disobey in the situation where the law is unjust:

> For years now I have heard the word 'Wait!'…We must come to see…that 'justice too long delayed is justice denied.'…One may well ask, 'How can you advocate breaking some laws and obeying others?' The answer is found in the fact that there are two types of laws: just and unjust...One has not only a legal but a moral responsibility to obey just laws. Conversely, one has a moral responsibility to disobey unjust laws. (p 72).

A final issue is the problem of how we can accept the disobedience of a certain group and not another? This type of argument is often referred to as the slippery slope (Volokh 2003). The fundamental idea is that we cannot allow any disobedience since the moment we accept any form of disobedience we will rapidly progress to the bottom of the slope and be required to accept all disobedience. Those who argue that the slippery slope will lead us to anarchy would prefer that no disobedience be allowed. This is a simple solution which provides us with an easily remembered rule. However the problem of disobedience is already complex and attempting to simplify it with absolute rules is not an equitable solution.

If we are to agree that there may be, in certain cases, morally justified disobedience then how shall these be motivated? To understand this we must look at four criteria: disobedience, civil, non-violence and justification. These criteria must be analysed and reinterpreted for application in the digital environment. These criteria have been chosen for their central role in discussions of disobedience but are not universally known as the only criteria worthy of discussion.

Disobedience: This is arguably the most important criteria since without this there is no discussion. A tolerance for disobedience is important in a civil society but to accept disobedience is not an option since disobedience by its nature cannot be permitted. Disobedience stems from the conscious desire to protest a law which conflicts with "more stringent obligations" (Rawls 1999). To comply, even with silent disapproval, does not constitute disobedience. To comply, after voicing disapproval, is laudable but not disobedience.

Civil: Disobedience brings with it unattractive consequences such as legal and social reactions and therefore there is a strong urge to hide ones disobedience. However it is important to remember that the publication of the disobedience is a necessary component of the actions and provide a greater degree of legitimacy (King 1991, Rawls 1999, Singer 1973). In situations where there is risk of great personal harm it is understandable that the disobedience does not take place publicly, however, civil disobedience generally has a role of public enlightenment (Bedau 1991).

Non-violence: Due in part to its traditions, there is a misconception that equates civil disobedience with non-violent action. Violence on its own does not invalidate an action from being civil disobedience. However, it is important to note that the use of violence in civil disobedience has been shown to take the focus off the message of protest and creates a lack of sympathy towards those who use it. Violence is in itself not static and there are different levels of violence which may be implemented. Violence can be seen from the prevention of others enjoyment of their private property (such as the sit-in), the defacement or destruction of property across to the more extreme causing of bodily harm to others. In practice and in literature there is no acceptance, within the civil disobedience discourse, in the causing of physical harm to others. However often theoreticians allow for the prerequisite of non-violence not to include violence to property (Månsson 2004). Therefore civil disobedience can include a level of coercion or harm but stops short of violence to others.

Justification: The classic justification of civil disobedience lies in a conflict of law with moral principle. Rawls (1999) is quite firm on this point, claiming that the protester must appeal to shared principles existing in the morality of the general public. Singer (1973) finds the qualification of shared values too limiting since the protester must appeal to a pre-existing norm. Another point of disagreement between Rawls and Singer is the question of the acceptance of punishment. While it naturally shows a great moral courage to be prepared to accept the punishment which stems from ones political acts – attempts to evade punishment on its own does not make the act less of civil disobedience. This is particularly true if the punishment is unduly harsh.

The discussion of whether there is a duty to obey the law is rarely taken to this extreme. However, the question of whether there is a duty of obedience towards the law and the state is an active one, since the question of when disobedience is valid remains. Practitioners of civil disobedience tend to justify their actions by pointing to the fact that they are fighting a larger injustice and in this role they have the right, some would even claim the duty, to break the law. Therefore the disobedients are doing what they believe to be morally right despite the fact that their actions unfortunately come into conflict with the enforced rules.

The modern historical developments of civil disobedience begin with the work of Gandhi. Spurred on by the success of Gandhi's approach to non-violent resistance, the methodology was adopted by King in his successful campaign to bring an end to racial segregation laws. The concept of disobedience as conceived by Gandhi and developed by King was to draw attention to the injustice and in this manner to commence a political discussion which would lead to the creation of more just society which is the purpose of civil disobedience (Rawls 1999). For many, the use of Internet-based civil disobedience was inevitable. The earliest formal connections seem to be made as early as 1996, when the Critical Art Ensemble (1996) published a book containing a chapter on the topic of Electronic Civil Disobedience.

Analysis: Actors

In its simplest form civil disobedience involves defying the law for a good cause. It is therefore essentially a conflict between the law and the morality. The purpose of this section is to look at the use of civil disobedience in online environments to understand what civil disobedience is, and how it is implemented, as a political force in the online domain. This study will look at three online activities described, by the perpetrators, as acts of civil disobedience. These three acts are: email bombing, web defacement and denial of service.

Email bombing: A number of organisations (Pickerill 2003, Klang 2004a, Cardoso & Pereira Neto 2004) encourage members of the public to use email as a form of protest. This can either take the form of sending a mass of emails intended to disrupt the receivers normal email use or it can be used to send messages of protest to key individuals. These two methods can also be combined. In certain cases all that is provided is the email address and a suggested text that can be copied into the body of the email. In other cases the system is automated that all an interested protester need do is to click on an icon. Examples of organisations, which have used email in the latter form expressed above, are Amnesty International, Greenpeace and Friends of the Earth (Klang 2004a).

Webpage defacement: Originally a hacker was a term used for a good programmer but today this definition has been overshadowed by the definition of the hacker as a person who attempts to gain unauthorised access to a computer or computerised system and the information it contains. Simplistic and one-sided media discourses on technology are common (Kling *et al* 2005) and hacking is an excellent example of this. The discourse has been very much focused on the vulnerability involved in connecting an organisation to the Internet and on the dangers represented by hackers (Taylor 1999). There is also a strong connection between the idea of the good or white-hat hacker, electronic civil disobedience and the development of hacktivism (Klang 2005a). However, while the act of hacking, or the gaining of illegal access, is in many cases both illegal (Klang 2005a) and not uncontroversial (Kerr 2003) it is usually the means, and not the goal, of an act of civil disobedience. This is not to say that those who carry out online civil disobedience are not considered to be hackers, by themselves or others (NIPC 2001), but rather that the act of hacking is only part of the act of disobedience since it is a necessary component of webpage defacement.

Webpage defacement entails gaining unauthorised access to a server and making modifications to the webpage. These modifications involve the addition of messages with or without the removal of the original data. Political webpage defacement can be carried out either to effect a political decision, such as an election. This was done in 1998 in Sweden, when on the eve of the Swedish general election the home page of the right wing opposition party was hacked. The page was altered and links to political and party information were replaced with links to pornography sites and to the left wing party. Defacement can also be carried out to protest government policy. This can be seen in the action carried out in April 2003, when the web page of the Irish Aviation Authority (http://www.iaa.ie) was hacked. The front page was replaced with the text containing the message "The people of Ireland demand that the Irish Government deny access to Shannon Airport to the U.S. military…The Irish people are told they live in a democratic, neutral country. Where is the democracy in the Irish government deciding without the vote of the people, that U.S. murderers have access to Shannon Airport?" The hacker also included information that "Nothing has Been Deleted" therefore no information was lost by the Irish Aviation Authority (Klang 2004a).

Webpage defacements often tend to follow patterns of real world politics. Targets often follow areas of tension such as Pakistan and India or Israel and Palestine or individual events such as the bombing in Bali, which was followed by attacks from Indonesia and Malaysia against South Asian targets. Among the more notorious long-term use of defacement as a political weapon are the actions of Indian and Pakistani hackers, their actions are motivated by the tensions in over the disputed Kashmir territory. In his article Srijith (2002) studies over 700 documented Indian webpage defacements occurring during a period of 20 months. He points out that generally most defacement attacks peak after security flaws are announced but he also notes that the trends in India do not mirror this worldwide trend. According to Srijith the defacement in India is more politically motivated with the most prolific attackers of Indian web pages originating from Pakistan. This claim is further corroborated by the anti-Indian propaganda left on the defaced pages.

Denial of Service: The denial of service (DoS) attack is usually described as an incident which prevents a legitimate user or organisation from accessing a systems resource or the delaying of systems operations and functions (Biegel 2001, Gibson 2002). The incidents or attacks can be related to a specific network service such as email, or to the domain name of the target.

Attacking the domain name has the added advantage for the attacker of tending to diminish all the victim's online functions since the domain name cannot be resolved. This means legitimate users attempting to access a web-based service are unable to connect to the server since the server is busy responding to false requests for information. This is due to the fact the server under attack is busy responding to its attackers' requests and is unable to reply to legitimate users' requests. The legitimate user, unaware of the ongoing attack, will only receive an error message from her browser that the server is unavailable.

Traditionally, the distributed DoS attack entailed the co-ordination of traffic to a designated website; this first required the marshalling of many protesters to be prepared at their computers to send information at a given time to a specific target. These attacks were complex affairs, and required a great deal of social cohesion and organisation amongst the protesters, who sat alone in front of their computers with only the virtual presence of others. To overcome some of these organisational problems, co-ordinating software may be used by protestors. Such attacks are known as co-ordinated point-to-point DoS attacks. In these kinds of attacks the attackers may use software with the same effects as that used in the point-to-point DoS attacks. Naturally, the more users and the more sophisticated the software, the more efficient the attack. The important issue with this type of attack is that it still requires a user to be involved in the attack, and to be efficient it requires the gathering of a large group of people who have the time, technology and will to carry out the attack.

While there are different forms DoS attacks, such as TCP SYN flooding, ICMP flooding, UDP flooding and ping of death, the most common is TCP SYN flooding. These types of attacks that still involve the physical intervention of the user have sometimes been called client-side DoS, to differentiate them from server-side DoS. While the client-side DoS requires the active participation of many like-minded individuals, the server-side DoS has no such requirement. To be effective the serverside DoS attack requires only one individual and the creation of an army of zombies . In this context a zombie is a computer containing a hidden software program that enables the machine to be controlled remotely (Gibson 2002). For the purpose of the DoS this remote control of other people's computers is done with the intent of attacking a specific victim server.

The most efficient method of introducing software into other people's computers with the capability of taking control of them at a specified date is either by hacking into the computer and installing the software directly, spreading the program in the form of a virus, or including the code within a piece of desirable software which the user will download and install himself. Two well publicised examples of server-side DoS attacks are the Mafiaboy attack, where a 15 year-old known only as Mafiaboy successfully attacked websites operated by Yahoo, eBay and Amazon.com (Klang 2004a), and the 13 year-old who used a DoS attack to take down a California-based computer security site (Gibson 2002).

The advantage of using zombies to carry out the attack on a server is that the attacker does not need to disadvantage himself by persuading and co-ordinating other users in participating in the attack. There is an added advantage of increased anonymity, since the attacker's machine is not directly involved in the DoS attack but acts only via its unwitting intermediaries – the zombies. With adequate time and effort in preparation the number of zombies created can be sufficient to create havoc with even the most sophisticated of servers. Naturally, the more time spent in preparation, the more likely it is that the plans will be uncovered prior to the attack and defences be created which will limit the effects of the attack.

The Activist Debate

When attempting to comprehend the driving forces behind the hacker, it is important to look beyond our own media imposed images. In his research into hacker culture, Taylor (1999) identifies six main driving forces that motivate hackers (addiction, curiosity, boredom, power, peer recognition and opposition); within the section on peer recognition, Taylor includes politically motivated actions. The book is an excellent starting point for those wishing to understand the hacker; however, it is important to recognise that it is based upon research carried out prior to the growth of online activism. Today, any serious work on hackers should recognise the effects of a larger group of politically motivated online activists if it is to be considered to be complete.

The actions of DoS attackers are, or are rapidly becoming, illegal. The question that therefore needs to be addressed is what it is that drives these people to carry out such actions. If they are merely criminals, then we need hardly proceed any further. The question is whether there can be any legitimacy in their actions. In order to explore this further, we must take a closer look at the motives underpinning online activists. This is not as simple as it may sound, since the current legal environment does not promote the development of an open dialogue between attacker and society.

A group of activists dedicated against the trend of clandestine action is the Electrohippie Collective. This group uses client-side DoS as a protest method and it does so in an open manner. They write:

> …we do not try to bury our identities from law enforcement authorities; any authority could, if it chose to, track us down in a few hours. However, because some of us work in the IT industry, we do not make our general membership known because this would endanger our livelihoods. (Electrohippies 2000).

Furthermore, the group has taken pains to publish its views in a series of publications available online.

In an attempt to create a dialogue on the subject of the use of DoS as a political activism tool, the Electrohippies have employed the sit-in as a metaphor and they term their attacks virtual sit-ins. Since they use the client-side method they do not employ zombie machines, and without zombies their actions must be supported by those willing to carry them out. One of their claims of legitimacy is that they have the popular support of the protesters: "Our method has built within it the guarantee of democratic accountability. If people don't vote with their modems (rather than voting with their feet) the action would be an abject failure." (Electrohippies 2000).

Since they are dependent upon popular support, in order to have any effect their actions must be deemed worthy of support by the protesting individuals. To obtain this support, the collective established four principles that govern any action they undertake. The principles are proportionality, speech deficits, openness and accountability. Proportionality refers to the insight that it is not acceptable to disrupt communications without justification; the attack itself must not be the focus. The tactic is a means and not an end: it brings publicity to an event that is the focus of the action. As an example, the Electrohippies (2000) cite their actions against the World Trade Organisation, which coincided with the offline protests in Seattle. The action can only be legitimate if a speech deficit exists, i.e. a lack of equality between the actors within the public discourse. The attack must therefore be used to draw attention to this inequality and is not in itself the intended goal. The principles of openness and accountability refer to the legitimacy of the attack, since without these it would be difficult to argue that the ultimate goal is an open discourse.

The early attacks of the Electrohippies in February 2000 were aimed at protesting against the commercialisation of the Internet and therefore they protested the presence and influence of online actors involved in electronic commerce. The focus of this protest and the motivation and political material presented online (Electrohippies 2000) caused another activist group to respond:

> This is the first and most egregious error that the Electrohippies make. It betrays their lack of understanding of hacker culture; it also creates a false bridge to their own anticorporate bias…It was irrelevant that the targeted sites were commercial and had e-commerce components. They could just have easily have been the Vatican, a Britney Spears fan site, or Aunt Beuears fan site, or Aunt Beulahs Jam page, that is, if those sites represented the same level of prestige and notoriety as the actual targets. (Ruffin 2000).

Ruffin is a spokesperson for the hacker group known as the Cult of the Dead Cow, which claims to be involved in online political activism and is therefore opposed to any frivolous use of the Internet as a tool of political protest if such use can have negative effects on other activists. They argue that using the Internet to protest electronic commerce actors is not a legitimate form of civil disobedience (Ruffin 2000) and they also posit that the functional equivalency approach to online/offline activities[13] is not adequate.

The Electrohippies further compound their misunderstanding of the Internet by assuming that the same rules hold in the digital realm as they do down on the street. They do not. Where a large physical mass is the currency of protest on the street, or at the ballot box, it is an irrelevancy on the Internet. (Ruffin 2000).

The Cult of the Dead Cow are more focused upon technology than the importance of popular political participation and they state this clearly when they argue for the importance of technology over people in political online activism with the words "Programs make a difference, not people" (Ruffin 2000). They address the problem of the democratic participation of the concerned minority (Singer 1973) by maintaining

> …if numbers lend legitimacy - as the Electrohippies propose - then the lone bomber who tried to assassinate Hitler in his bunker was wrong and the millions who supported the dictator were right. (Ruffin 2000).

Ruffin (2000) further argues that since DoS attacks are a violation of people's freedom of expression and assembly, "No rationale, even in the service of the highest ideals, makes them anything other than what they are – illegal, unethical, and uncivil" (Ruffin 2000). The Electrohippies are aware of the paradox of using DoS attacks for the purpose of promoting open and free speech since they are curtailing the speech of others, but they maintain

[13] See *Theoretical Focus* page 38 *et seq.*

that their actions are justified if their principles are adhered to (Electrohippies 2000). In March 2003, virtual sit-ins organised by the Electrohippies against the war in Iraq managed to disrupt the Prime Minister's website (www.number-10.gov.uk), causing it to be unavailable on several occasions. In response to criticism, they argued that their actions did not prevent any communications between the allies but were intended to show the use of official websites as a part of the propaganda directed at

> …seeking to sanitise their violation of International human rights law. Action by the Collective is therefore valid in order to highlight their violation of fundamental rights by a method that seeks to restrict their misuse of the right to freedom of expression under the UN Universal Declaration. (Electohippies 2003).

In terms of public education the group publishes its views on both their politics and their method of protest in a series of publications available freely online. This is an attempt to create a dialogue on the subject of the use of DoS as a political activism tool they have employed the sit-in as a metaphor and they term their attacks as virtual sit-ins. "Our method has built within it the guarantee of democratic accountability. If people don't vote with their modems (rather than voting with their feet) the action would be an abject failure" (Electrohippies 2000).

As we can see from the presentation above the Internet has become a de facto base for civil disobedience. While the actors themselves are attempting to come to terms with acceptable forms for the online disobedience none of the actors would deny that the Internet is an important tool for political protest. Offline political protest is a not uncontroversial method that has both supporters and critics. The same can be said of online political protests. The different groups are prone to argue methodologies and legitimate protest goals but these disagreements should in no way be understood to mean that the Internet is considered to be an unsuitable tool for online civil disobedience.

Analysis: Structures

It is important to observe that in the discourse on online activism today one of the terms being used with alarming regularity is cyberterrorism (Denning 2000). When invoking the spectre of terrorism it is important to remember that today the relevance of the correct label in this case is far from academic. If the act of online political activism is seen to be disobedience the courts may show tolerance, if it is seen to be criminal the courts will punish it, but if it is seen as terrorism then society will neither tolerate the actions nor forgive the proponents.

From the point of view of the activists the main question is one of obtaining the correct degree of disobedience. However from the point of view of the regulatory structure the activists' discussion is irrelevant since all the actions described above constitute illegal acts in most jurisdictions. The regulatory trend is moving towards an increased level of criminalisation of any activities similar to the ones described within this chapter.

The three forms of online civil disobedience described in this chapter (email bombing, web page defacement and DoS) tend to fall into three different areas of criminal activities. While the exact mode and form of regulation differs between jurisdictions there are areas of wide consensus in the approach to the suppression of such acts in online environments.

Email bombing is the most difficult act to regulate since the individual act of sending an email cannot be easily criminalised without encroaching on the legitimate use of email. If the attack originates from a single source the sending of massive amounts of email has yet to be criminalised in jurisdictions such as the UK, USA and Sweden. However this act is being redefined as DoS (more on this below). In a recent case in the UK where an individual bombarded an ex-employers email server causing it to crash explained, that since the email server was set up to receive email – sending email could not be a criminal offence. "In this case the individual emails caused to be sent each caused a modification which was in each case an 'authorised' modification. Although they were sent in bulk resulting in the overwhelming of the server, the effect on the server is not a modification addressed by section 3 [of the CMA]"[14]. This case is under appeal. Similar approaches can be found in the USA and in Sweden. While this is not a criminal act the injured party may still sue for damages under all three legal systems.

The activity becomes even more complex if the emails do not originate from the same sender. This is a traditional modus operandi of Amnesty whose letter writing campaigns consist of asking people to copy and send physical letters to government officials in countries who are failing to respect human rights (Power 2002). This method has been modernised and activists can now even send emails. While this will not fall afoul of

[14] District Judge Kenneth Grant sitting in the Wimbledon Youth Court on 2 November 2005.

Computer Misuse legislation recent legislation is being implemented to prevent SPAM which in addition to preventing SPAM also provides the means for the criminalisation of this activity. This use of email has however recently been made illegal within the European Union through the *Directive* (2002/58/EC) *on privacy and electronic communications* which has been implemented in the United Kingdom through *The Privacy and Electronic Communications (EC Directive) Regulations*. This regulation criminalises "the transmission of unsolicited communications by means of electronic mail to individual subscribers…a person shall neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of electronic mail…" (Article 22).

Due to the wording of this regulation it is interesting to ascertain whether a political protest message can fall under the definition of "communication for the purposes of direct marketing". The legal definition of direct marketing in the United Kingdom can be found in the Information Commissioners (2003) Guidance to the Privacy and Electronic Communications (EC Directive) Regulations 2003 - Part 1: Marketing by Electronic Means which begins by stating that the *Data Protection Act* (DPA) defines direct marketing as "the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals." The Guidance explains that the term direct marketing covers

> …a wide range of activities which will apply not just to the offer for sale of goods or services, but also to the promotion of an organisation's aims and ideals. This would include a charity or a political party making an appeal for funds or support and, for example, an organisation whose campaign is designed to encourage individuals to write to their MP [Member of Parliament] on a particular matter or to attend a public meeting or rally. (p 3).

This definition therefore covers any use by an organisation wishing to market either there ideas or any direct actions which they are planning to undertake to any individuals who have not, in advance, accepted that they are prepared to receive email from the organisation.

The legal position on web page defacement is the most clear since the defacement entails both entering into the server without permission and then changing the information stored therein. This is easily prohibited by the traditional offline laws of trespass and criminal damage. However there is a move to 'upgrade' the action of web page defacement from criminal trespass and compare it to an act of terrorism. Political activists who use this tactic want to equate defacement with traditional protest comparable to hanging a protest sign on a building owned by a corporation against whom the protest is aimed. These are tactics very familiar in the offline world. However since the online world contains no street corners or public spaces such analogies become difficult to make. Despite this the move to apply stricter sanctions to this online behaviour has awoken concern among civil liberties groups. An example of this can be seen in the letter addressed to Governor Pataki sent by the two civil liberties groups: Center for Democracy and Technology and the Electronic Freedom Frontier (CDT & EFF 2003). In the letter protesting a bill passed through the New York Senate they write:

> This bill is not effective cyberterrorism legislation. It does not distinguish between those engaging in petty crimes, and those whose aims are to seriously damage a computer network in order to cause physical harm to civilians, severe economic hardship, or the crippling of critical infrastructures. CDT and EFF believe that these complex issues deserve careful review and public hearings before legislation is enacted. We encourage the State of New York to combat cyberterrorism, but not to brand as "terrorists" those who commit minor illegal acts in cyberspace, just as those who commit civil disobedience offline are not punished as terrorists.

With legislation such as the Cybercrime convention (see more below) states are encouraged to view traditionally nuisance actions (trespass and defacement) as being comparable to serious criminal acts such as terrorism.

The legal position on Denial of Service is reasonably straightforward. The United Kingdom Computer Misuse Act (CMA) 1990 provides no remedy against DoS attacks. It creates three offences: unauthorised access to computer material, unauthorised modification of such material, and unauthorised access with intent to commit or facilitate commission of further offences. This means that the CMA can only be applied in server-side DoS attacks since these attacks require the use of zombies. The UK realised that legislation in this area needed to take technological developments into account, and in May 2002 an amendment to the CMA was introduced to the House of Lords, which inter alia dealt with DoS attacks. It defined what DoS is, and the terms under which a DoS action is a criminal offence. The amendment also included changes to ensure that a person could be prosecuted for a DoS attack where proof of the action was available within the jurisdiction of the United Kingdom. However, the Bill was never passed. Legislation which can be used against DoS attacks includes the Terrorism Act 2000, which defines terrorism in this context as the use or threat of action which is designed to seriously interfere with or seriously disrupt an electronic system for the purpose of advancing a political, religious or ideological cause.

Internet-based crime led to calls for harmonisation of the substantive and procedural security laws of EU Member States, and for the UK to ratify the European Cybercrime Convention and the European Commission's proposal for a Council Framework Decision on attacks against information systems.[15] Article 4 of this Decision deals directly with the criminalisation of DoS attacks.

These developments have had the effect of criminalising DoS attacks. Additionally, the Convention on Cybercrime reinforces the legal position that these acts are criminal offences or should be criminalised, leaving little room for interpretation of DoS as a tool of protest. In the case of DoS attacks, actions which hinder the functioning of a computer system by suppressing computer data are criminsalised by Article 5 of the Convention. Despite the increase in legislation in this area, several issues of legal interpretation remain unresolved (Kerr 2003) and this creates an unsatisfactory position vis-à-vis the predictability of the law.

In a recent decision[16] (May 22, 2006) the First Penal Senate of the Higher Regional Court of Frankfurt has overruled a decision of the first-instance court of Frankfurt in favour of a group of online civil disobedients. Two groups, "Libertad" and "Kein Mensch ist illegal" (No one is illegal), carried out an online denial of service demonstration in June 2001. The motive for the demonstration was to protest Lufthansa's participation in deportation of immigrants. The court found that the demonstration was not a show of force but was intended to influence public opinion. This interpretation had the effect of freeing the participants from charges of coercion.

While this Lufthansa-decision can be interpreted as an important change in regulatory direction but it remains much too early to draw such conclusions.

Discussion

There is a *prima facie* moral duty of the individual to follow the law. For most, this duty to obey the law is based upon the belief that without this obedience either the state would be unable to function or without total

[15] COM (2002) 173 final. Adopted in April 2002, it provides a general framework to approximate and increase judicial and police co-operation in relation to attacks against information systems. Member States had until 31 December 2003 to implement the proposed framework.

[16] 1 Ss 319/05.

obedience some would gain unfair advantages however this position is not unchallenged (Raz 1999).

It is interesting to note that the four criteria of civil disobedience discussed above have been developed in a pre-Internet environment and the question is whether they can be applied to disobedience in an online environment. If the criteria can be transferred into a digital environment then there is no reason why the use of digital technology as a form of protest should not be viewed as being functionally equivalent to other means of protest and be respected as such. If the four criteria do no transfer into the digital environment the question then becomes whether the online actions can be seen as legitimate forms of civil disobedience and therefore the theoretical basis of civil disobedience should be adjusted to fit the reality of the day. Alternatively the acts are merely illegal and have no moral justification as forms of protest.

Probably the easiest criterion to fulfil is the question of legality. The actions mentioned in this chapter are illegal, or rapidly being criminalised in most jurisdictions. The act of criminalisation is taking place both in national legislation such as the CMA of the United Kingdom or the American PATRIOT Act and in regional developments such as EU directives and the Convention on Cybercrime.[17] This move towards criminalisation has not only involved the loss of civil liberties in general but also brings with it an additional threat. This threat is the comparison of cyber crimes with terrorism which create a more serious environment for the perpetrator of such acts (Klang 2004a, Manion & Goodrum 1999). Civil disobedience will always remain an illegal act since, in part, making it legal would remove the concept of disobedience but it is important to consider the way in which the regulator views such acts. By attempting to classify acts which do little damage as terrorist acts not only limits the ability of groups to actively voice alternative opinions within the participatory democracy but also belittles real acts of terrorism and their victims.

Online disobedience gives rise to many questions in relation to the term civil. Even if we accept that the actions are carried out to create publicity and to educate the general public it is interesting to note that online civil disobedience has been carried out in two untraditional circumstances. Firstly the attacks need not be directed only at state actors but even larger multinational corporations have been effected by disobedience. Secondly

[17] The Lufthansa-decision mentioned earlier may be a break in this trend but it remains too early to draw any such conclusions from this single case.

the disobedience is not only limited to citizens within the state they are protesting. These circumstances have the effect that the actions fall outside the broader definition of civil disobedience put forward by Bedau (1970).

Taken together online disobedience offers the disobedient party the ability to carry out activities which hamper the lawful activities of a private actor in another country. This raises questions of legitimacy since the attacked party may be following the law and morality of the culture were business is carried out. Additionally those carrying out the disobedience are not personally effected by the action of the attacked party and therefore must rely on a secondary right. They are acting in the name of the injustice carried out against others. At first glance this may weaken the legitimacy of the disobedience.

The main complaint concerning violence in relation to online civil disobedience activities is in relation to the limitation of user's enjoyment of their property. In situations where webpage defacement, DoS attacks, mail bombing or unsolicited mail are used as tactics of civil disobedience they tend to impair the users (or the websites customers) legitimate use of property. Personal violence or physical harm can be caused if, for example, a user is dependent upon a website for information however, to this author's knowledge; no such cases have been reported. Damage to property in during these attacks is not necessary and even in the case of DoS attacks the web pages or services have been disrupted only for brief periods.

If we are to see justification as containing an acceptance of punishment (but not necessarily a masochistic search for one) and the active presentation of ones ideas, subjecting oneself to the evaluation of society, we can then evaluate these criteria by an example. The electrohippie collective use client-side DoS as a protest method and also maintains an open dialogue "…we do not try bury our identities from law enforcement authorities any authority could, if it chose to, track us down in a few hours. However, because some of us work in the IT industry, we do not make our general membership known because this would endanger our livelihoods" (Electrohippies 2000). They do not hide themselves or their actions but at the same time they do not advertise their identities. While the Rawlsian approach to disobedience may disapprove of their method, Singer (1973) seems to sympathise.

Discourse Control

In the press conference presenting the Commission's proposal for a Framework Decision on attacks against information systems, the

Commissioners created clear links between DoS and terrorism (Klang 2004a). Since September 11, 2001, as we have seen, discourse on the response to terrorism has become increasingly harsh. This has led to greater calls for the criminalisation of DoS attacks with little attention being paid to their role as a method of peaceful democratic protest. It is often pointed out that freedom of expression is the foundation upon which any democracy stands, since without the ability to freely spread and collect ideas there cannot be a functioning democracy. Naturally, even this right must be balanced so as not to seriously hamper the rights of others.

In the physical world we tolerate (to a varying degree) our lives being occasionally disrupted. Environmentalists hang banners across privately owned buildings, animal rights protesters may hamper our ability to enter fast food restaurants; anti-war demonstrators may hinder our ability to travel through city centres as we normally do. At times this toleration depends upon the fact that actions offline are conducted in the public sphere or on common ground as opposed to private property.

Our daily lives are also hampered by jubilant rugby supporters cheering the homecoming team, crowds viewing royal pageants, or roadblocks and diversions set up to protect visiting politicians. Around the world on New Year's Eve there is mass disobedience in the streets as the New Year is ushered in. These events are tolerated by society since they are deemed important to society. Most protesters believe in the importance of their actions. To the rest of society, these actions are mere annoyances. Despite this, such annoyances are important since they are the voice of dissent, and it is only through the growth of dissent into mainstream thought that societal development can take place.

Therefore the actions of protesters in city centres are tolerated or endured even by those who do not share their cause. We have come to understand the street or public space as the venue of manifesting public dissent. The problem with the Internet is that there is no such space. Everything done online is dependent upon privately owned equipment. The lack of public space is a serious weakness in developing both online rights and a genuine public sphere for online environments. Through the lack of public online spheres the Internet is seriously hampered as a place of political discourse.

Despite the fact that we today feel that the causes people such as King and Gandhi fought for were just and their methodology is seen as being worthy of our admiration, this does not mean that civil disobedience is commonplace and acceptable in society. The goals and methods of civil disobedients in the past are always easier to accept than the goals of those protesting against the status quo today.

On the surface it would seem that society cannot create a right of civil disobedience since there can be no permission to disobey. Those who fear civil disobedience see a state of anarchy where individuals disobey rules on a whim. Fear of this anarchy maintains the status quo: a belief in the ideals of civil disobedience, a respect in the past practitioners, but no desire to create a toleration of disobedience.

A common position adopted by those who oppose disobedience is that civil disobedience has no place in a democratic society. This argument is based upon the belief that democracy is the ultimate form of self-rule, which allows the greatest amount of input from the individual on the rule of law (Harrison 1995). Therefore, disobedience against the system is not the answer since the system itself is meant to be self-correcting and inequalities can be changed from within. It is important to make the distinction that while the state may be democratic, it does not necessarily follow that all practices therein are just. To be able to redress an injustice within this system, those who are affected by it must appeal for change. This appeal is the process of bringing the injustice under the gaze of those who have the ability to create change. Singer has defined the process of disobedience as one method for a minority to appeal to the majority to reconsider an injustice (Singer 1993). The need for disobedience in such an appeal is necessary when the democratic process itself prolongs the injustice. Disobedience is therefore not intolerance towards the system but the view that allowing the democratic process to run its course perpetuates the injustice.

The fear is that the legitimate actions of people like King will be copied by the less scrupulous. While King ensured the justification of his actions by using four stages (Determining whether injustices exist, negotiation, self-purification, and direct action) and also insisting upon non-violence from his supporters, it is often assumed that copycats will be less thorough. This increase in lawlessness due to the acceptance of disobedience has, however, been disputed (Dworkin 1978).

There is another problem: if we are to objectively accept that disobedience is justified for a certain group, then how may disobedience be limited for others? This type of argument is often referred to as the slippery slope (Volokh 2003), the idea being that we cannot allow any disobedience since the moment we accept any form of disobedience we will rapidly slide to the bottom of the slope and be required to accept all disobedience. Using the slippery slope to create a feeling of insecurity is not an acceptable solution. Such arguments have been used and abused over a long period of time (Volokh 2003); their complexity may create a desire to simplify. Let us not deny justice for the sake of simple arguments.

If the protest, even the DoS, is an appeal from a minority group to the majority to reconsider, to pay attention to what is occurring within a certain situation, then it fulfils a worthwhile purpose. If the effects of DoS attacks are ephemeral, the purpose also justifies the cost. Therefore, the creation of legislation with the intent of criminalising protest under the guise of terrorism is to minimise the openness we presently enjoy in society.

In his thesis on political terrorism, Bauhn (1989) notes that defining terrorism often hinges on the innocence of the victim. While he disagrees that the act should be defined by the victim's innocence, he sympathises with previous authors' attempts to define the actions of the politically motivated terrorist. His own definition is founded upon an understanding of the difficulties of definition. He defines the terrorist as the perpetrator of terror, and "political terroristic acts are violent, intimidatory and…have political purpose."

While in the main the negative connotation remains, the general concept of terrorism has been under development, particularly so since 2001. The political discourse on terrorism has shifted the focus from the methodology of violent action to the descriptive term for those who would oppose the established order. The main change is that whilst in the past a violent political group was not necessarily terrorist, today a terrorist group does not necessarily have to have committed an act of violence.

The liberation of the terms terrorist and terrorism from the actual act of terror has allowed for a more flexible use of the label. Those who fight against terrorism are justified since terrorism is something reprehensible. This legitimacy is important since the violence perpetrated by the counter-terrorist can at times be greater than the violence carried out by the terrorist (Gearty 2003). Gearty (2003, p 377) talks of "the deliberate or reckless killing of civilians, or the doing of extensive damage to their property, with the intention of thereby communicating a political message of some sort to a third party, usually but not necessarily a government."

While the removal or reduction of the need for violent activity from the definition of terrorist has made it easier for the counter-terrorist to legitimise violence in the name of combating terrorism, it has also allowed for the creation of a more confusing concept of cyberterrorism, which is defined by Denning (2000) as the convergence of terrorism and cyberspace. Since the attacks are online, Denning's terrorist has to be redefined as one who attacks or threatens to attack information; she also adds the requirement that the attack should "result in violence against persons or property, or at least cause enough harm to generate fear". This final part is worrying, since the attack need not cause devastation for the label of cyberterrorism to apply; it is enough if the attack generates fear. The qualification of fear has not been a necessity when defining or discussing offline terrorism. Whether the government or populace is afraid has little bearing upon the justification in applying the term terrorism to a political action. This addition of fear may be due to the fact that there have been few cyberterrorism attacks of any dignity, if indeed there have been any at all (Vegh 2002). Despite the publicity and discussions of the vulnerability of the information society, the cyberterrorist remains a ghost in the machine rather than a serious threat.

Conclusion

The politically motivated online disobedient is actively partaking in a political discourse, the goal of which is to create a more equitable society. The disobedient is exercising fundamental rights of participation in a participatory democracy. Traditionally such rights are not limited without serious cause. The present trend is the use of *hierarchical* (Murray & Scott 2001) regulation to criminalises DoS attacks and more in the name of terrorism are much too far reaching and seriously hamper the enjoyment of individuals' civil rights. The blanket limitation of civil rights within a society should only be tolerated if the limitation also has the effect of removing a serious threat to the society that faces those limitations. The threat of cyberterrorism has been greatly overstated and is founded upon a lack of understanding of the technology, or even technophobia. If the threat comes not from terrorists but rather from criminal use of the DoS technique, then the legislation goes too far in its attempts to create order.

The criteria of disobedience and justification are easily met in online environments and do not conflict with traditional theory. The issue of non-violence is a bit more complex in the sense that the non-violence can be interpreted as zero violence, however this is a flawed interpretation as zero-violence is an unobtainable goal. In the physical world we tolerate (to a varying degree) our lives being occasionally disrupted.

The main issue is one of the moral right (or obligation) to react within a globalised civil society. Within traditional theory the protester would ideally be reacting to either to a moral wrong or withdrawing support for a government carrying out morally wrongful acts. This limitation should not, however, prevent the actions of those who protest in the name of others. The a-national nature of information technology has the effect that it can be used to conduct global protests to aid those who are unable to create a moral majority within their own nation state.

As this chapter has shown, the online political discourse is being threatened and is facing serious discrimination. Activities that would be tolerated or endured offline are being persecuted online. The present day attempt to create harsher penalties for nuisance offences is a serious threat to the development and use of the Internet for online participatory democracy. The rush towards criminalisation should be tempered with a toleration of political discourse and if the regulator wishing to promote online democracy then discrimination of online participation through the overregulation must be avoided.

5

Communication

Genuine poetry can communicate before it is understood.
T.S. Eliot

Introduction

A basic necessity of participatory democracy is the ability to communicate freely (Petäjä 2006, Schauer 1982). This is a relatively uncontroversial statement until this communication is put into practice. Attempts to communicate unpopular information or to communicate information in unappreciated manners are often prevented. Therefore the need to protect communication within a participatory democracy stems from the need to protect the forms of communication that are disliked. Communication, which everyone agrees with requires no special protection. Due in a large part to the simplified media discourse (Kling *et al* 2005) the concept of virus is almost universally vilified. Regulatory structures in most areas affect a unified approach towards viruses and prohibit their creation and dissemination. While it may seem easy to regulate the virus, the definition of a virus is not easy to achieve without including non-harmful or beneficial virus-like code. This causes several non-harmful virus-like applications of software to fall under this regulation. The reliance on the simplified view of viruses creates a hindrance for certain forms of communication thus creating a democratic deficit. The role of freedom of expression is vital within a participatory democracy.

The motivation for the work carried out in this chapter is the discussion, or lack of discussion, which preceded and followed the Cybercrime Convention. There were concerns raised by different actors concerning the implications of the Convention to civil liberties and participatory democracy however these discussions remain relatively anonymous and seldom reach the main political agenda. Therefore the interaction between the regulatory structures, represented both by national legislation and the convention and groups of actors attempting to negotiate and discuss the effects of structural regulation became highly interesting for the theme of this work.

As this chapter will show, the virus is an excellent example of a disruptive technology. The computer virus is many things. It is a piece of software, a technical artefact, a socially defined and constructed phenomenon (Berger & Luckman 1967), and finally it is also a metaphor (Lakoff & Johnsson 1980). The computer virus has become a part of our vocabulary and carries with it certain connotations. The development and dissemination of computer viruses has brought with it social changes in language, behaviour and culture. This specific technology has spawned an industry working to prevent its effects.

There may be those who claim that writing in defence of viruses has no place in democracy. In 2003 the Department of Computer Science at the University of Calgary offered, as a part of a set of courses on Computer Security, a course on computer viruses and malicious software (malware). The decision to offer such a course met with protests from computer security industry (Bontchev 2003). The arguments against the course reflect the prevalent attitude in the computer security industry that there can be no such thing as a good virus. The position taken by the computer security industry is understandable and natural from their point of view. There is however a need to problematise this position. The goal of this chapter is to question the negative attitude towards viruses. The reason for this is that it is this attitude that informs the structural regulation of this technology. Therefore to problematise the virus is to develop a deeper understanding of our regulatory structures.

To better understand the role of both the regulatory structures and the actors a specific area needed to be studied. The work in this chapter focuses upon the regulation of computer viruses. The harmonising effect of the Convention ensures that nation states cannot take an individual perspective on the computer virus and its regulation. Therefore it is of particular importance to be able to define and delineate the computer virus to ensure regulatory coherence and rigour. *The purpose of this chapter is to explore the regulation of online communication by exploring the attempts by the regulator to come to terms with the computer virus.*

Within this chapter the structure is therefore represented by the regulatory acts undertaken by a state or a supra-national organisation. The actions of the actors will be represented by actions those parties which the regulation effects directly or indirectly purposely or inadvertently. The role of the virus in the democratic debate will also be briefly addressed below. At this point it is important to point out that if the goal is to promote a pluralistic participatory democracy, then regulation should be curbing the negative effects of certain things without preventing, or only minimally effecting, legitimate uses, which cause no harm.

Theory

Traditional arguments on freedom of communication are either found in the areas of freedom of the press, freedom of speech or freedom of expression. These three areas reflect the technical developments within the communications field (de Sola Pool 1984). Prior to the development of voice carrying mass mediums freedom of the press was the focus, prior to the development of vision carrying mass mediums freedom of speech was deemed sufficient. With the development of television the concept freedom of expression comes into focus (de Sola Pool 1984). Today with the width of communications technologies available the freedom of communication is in focus. Despite the large amount that has been written about freedom of expression the main arguments tend to fall into three groups for the purpose of free expression: truth, democracy and self-fulfilment (Petäjä 2006, Schauer 1982). The truth argument is represented by Mill (1980 [1859]) who argued that the purpose of free expression was to discover the truth and to this end he presented four arguments against the limitation of the right to freedom of expression. Stated briefly they are:

> First, if any opinion is compelled to silence, that opinion may, for aught we can certainly know, be true. To deny this is to assume our own infallibility.
>
> Secondly, though the silenced opinion be an error, it may, and very commonly does, contain a portion of truth; and since the general or prevailing opinion on any object is rarely or never the whole truth, it is only by the collision of adverse opinions that the remainder of the truth has any chance of being supplied.
>
> Thirdly, even if the received opinion be not only true, but the whole truth; unless it is suffered to be, and actually is, vigorously and earnestly contested, it will, by most of those who receive it, be held in the manner of a prejudice, with little comprehension or feeling of its rational grounds. And not only this, but, fourthly, the meaning of the doctrine itself will be in danger of being lost, or enfeebled, and deprived of its vital effect on the character and conduct: the dogma becoming a mere formal profession, inefficacious for good, but cumbering the ground, and preventing the growth of any real and heartfelt conviction, from reason or personal experience. (pp 115-116).

Therefore the arguments from truth presuppose that if freedom of expression is allowed and unregulated the truth will emerge from these discussions and errors will be corrected. Naturally this approach takes for granted that the truth will always be positive for a society.

The democratic argument has its roots in the writings of Spinoza, Hume and Kant but its most eloquent modern presentation can be found in the work of Alexander Meiklejohn (Schauer 1982). It is based upon primary acceptance of democratic principles as the correct mode of state governance and includes an autonomous decision maker (Schauer 1982). The democratic approach believes freedom of expression to be a necessary component in any society that presupposes the population at large is sovereign. In these societies freedom of expression fulfils two necessary requirements: (i) providing the sovereign electorate with the information it needs to exercise its sovereign power, and (ii) making government officials and public servants accountable to the population at large (Schauer 1982). The democratic approach tends to be biased towards politically oriented expression. Communication between the electorate and officials is understood to be more valuable than other non-political expression.

The self-fulfilment argument for free expression focuses on the role of free expression in the individuals right to self-development (Schauer 1982). Since free expression is a necessary part of the individual's self-fulfilment any limitation to free expression is a hindrance to this fulfilment. This argument is often refered to as the Millian principle since it takes its starting point from Mill's arguments but does not have the same focus on the truth. Whether the truth emerges or not, expression is an important element of self-fulfilment and therefore should not be limited. An exponent of this view, Scanlon (1977), presents the harms that cannot be used to justify legal limitations on acts of expression. These are (i) harms to certain individuals that consist in their coming to have false beliefs as a result of those acts of expression. (ii) Harmful consequences of acts performed as a result of those acts of expression, where the connection between the acts of expression and the subsequent harmful acts consists merely in the fact that the act of expression led the agents to believe (or increased their tendency to believe) these acts to be worth performing. Scanlon (1977) accepts limitations on expression where such expression causes: direct physical injury or damage, produces harmful or unpleasant states of mind, causes others to form an adverse opinion, or defamation, or interference with right to fair trial, causes panic or constitutes a conspiracy to commit a crime. Despite this list of exceptions to the rule the argument for freedom of expression as self-fulfilment is strong since it takes its default value that freedom of expression is the norm and deviations from this norm must be well motivated.

The Computer Virus

While the first use of the term virus to refer to unwanted computer code appeared in the 1970s and the first better definition in the early 1980s the term computer virus continues to be inexact. While the term does have a certain amount of precision in the computer science field this precision is based upon a loose consensus as opposed to exact definition. For the computer scientist this loose consensus is satisfactory but for the law the lack of definition is a major problem in the creation of fair and balanced legislation.

The first problem occurs with the actual term, virus. It was chosen to represent three characteristics: first the fact that the code self-replicates, second that it is unwanted and third that it is ominous. This is fine for most cases but not all programs that are seen under the law as viruses self-replicate.[18] The attempts to define the term have not been all too successful. The first formal attempts were made in Fred Cohen's (1994) doctoral dissertation and included types of computer code with the ability to self-replicate. This definition will therefore include many non-harmful or even useful or beneficial programs.

The term has also captured the interest of the media. The media have used the term carelessly and wrongly in defining almost any occurrence of computer software failure or the loss of data due to anything from carelessly written program code to user error. The virus is an excellent example of the medias use of popular suspicion towards unknown technology to create a shallow media discourse (Kling *et al* 2005). A simplified portrayal of viruses often repeated in the media is one of 'malicious' software. This description is hardly useful since code is inanimate and therefore without emotions, whether malicious or beneficial. If malicious was to be understood to refer to the potential damage then weapons of warfare should also include the prefix malicious.

The problem faced by the law is to be able to define which behaviour it wants to criminalize and to do so without preventing rightful or legitimate behaviour. To be able to do this the definition the law chooses to use must take into consideration alternative factors such as the occurrence of benign

[18] Worms and sometimes even Trojans and Logic bombs are seen as viruses under the law.

viruses, the need for virus research, the role of the recipient of a virus and the role of social engineering etc.

Using the metaphor virus to describe malicious computer code (malware) is not a well-chosen one. Based on the Latin word for poison and equated in everyday speech with something that should be avoided the legislator often forgets that the virus in itself is not necessarily bad. Before continuing a working definition of the computer virus must be given. While definitions have been debated and argued upon a working definition for the purpose of this chapter is necessary. I will use the definition quoted by Brontchev (1996) "We define a computer 'virus' as a self-reproducing program that can 'infect' other programs by modifying them or their environment such that a call to an 'infected' programs implies a call to a possibly evolved, and in most cases, functionally similar copy of the 'virus'."

Phenomena which are often confused with the virus are Worms or Trojans. While these are not viruses they tend to be referred to as viruses by the media or the uninformed. This causes additional complexity when discussing the legal status of computer viruses. The worm is a program that can run independently and travel through networks from one computer to another. The worm is also capable of having different segments of itself on different machines acting in harmony with each other. Worms traditionally do not alter other computer programs but they can be used to carry other viruses that have the ability to affect other programs. The fact that the worm replicates have led many to class them as viruses since they fall naturally into Cohen's formal virus definition. This chapter will include worms in the definition of viruses even though they are technically not viruses. This is necessary since the legislation is often enacted without any particular concern for the correct terminology.

One must remember that even those who are staunchly against viruses agree that viruses can cause greater or lesser harm. Theoretically viruses can be described as being destructive or benign. If benign they cause no damage, some may not be noticed by the user at all or they may, for example, display a message on the screen or play a sound. If the virus is destructive they are able to cause serious damage to the computer system anything from taking disk or memory space, occupying the central processing unit and introducing the risk of incompatibilities and conflicts.

What is Infected?

There are two ways of defining the history and evolution of computer viruses, first by looking at the technical development of the virus and second by taking a strictly chronological view of viruses. Since this chapter is concerned with the regulation of the computer virus the presentation here will be based upon the technical development of the computer virus, explaining briefly what each stage of development entails and when suitable presenting historical data. The presentation here is a simplification. Many viruses are hybrid of several stages of virus evolution. The purpose of this section is to give the reader a general understanding of what the computer virus is and what it can do.

In keeping with the metaphor of malicious software as virus, the virus can be seen as having a life cycle of stages in which it progresses. The dormant phase is when the virus is idle awaiting activation by a specific event such as a date or the presence of a program or file. The propagation stage is when the virus replicates itself and makes an identical copy of itself into other programs or onto system areas on the disk. Each copy is able to propagate and therefore recreate itself. The next stage is known as the triggering stage, this is when the virus is activated and this moves it to the execution stage where the actual event occurs. This could be anything from the destruction of data to a more benign act such as a message on the screen. Viruses can even have no effect, or no visible effect, at all.

Viruses may also be defined via this last execution stage. From the execution stage viruses can be inserted into four different categories: the file infectors, system or boot infector, multi-partite infector and the macro infector. The file infectors most commonly attaches itself to program files but are generally able to infect any file containing executable code (for example script or configuration files) the virus is activated once the file is executed. System or boot-record infectors do not necessarily infect a file but tend to target the portion of the hard drive used for system processes, including the boot-record (the section responsible for booting the operating system). On diskettes the viruses can attach themselves to the Master Boot Record and replicate themselves onto any media in which the disk is inserted. Multi-partite viruses infect boot records as well as files. This hybrid virus therefore manages to create more damage than either of the two mentioned above. It is also therefore more contagious than the previously mentioned viruses. The Macro viruses infect macro-enabled documents. When such a document is opened, the document executes its macro commands automatically. Sometimes the virus is such that the execution does not occur unless triggered by the user.

Another commonly used method in virus description and definition is by observing the historical evolution of the virus. This is not the historical evolution of a single virus but rather the development of virus code. The evolution of viruses has been sub-divided into five different eras, known as generations. These generations do not necessarily represent a historical overview since first generation viruses are still being created today. The generations represent the development of virus creation techniques. Often the later generations include the techniques from the earlier generations.

The first generation are sometimes known as simple viruses were not especially impressive. There main ability, sometimes only ability was their ability, to propagate. While the effects could be serious, such as the case of boot sector viruses which would cause a long chain of linked sectors. In program infecting viruses the viruses tended to keep re-infecting the infected program. The viruses do nothing to disguise or hide their presence. This open re-infection increases the size of the infected programs, which facilitates detection by either noting an increase in size or the repletion of a section of code.

The second-generation viruses where able to remedy the flaw in early virus manufacture, this was done by making the virus aware of itself. Since the first generations continuous growth facilitated detection and therefore destruction the second generation would only infect previously uninfected files. This is usually done by the virus creating a special signature during the first infection. The virus then searches any file for the signature prior to propagation. If the signature is present propagation does not take place.

The third-generation of viruses is sometime known as the stealth virus. They are called stealth since they differ from earlier stages of virus evolution by the ability to disguise themselves. Scanning the secondary storage and searching for a pattern of data unique to each virus could discover earlier generations of viruses. Virus writers counteracted this by employing stealth techniques. These viruses subvert selected system service call interrupts when they are active. For example attempts to perform scans where intercepted by the virus and the scan returned the incorrect answer that the disks were uninfected.

The armoured viruses heralded the fourth generation of viruses. This strain was designed to evade the anti-virus software by confusing it. Methods, which were used, could be the adding of unnecessary code to make detection, identification and destruction more difficult. Some fourth generation viruses used the concept of attack being a form of defence and have the ability to disable the anti-virus software.

The latest generation of viruses, the fifth, encrypted or polymorphic viruses are again attempting to disguise their existence by mutating. The virus infects the target, not with an identical copy of itself but with a mutation. The mutation takes the form of a modified or encrypted version of itself. The virus is able to modify the code sequences it uses to infect the target or encrypting the infecting virus with random encryption keys. This shape shifting makes the virus difficult to detect by simple byte matching and identification therefore requires the employment of more sophisticated algorithms which must be able to decrypt the virus to detect the presence of the infector.

Analysis: Actors

The original Latin word virus meant poison, our culture has learnt that a virus is something to be avoided, and catching a virus is not something to be envied. The whole subject matter is connected to negative connotations. In the digital world the word has had the same negative connotations and this has led to the almost unanimous idea in society, which is reflected in legislation, that the virus is bad and therefore the virus must be eradicated. Anyone intentionally creating a virus must be a bad person and therefore deserves to be punished.

Bontchev (1996) argues that viruses are bad even if they may have potentially "good" or beneficial uses. He begins by stating that technology is in itself a neutral and is therefore neither good nor bad it is only the use of technology that can be deemed as bad. However he concludes that viruses on the whole negative and therefore, according to Bontechev (1996) all viruses are bad. From this he arrives at the conclusion that the eventual beneficial uses of viruses cannot outweigh their negative effects. Cohen (1994) has also argued that there could, in theory, be "good" and beneficial viruses. This position is not without its opponents, Kelman (1997) argues that virus writing is evil and cannot be justified under any circumstances.

The position of this chapter is not to argue the absolute good or evil of viruses, virus writers or virus spreaders. It is not the role of the regulator to define what evil is; definitions of evil should be left to theologians, or maybe philosophers. The position of this chapter is to discuss the importance of recognising the alternative uses of viruses (if any) and to discuss their importance. If there may be important social roles for viruses to play then their outright vilification or criminalisation is not a step forward and this is something that any legislation and court must address. This chapter will present five non-harmful and possibly beneficial uses of virus-like software.

The purpose of this list is not to be exhaustive but rather to exemplify possible beneficial uses from different realms. The point being that if there are beneficial uses for this technology then the regulatory approaches of general prohibition is an incorrect one.

Virus as Art

Art can be understood as the implementation of skill and imagination in the production or creation of aesthetic artefacts, environments or experiences that can be communicated to others. Within the concept of art there are several modes or methods of expression, some of which are generally recognized while others are seen as more extreme. The movements from the accepted to the extreme are not fixed in time nor can they be seen as a linear development (Ross 1984).

Any definition of art will either be too limiting or too vague to be useful. Art almost defies any real definition. As such it was inevitable that the computer software would eventually appraised as an art form in its own right. As Bond (2005) writes: "A programming language is a language after all, albeit a highly constrained one. As such, it is a perfect medium for the poet comfortable with other highly constrained poetic forms like the sonnet or haiku."

The next stage, to create an aesthetic software virus was therefore an inevitable one. Conceived and compiled for the invitation to the 49th Venice Biennale (2001), one of the more important European art events, a European Net Art Collective presented a computer infected with the virus "biennale.py". The virus was developed by the collective 0100101110101101.ORG in collaboration with another group known as epidemiC. The virus is written in the programming language Python.

The collective hoped that the main spread of the virus would be limited to the source code printed on t-shirts and cd roms. They group has also contacted the main anti-virus companies with their virus (Reena 2001) in an attempt to minimize any ill effects of the virus. They describe their work as:

> …Biennale.py is both a computer virus and a work of art. The virus is made public and spread from the Slovenian Pavilion on the opening day of the exhibition, June the 6th 2001. Biennale.py becomes headline-hitting news, suddenly turning into an unprecedented performance, a controversial work of art revealing how media hysteria can be theoretically provoked and raised. Following the spreading of the virus, Symantec Corporation, world leader in Internet security technology, detects Biennale.py and starts the hunt. Eva,

> 0100101110101101.ORG's spokeswoman, says: «As part of an organization that produces art, my only responsibility is to be irresponsible».[19]

The subject of computer code art has also been discussed for a few decades (Bond 2005) which is unsurprising considering the brief amount of time software has been available compared to other more traditional art forms. The aesthetics of software were addressed by Donald Knuth on his 1972 ACM Turing Award lecture entitled "Software as Art" (Bond 2005).

> Lucidity is often pursued as an aesthetic goal unto itself and, when it is achieved, it can impart the most powerful of all reactions. In this respect, a lucid program exhibits a beauty analogous to the beauty exhibited by a profound mathematical theorem, or theory of physics. Typically, it is the mathematically oriented computer scientists who produce the great works in this genre. (Bond 2005, p 121).

Therefore the question is not whether a software virus can be an aesthetic representation but rather whether there is room for these forms of representations within the IT-based participatory democracy.

Virus as Advertising

Advertising is all about transferring information about products, services, opinions, or causes to public notice for the purpose of persuading the public to respond in a certain way toward what is advertised. There is little dispute about the power of advertising to inform and influence the intended audience, nor is their much dispute of the importance of advertising to the advertiser. The ability to market the message and inform the public is often a matter of survival for the advertiser. There are important issues concerning the ability of small organisation to reach a wider audience. Established marketing techniques are often too costly and beyond the reach of smaller organisations.

The use of information technology has been suggested as a method for less wealthy groups to be able to reach a wider audience. Human rights organisations have seen an upswing due in part to their ability to find new members via information technology (Castells 1997, Hick & Teplitsky 2000, Meikle 2002, Pickerill 2003, Walch 1999). The question then is what part of the information technology can be used as a part of advertising.

One such example is the Prolin worm. The W32.Prolin.Worm uses Microsoft Outlook to email a copy of itself to everyone in the Outlook address book. The worm moves all .mp3, .jpg, and .zip files to the root

[19] http://0100101110101101.org/home/biennale_py/index.html

folder. It renames each of these files and appends the following text to the extension of each file: "change atleast now to LINUX".

The W32.Prolin.Worm uses Microsoft Outlook to email a copy of itself to everyone in the Outlook address book. It sends an email with the subject message "A great Shockwave flash movie" and contains the message "Check out this new flash movie that I downloaded just now ... It's Great Bye" in the body. The attachment is named Creative.exe. The worm creates a copy of itself with the name Creative.exe in the C:\Windows\Start Menu\Programs\Startup folder. The worm will run each time Windows is started. Finally the worm leaves this text message in the root folder:

> "Hi, guess you have got the message. I have kept a list of files that I have infected under this. If you are smart enough just reverse back the process. i could have done far better damage, i could have even completely wiped your harddisk. Remember this is a warning & get it sound and clear... - The Penguin" (Klang 2004a, 2005a).

Another example is the MacMag Peace virus. The MacMag virus printed this message on the screen of Apple computer users: "Richard Brandlow, the publisher of MacMag, and his entire staff would like this opportunity to convey their universal message of peace to all MacIntosh users around the world." (Branscombe 1995, p 92) After displaying the message, the virus deletes itself. Although MacMag is not designed to be malicious, infected systems can display a variety of problems (Klang 2004a, 2005a)

These two examples show how viruses may be used to transmit messages to a wider audience. While the recipient may not be pleased to receive this message or she may even be annoyed to receive it the question is whether this is enough of a reason to prohibit such communication. While the Prolin example caused minor damage in terms of annoyance the level of damage caused by the MacMag example must be seen as being exceedingly low. It is a relatively easy task to find people who are disturbed by more traditional advertising such as billboards and neon signs but this alone is not enough to stop this form of provocative communication.

Virus as Free Expression

Freedom of expression is a fundamental human right described in the first session in 1946 by the United Nations General Assembly as the touchstone of all the freedoms to which the United Nations is consecrated (A/RES/59(1): Para.1). Freedom of expression is often described as the precondition of individual self-expression, self-fulfilment and true democracy. The right of expression is, to paraphrase Orwell, the right to tell people what they do not want to hear. It is just this value of telling society what it does not accept to be true or given where free expression plays its most important role. To express an opinion shared by everyone is not something that requires legal protection. To express that which is uncomfortable does.

Despite its importance it is not an absolute. The freedom of expression can easily come into conflict with other rights enjoyed by society and this balance of rights must be carefully weighed and balanced in an open society. First, can a virus writer or distributor be exercising the right of free expression and if so should this right be curtailed? Suffice to say that whether we choose to look at philosophy from Mill to Habermas, international or regional conventions or national law in most cases the writing and distribution of programming code, benign or malicious must be viewed as a communicative act of expression.

There is, however, no doubt that this expression may be curtailed. The classical example that no man may cry "fire" in a crowded theatre is an excellent analogy. The freedom exercised must not cause harm. This then is the necessary balance that must be achieved if the legislator is to attain the goal of both freedom of expression in the case of computer viruses while maintaining a secure environment and protecting property.

The Helpful Virus

There have previously been theories proposed as to what a beneficial virus could be. Researchers such as Cohen (1994) and Bontchev (1996) have proposed both beneficial uses for viruses and rules for which these may be used. Examples put forward to exemplify the concept of the helpful virus are viruses used in research and development. The creation and study of viruses under controlled conditions is an often-cited need for the advancement of anti-virus research. There have also been experiments, mainly within closed networks, to use viruses and worms to help users with updates, bug-fixes and general security issues.

Virus as Artificial Life

> I think computer viruses should count as life. Maybe it says something about human nature, that the only form of life we have created so far is purely destructive. Talk about creating life in our own image. (Hawking 1994, p 1).

In 1997 the Tierra project announced that they had successfully conducted and experiment with the evolution of artificial life. The research was based upon computer programs that were capable of Darwinist evolution. The study was to increase the further knowledge on evolution and the biologist

Thomas Ray used computer programs similar to viruses to be able to understand how the evolutionary process works. The goal of the project was to show that the organisms could survive under conditions of free evolution and secondly, to develop a digital model of the Cambrian explosion of life which took place on Earth about 530 million years ago when the first multicellular creatures with hard parts suddenly evolved.

The question as to whether computer viruses also may be seen as artificial life has been discussed by Spafford (1994) in this article he discusses ten criteria for the definition of life and compares them to the behaviour of computer viruses. He concludes that the computer virus is something akin to artificial life but cannot be refined to develop into an artificial life form. Despite the fact that Spafford (1994) does not believe that the virus may be refined into an artificial life form he concedes that the study of viruses is an important one.

Analysis: Structures

The legislative approaches to computer viruses tend to follow the general arguments found in the relatively uninformed media debates (Kling *et al* 2005). Those who would speak in favour of computer viruses are considered to be naïve or misguided since they do not comprehend the damage malicious viruses cause and since malicious viruses cause damage to property they are inherently bad and must be prohibited. Those who argue against the computer virus are often seen as being either anti-virus corporations attempting to create scares or law enforcement officials who have no appreciation of either the rights and necessities involved in the use of computer viruses.

Another issue is the fact that the term “virus” is often inadequately defined in legal texts. This lack of adequate definition leads to the problem that many benign, healthy and helpful programs fall under the definition of computer virus. This does not necessarily mean that the creators and distributors of these programs will be prosecuted but what it does mean is that there is an uncertainty in the law. The need for predictability and certainty is not satisfied when the law states not what a virus is but allows the virus to be either the fact that unwanted damage occurred or the fact that the regulator disapproved of the program.

Spanning the possible width of legislative approaches is the liberal laissez faire combined with the free expression arguments to the restrictive approach of full criminalisation. The free expressionists tend to attempt to argue that the law should not limit their expression via viruses. The laissez fair approach seems often to be seen as a lack of action or it can take the position of "wait and see".

The arguments, for full criminalisation, are based upon the concept of the virus as an indisputable evil and as such have no place in society. Kelman (1997) equates virus writers to murders and terrorists.

> As a staunch defender of Free Speech and the rights of young people to experiment with their lives in recent months I have had to face up to some unpalatable facts - virus writing is evil and cannot be justified in any circumstances. It follows that prosecution of virus writers is something which should be universally accepted as appropriate action. Virus writing needs to be recognized as a criminal act by international conventions and virus writers should always be subject to extradition. Just like murderers and terrorists, virus writers should find no escape across national boundaries. And the investigation of computer viruses needs to be a regulated activity with failure to apply for regulation being a criminal offence.

Kelman (1997) therefore advocates the addition of the computer virus writer to the list of criminals that, under international law, are to be seen as terrorists or war criminals. They are to be offered no harbour or defence for their actions. This approach is frightening since it is all to simple to point to other actions or uses of technology that have caused more pain, suffering or human and property damage without achieving any of the status argued for here.

While both these extremes are positions, which should be avoided the latter position is more worrying since it does not attempt to define what it is that actually makes a virus writer a terrorist. Without an adequate definition anyone who writes or modifies computer code can fall into this category irrespective of any criminal intent.

What is the Crime?

One question in looking at what should be protected and what should be criminalised in connection to computer viruses is the question of which effects the virus has. There are seven different basic criminal acts, which could be of special interest in connection to viruses. The first is the actual writing of the code, which could be seen as a preparation to commit a crime, second is unauthorized access, which occurs when the virus enters into a new computer without the authority of the legitimate user. Third is the question of unauthorized modification, which could be the infection of a file, boot sector, or partition sector. Fourth, is loss of data, the effects of the virus may be that the data is no longer accessible by the legitimate user. Fifth may be the endangerment of public safety due to the failure or reduction of efficiency of the computers. Sixth, the making virus code available to others may be seen as incitement. This includes making available viruses, virus code, information on virus creation, and virus engines. Seventh is denial of service, which may be the effects of the virus. The second issue, which must be addressed, is how to deal with the actions of preparation to commit and attempt to commit. Also the legislation should take into consideration mitigating circumstances, minor offences and the actions of the recipient.[20]

The issue is not one of regulation or not. There is obviously a need for anti-virus legislation. But not in the sense of virus legislation as it is today. There is a need for the legislation of malicious software no matter the form. There is also a necessity of clarifying the responsibility of legitimate software that causes harm or property damage However this case study will limit itself specifically to the role of viruses and not to this latter larger issue of clarifying the responsibility of legitimate software which causes harm or property damage. The following three sections will present virus regulation within three different jurisdictions.

The United Kingdom Approach

Prior to legislating against computer viruses, tort law and the Criminal Damage Act where used. In the case of *Cox v Riley*[21] charges were brought under the Criminal Damage Act 1971 which states:

> A person who without lawful excuse destroys or damages any property belonging to another intending to destroy or damage any such property…shall be guilty of an offence.

Cox was employed to work a computerised saw. The equipment in question consisted of a powered saw whose operations could be controlled by means of the insertion of a printed circuit card containing a number of computer programs. The equipment contained a program cancellation facility. This was used by Cox, deliberately and without due cause, so that the programs were erased and the saw rendered useless until it was reprogrammed. The Divisional Court held that the critical factor was that as a result of Cox's conduct, the saw's owner was required to expend time and money in restoring the saw itself to its original condition.

[20] Little or no room has been given to this issue in this work. The role of the recipient is crucial in the limitation or damage.

[21] (1986) 83 Cr App R 54.

The need to improve legislation to also include computer equipment into the Criminal Damage Act was clear. The Law Commission expressed the view that difficulties had been encountered in the bringing of prosecutions under this Act. Acting on its recommendations, the Computer Misuse Act was enacted which provides in section 3 that an offence will be committed by a person who causes a modification to the contents of a computer system with the intention of impairing its operation. The Act also modifies the Criminal Damage Act to make it clear that for the purposes of the Criminal Damage Act 1971 a modification of computer software shall not be regarded as damage unless the effects impair the physical condition.

Section 3 of the Computer Misuse Act 1990 refers to the unauthorised modification of computer material. This section must be read in conjunction with section 17, which is concerned with the interpretation of the Act. From section 17 we can surmise that section 3 covers a wide range of different activities. It covers all form of intentional alteration and erasure of programs and data (Computer Misuse Act 1990 (s.17(1)(a))) where the intention is to impair the operation of the computer or hinder the use for the legitimate user. It is important to note that recklessness is not sufficient mens rea for this offence (Wasik 2000).

Soon after the enactment, the Court of Appeal delivered its judgment in the last computer related case brought under the 1971 Act. In *R v Whitely*, the intentional alteration of information contained on a computer disk caused significant impairment to a range of computer systems including some used in connection with medical research. He was convicted of offences under the Criminal Damage Act. The Court of Appeal sustained the convictions holding that damage to the contents of computer systems constituted criminal damage in the same manner as damage done to tangible property under the same Act despite the fact that changes in the magnetic particles on the disk could not easily be viewed (*R v Whitely* [1993] FSR 168 (CA)).

A more recent case was that of “the Black Baron” - Christopher Pile released a toolkit, named SMEG, which could randomise the code of existing viruses and therefore making them more difficult to detect, he also released two SMEG viruses called Pathogen and Queeg. These viruses where both polymorphic and encrypted, they displayed messages such as this one for the Pathogen virus:

> Your hard-disk is being corrupted, courtesy of PATHOGEN!
>
> Programmed in the U.K. (Yes, NOT Bulgaria!)
>
> [C] The Black Baron 1993-4.

> Featuring SMEG v0.1: Simulated Metamorphic Encryption Generator!
>
> 'Smoke me a kipper, I`ll be back for breakfast.....'
>
> Unfortunately some of your data won't!!!!! [22]

Pile was charged under the Computer Misuse Act and in 1995 he was sentenced to 18 months in prison (R *v Pile* (1995) unreported).

A noteworthy aspect to consider in the move towards criminalisation is that even if the act becomes criminalised the damages caused are not automatically resolved. The person or organisation must still apply for damages despite any criminal court proceedings prosecuted by the state.

The United States Approach

Before legislation in the eighties the American courts used common law principles to prosecute computer crime. Most often, drawing analogies between ordinary crimes and the new situations created by the new technology. It became a difficult task to attempt to analogise virus distribution to traditional common law transgression such as trespass. The increase in technology use led to further cases and the widespread realisation that legislation was required to improve the situation.

The Computer Fraud and Abuse Act of 1986 replaced the first piece of legislation (The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984) this was a marked improvement in clarity and usability. This new Act specified that "unauthorized access to a government computer" was a felony, and "trespass into a federal government computer" was a misdemeanour. The difficulties with this act became clear in its usage. It soon became clear that the Act prescribed a too narrow standard of culpability (Colombell 2002). The Act required that the virus writer or distributor must "knowingly" or "intentionally" cause the damage. This becomes difficult to prove due to the fact that once the virus is released it is almost impossible to know how and where it will strike and therefore also which damages it may cause.

More recently there have been amendments to the legislation concerning virus regulation in the form of the 2001 PATRIOT Act (Field Guidance 2001). In Section 1030(c), the PATRIOT Act amends the penalties for hackers that damage computers and also it eliminates mandatory minimum sentences. Prior to the amendment offenders violating section 1030(a)(5) could receive no more than five years imprisonment while repeat offenders

[22] http://securityresponse.symantec.com/avcenter/venc/data/smeg.pathogen.html

received up to a maximum of ten years. It was felt that these sentences where inadequate to deal with such offenders, such as the creator of viruses, like the Melissa virus, which caused huge damage (Klang 2004a, 2005a).

Previous law also included mandatory sentencing guidelines with a minimum of six months imprisonment for any violation of section 1030(a)(5), as well as for violations of section 1030(a)(4) (accessing a protected computer with the intent to defraud). The amendment (Section 814 of the Act) raises the maximum penalty for violations for damaging a protected computer to ten years for first offenders, and twenty years for repeat offenders (18 U.S.C. § 1030(c)(4)). At the same time the amendment removes the mandatory minimum guidelines sentencing for section 1030 violations.

The Swedish Approach

As early as 1992 the *Datastraffrättsutredning* (1992) suggested that a new type of (*allmänfarlig*) crime should be created in Swedish law. The crime was to prevent the manufacture and spread of computer virus. The wording of the legislation was to prevent the manufacture of program code that was created with the intent to alter data without the consent of the data owner. It was also to prevent the spreading of code that had the ability to cause a danger of data loss. Despite the interest in this proposed legislation no measures have been taken by the government in the creation of any such legislation.

There is no specific prohibition on the manufacture of viruses or malicious software under Swedish law. However, the manufacture and spreading of malicious code (computer virus) can fall into several criminal categories such as illegal computer entry (*dataintrång*), criminal damage (*skadegörelse*), and sabotage (*sabotage*).

Illegal computer entry, according to the Swedish Criminal Code (*Brottsbalken*) Chapter 4 Article 9(c) states that anyone who without authorisation gains access to data or without authorisation makes changes or erases data will be sentenced to illegal computer entry to fines or imprisonment for up to two years. The legislation on criminal damage (Ibid Chapter 12) is both simple and clear. Destruction of, or damage to, property, which affects another's rights to said property would be sentenced to fines or imprisonment for a maximum of six months. Sabotage (Ibid Chapter 13 art. 4) is more concerned with the damage or destruction of property which is of vital importance to the defence of the realm, public maintenance, the process of justice or administration or the maintenance of public order and public safety shall be sentenced to imprisonment for the crime of sabotage for a period of a maximum of four years.

The ability to prosecute the perpetrator involves a problem of a legal-technical nature. This is due to the fact that for responsibility for these actions to be sentenced, the attack must be directed towards a certain target, for example a certain data. The prosecutor must also be able to show that the perpetrator had intent to cause the damage to the target. This is often very difficult to prove since the virus manufacturers or distributors are usually unaware of the full extent of the damage their virus may cause. If data, which is damaged by a virus, can be seen as damage to property (*sakskada*) then this can lead to a claim of damages even in a non-criminal use of viruses. A condition for a successful claim for damages is that they have been caused by criminal negligence.

Since July 1, 2001 the law has been amended to also criminalize the manufacture of viruses. The purpose of the change was also to clarify that not only physical, but also "immaterial" objects can be seen as such criminal aides that are included in the crime of "preparation to commit a crime" (Ibid Chapter 23). The preparatory works specifically mention computer viruses, computer programs exclusively manufactured to gain illegal entry or other types of crimes such as forgery (Proposition 2000).

In the crime of "preparation to commit" the law does not require that the manufacturer of a virus has had the intent to commit a specific attack but rather that there is an intent to commit a certain crime, sooner or later.

Convention on Cybercrime

The Convention on Cybercrime includes provisions dealing with illegal access and interception of computerized information of any kind, including data and system interference. Some provisions contained in the draft treaty limit the production, distribution, and possession of the software used by hackers to exploit computer vulnerabilities.

The most important regulatory tool at present is the Cybercrime Convention (2001) since it has recently been adopted and is in the process of being ratified in several countries. It is both an instrument of harmonisation and a harsh instrument which will become the de facto standard of regulation for many of the activities described in this thesis. This convention has been heavily criticized for many things, amongst others, the way in which it was developed, its lack of concern for privacy and human rights and its tendency to grant sweeping powers to police and investigatory agencies (Akdeniz 2005). Amongst the many acts, which the draft convention attempts to regulate, is the creation and distribution of the computer virus.

> Article 4 – Data interference
>
> 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
>
> 2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

The aim of Article 4 is to provide computer data and computer programs with protection similar to that enjoyed by corporeal objects against intentional infliction of damage. The protected legal interest here is the integrity and the proper functioning or use of stored computer data or computer programs.

In paragraph 1, 'damaging' and 'deteriorating' refer to the alteration of computer programs or data. Deletion is equated with the destruction of a corporeal thing since deletion makes data useless or unrecognisable. The concept of suppressing data is the making of data unavailable to the legitimate user. Alteration refers to the modification of existing data and would include the addition of viruses, Trojan horses and logic bombs etc. The actions in Article 4 are only punishable if they are committed without authorisation and the offender must have acted with intent.

The second paragraph allows for legislation to include the proviso that criminalisation must require serious harm. The concept of serious harm is left up to each legislating state to decide but each state is under obligation to notify the Secretary General of the Council of Europe of their interpretation if use is made of this reservation possibility.

> Article 5 – System interference
>
> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

The purpose of this provision is to criminalise the intentional sabotage which prevent the lawful use of computer systems, here computer systems also include telecommunications facilities, by using or influencing computer data.

The attempt is to create a level of protection for the legitimate interests of the users of computer or telecommunications equipment. The term "hindering" refers to any and all actions that interfere with the proper functioning of the system. This could be anything from inputting, transmitting, damaging, deleting, altering or suppressing computer data.

To create criminal sanctions it is not enough that hindering has taken place it is also necessary for the hindrance to be of a serious nature. Each state shall be able to define for itself what the level of seriousness may be. The drafters of the convention, however, consider serious

> …the sending of data to a particular system in such a form, size or frequency that it has a significant detrimental effect on the ability of the owner or operator to use the system, or to communicate with other systems (e.g., by means of programs that generate "denial of service" attacks, malicious codes such as viruses that prevent or substantially slow the operation of the system, or programs that send huge quantities of electronic mail to a recipient in order to block the communications functions of the system). (Cybercrime Explanatory Report 2001).

Misuse of Devices (Article 6)

With paragraph 1(a)1 the idea was to criminalise the production, sale, procurement for use, import, distribution or otherwise making available of a device, including a computer programme, designed or adapted primarily for the purpose of committing any of the offences established in Articles 2-5 of the present Convention. In this section 'distribution' refers to the active act of forwarding data to others, while 'making available' refers to the act of making available by the placing of said devices online for others to download and use. This also includes the disputable act of linking to a computer virus.

The Convention goes quite far in its criminalisation of the computer virus. The creation of a virus will become, under this convention, a criminal offence, the same with the distribution of any virus programs. The interesting issue is that even a hyperlink to a virus will entail prosecution for distribution. One cannot help but wonder how far the crime of linking to material can be interpreted as being a criminal act.

Discussion

It is necessary to be clear upon one point: The spreading of software, which causes damage to others property, is not what this chapter seeks to defend. The purpose of this chapter is to question which issues present and future regulation must take into consideration when dealing with computer viruses. One point that becomes quickly clear is the fact that the term virus is not one which can, or should, be used by regulators since the term does not clarify the problem. When it is defined it is badly defined at best and without definition the term serves no useful purpose except to create a spectre which to persecute. Besides the point that the term virus is exceedingly inaccurate this chapter attempts to show that the term virus can, and does, include several uses that may not be such as to warrant criminalisation.

If we are able to create a virus as an art form, that must necessarily include the proviso that it does not damage other people's property or harm their persons, the suppression of a creative form of expression is to be equated with censorship. Censorship is not only an abusive practice it is also today frowned upon in open societies. The practice of censorship has long been used to suppress that which does not please the mainstream of society (for more on this topic see Chapter 9). The question, which must be posed, is whether a virus can be spread without damaging other people's property, this question is often answered in the negative. The reason for this negative response is the fact that viruses take up space on other people's computers that therefore prevents them from using their property to the full extent. There are three interesting points that can be raised against this. The first is the question of whether today computer storage memory can still be seen as the limited resource it once was. Secondly there is the question of whether the argument of disk space can be used against many badly designed programs which tend to use more than their needed space on the disk and finally, can this be a valid argument if the program code destroys itself and leaves no lasting damage. Any legislation, which states that viruses are forbidden, will go beyond that which is necessary and border upon censorship.

If there can be such a thing as an advertising virus which fulfils the same requirements as the artistic (self destructing and non-damaging) the question again can be posed – should the regulator go so far as to outlaw the virus. The marketing virus should be dealt with under marketing law in much the same way as spam or the irritating pop-up windows.

The question of viruses being used either to market human rights groups is no different from the marketing argument above. But one of the least discussed issues is whether a damaging virus can be used for good. As earlier mentioned Bontchev (1996) reminds us that viruses are only technology and as such neutral, this means that it is only in the actual use that we can define if the virus is good or evil (Kallinikos 2005).

In the legal debate we often see actions not only from their effects but also we attempt to value the actions based upon the intentions of the perpetrator. In certain cases we allow harmful acts if they are done to prevent a greater evil. One such example is the permissibility of the use of force in self-defence or in the protection of property. On the web there is a growing practice of hacktivism (Klang 2004a, 2005a) (for more on this topic see Chapter 4). This is the use of hacker techniques to either change the message on others web pages or to use multiple browsers to access a site thus preventing (in theory) legitimate use of the site. These denial-of-service attacks can be seen as being a form of picketing or demonstration, but they can also be seen as being a form of trespass (Klang 2004a, 2005a). What would be the role of a virus used for these purposes and how should the law deal with the desire of the populous to protest and the rights of corporate individuals.

There is also the issue of useful software containing much of the same characteristics as the computer virus. Both naturally helpful programs which help the user carry out tasks such as copying files, updating systems and more and the more specific programs created for either virus research or research into such areas as the Cambrian explosion mentioned above. The limitation of the use of any programs that would fall under a definition of virus would in this case be more of a hindrance than a help to the legitimate user or society at large.

The question therefore remains whether legislation has gone too far? And what should the alternative approach be. One interesting methodological approach is the use of functional equivalency[23]. The main concept is transferable to virus legislation. Instead of creating new and nationally diverse legislation the idea is to allow the courts a greater amount of independence when deciding upon cases involving new technology. This approach is most closely seen in the type of legislation adopted by Sweden in its attempts to come to terms with viruses.

No matter which legislative approach is chosen the problem is here to stay. Not only have we only seen the beginning of the problem with the insertion of more technology and more computer code into everything from mobile telephones, cars, fridges and any hand-held device, the computer virus as a menace and as a fact will become a common event. The interconnectedness (Kallinikos 2005) of devices will additionally lead to the problem of not being able to limit the spread to certain types of devices. Therefore the

[23] See *Theoretical Focus* page 38 *et seq.*

traditional defence of isolation will not work to protect our devices from each others viruses.

The width of choices for different countries in legislating viruses will make for interesting cases where countries such as the United States penalising virus writers with jail terms running into decades while other countries may be choosing to fine its viruses writers. The cybercrime treaty is one way to go but as we have seen with other such ideas the application of multinational treaties are difficult to ensure.

Today, and for a long time into the future it is still up to the legitimate user to take precautionary measures to ensure the integrity of their systems. The question is when will the law begin to demand a reasonable standard of care from the legitimate users. Is it fair to cry foul when a virus infects a system and damages data if it was triggered by an employee wishing to read an anonymous love letter or see nude pictures of tennis stars (Klang 2003a). The effects of the social engineering of the virus must eventually be taken into account if virus legislation is to become well balanced. By now anyone who opens unknown attachments should know (or should be informed) that they are playing with fire.

The legislation of viruses is a serious affair. The concept itself is shrouded in mystery and fear. This is not a good basis for a balanced and fair debate but tends to be the basis of a witch-hunt. The creation of destructive software must obviously be dealt with swiftly and efficiently by the law in the same manner as any other form of criminal damage. At the same time the new legislation must not be used to give sweeping powers to the courts to remove anything that does not conform to the mainstream of computer usage.

Conclusion

From the three national approaches to the regulation of the disruptive technology of viruses we can deduce two basic approaches to regulating the phenomenon, these are *hierarchical* and *design-based* regulation (Murray & Scott 2001). The *design-based* control is seen through the use of anti-virus software – this has not been the focus of this chapter.

The focus of this chapter has been on the two opposing methods of *hierarchical* regulation. The more common approach is the general prohibition of the creation and dissemination of viruses. This approach negatively affects any virus-like software that may be harmless or even beneficial. The case study has presented examples of virus software that can be classified as being beneficial (in the case of research and development) or harmless (in the case of advertising). In these cases a general prohibition limits the manner in which certain individuals can communicate their ideas to others.

The less common approach of *hierarchical* regulation is represented in this work by the Swedish position on viruses is not to criminalise the software. The latter position has the advantage of not having to attribute character traits to inanimate objects – as is the case with the concept of malicious code. This approach is interested only in demanding that individuals act responsibly and are liable for any damages they may cause. Such an approach is common in many other social regulations, for example in the case of car insurance. The technology is not prohibited but damages caused by the reckless driver must be carried by the driver or his insurance company.

However, as this case study has also shown, this third approach is not going to be able to remain in place much longer. Due to the moral panics (Thompson 1998) and the shallow media discourse (Kling *et al* 2005) the topic of viruses has become a high level concern. In response to this the Convention on Cybercrime has been developed and is now in the process of implementation in large parts of the world. This convention reflects and reinforces the repressive views of the regulation shown here. The effect of this is that the regulatory position in relation to viruses will be criminalisation of the creation and dissemination. This entails a limitation of one of the core values in a democratic society while few believe that harmful viruses can be eradicated by prohibitive legislation the effect is one of ensuring that non-harmful virus-like software cannot be used as a form of communication.

Therefore, as this case study has shown, the disruptive technology in the form of the virus has created a drive towards regulation. In the desire to regulate, the regulator chooses a method, which creates a blanket prohibition against the disruptive technology notwithstanding, that the technology itself contains legitimate uses within a participatory democracy. The net effect of these regulatory actions is the loss of democratic interaction in the virtual environment and the discrimination of the online environment in favour of the more conservative communication of the offline world.

6

Integrity

Forty years it had taken him to learn what kind of smile was hidden beneath the dark moustache...But it was all right, everything was all right, the struggle was finished. He had won the victory over himself. He loved Big Brother.

George Orwell

Introduction

This case involves the examination of the role of integrity in a participatory democracy. The importance of the connection between integrity and democracy should not be understated. Integrity is, as Sundström (2001) writes, a prerequisite for democracy. In this study we can see the effect of when users experience a lack of integrity through spyware. The perceived lack of integrity causes concern among users. This concern was however met with a regulatory inertia since the apparent legal position of the software in question could be disputed. This lack of concern for the users opinions vis-à-vis integrity resulted in the creation of a market based regulatory solutions. These solutions came in the form of integrity protecting, spyware removal software.

The earliest uses of the term Spyware to denote a particular form of software that gathers, without the users knowledge, information about the user and transmits it back manufacturer appeared around 2000 (Zone Alarm 2000). However awareness of the concept grew slowly. The empirical work that provides the foundations of this chapter was carried out during the period of 2002-2003. This was a period during which the discussion of spyware was growing in importance among privacy[24] advocates.

This chapter discusses an unusual type of surveillance software, which may be installed in many computers. The strange aspect of this software is that it has often been downloaded and installed by the user, but without her knowledge. The software is mainly designed to collect information about the user of the computer and relay this information back to the software manufacturer. The download, installation, data collection and data transfer all take place within the users own computer but very seldom with the users knowledge (Freeman & Urbaczewski 2005, Zhang 2005). It is the intention of this chapter to describe the technology involved and thereafter discuss how this new technology is affecting the online privacy debate. The chapter continues to discuss the basis for legitimacy of technology and also the current level of technological deterrents available. The chapter concludes with a comparison of two approaches at resolving the current problem, via legislation or the market approach.

The importance of the discussion of spyware lies in the discussion of control of user data and user control over the personal computer. Despite being installed via deceit (Klang 2004b) those discussing the effects of spyware on user integrity and privacy issues were aware of the fact that causing spyware to be installed was not an illegal act. Therefore the discussion becomes a practical definition and implementation of the concept of online privacy. Groups of actors perceived spyware to be a threat to individual privacy despite the uncertain legal position gives spyware manufacturers an upper hand.

The failing ability of regulatory structures to provide protection against the perceived threat of spyware create the rise of a market based solution where software manufacturers created anti-spyware software to provide users the wherewithal to prevent spyware from operating within their computers. The example of spyware provides an excellent case of the failure of structural regulation, the rise of a perceived threat among actors and the development of a market-based solution to the perceived threat. By studying this example we may find a method where the slowness of structural regulation to react to a perceived user threat provides both an economic opportunity for actors and provides an example of how online problems can be resolved without the intervention of regulatory structures.

[24] For the purpose of this work the terms privacy and integrity are viewed as synonyms and used interchangeably.

The purpose of this chapter is to illuminate an example where regulatory structures fail to act in an adequate manner and the solution to the problem is enacted by the socio-technical means in the sense that the solution lies in a combination of technological, organisational and social solutions.

Theory

The discussion of privacy as a philosophical, social and legal value has been lively ever since the publication in 1890 of the influential paper, *The Right to Privacy* (Warren & Brandeis 1890). Arguably the clearest conclusion from this long debate is that the interpretation of privacy is context dependent. However despite the width of the arguments most can be categorised either as belonging to the reductionist approach or by viewing privacy a necessary individual right (Thompson 1975). The reductionist approach understands privacy as being described by its component parts while ignoring the relationships between them. This is the view that privacy is not unique and can be reduced to other interests. The second approach to privacy is to see it as a fundamental human need or right and therefore it needs not be derived from other rights. Thompson (1975) argues that privacy is not an individual right but can be motivated and defended by using other rights, which makes the right to privacy *per se* unnecessary.

> For if I am right, the right to privacy is 'derivative' in this sense: it is possible to explain in the case of each right in the cluster how come we have it without even once mentioning the right to privacy. Indeed, the wrongness of every violation of the right to privacy can be explained without even once mentioning it. (Thompson, p. 313).

Posner (1984) argues for the reductionist approach by using an economic analysis of privacy. He argues that "personal privacy seems to be valued more highly than organizational privacy, a reverse ordering would be more consistent with the economics of the problem." The reductionist arguments have often been attacked by scholars (Rachaels 1975), who claim that the distinctive right to privacy is both desirable and important when attempting to support and protect this interest.

The debate on integrity has developed over time (Wong 2005) and has always stood in relation to the level of technology of the day. The seminal Warren and Brandeis (1890) article on privacy was very much a result of the technology of the time. They recognized the developments of technology and feared, amongst other things, the continued development of the small portable camera that could be handled by the amateur (Kern 1983).

The idea behind the Warren and Brandeis (1890) article was to explore whether existing US law afforded a principle of privacy protection. Their conclusions have been actively discussed since then. The reason for this discussion is that privacy is an ambiguous term definitions have ranged between the right to be let alone, (Warren & Brandeis 1890), the development of personality (Strömholm 1967) to the right to control information about oneself (Fried 1970). This privacy includes other notions such as individual dignity and integrity, personal uniqueness and personal autonomy.

Westin (1967, p 25) examines privacy from the starting point that "…the constant search in democracies must be for the proper boundary line in each specific situation and for an over-all equilibrium that serves to strengthen democratic institution and processes." The search for an adequate understanding of privacy is further complicated by different methods implemented in attempting definitions. Therefore some writers have described the condition of privacy, characterising its features but not offering a definition (Parker 1974) while others have attempted definitions.

Westin (1967) conducted anthropological studies of privacy and through these he offers a control-based definition of privacy claiming that it is the:

> …claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal means, either in a state of solitude or small-group intimacy, or, when among larger groups, in a condition of anonymity or reserve. (p 7).

While control-based definitions have their advantages and are attractive to the individual or group invoking privacy rights they have been criticised for their focus upon individual autonomy since this focus becomes a weakness when attempting to formulate privacy protection policies (Regan 1995). In rejecting the control-based approach as being inefficient for policy formulation Regan (1995) argues that greater recognition should be given to the "broader social importance of privacy". The reasons for this are threefold, firstly privacy should be understood as a common value in which all individuals value some degree of privacy, secondly privacy is as a public value, which is not merely of value to the democratic political system and thirdly privacy can be understood as a "collective value" in light of technological developments and market forces, requiring minimum levels of privacy protection.

A flaw contained within the control-based definition is that it is inadequate when considering instances where personal information is obtained without the individuals knowledge and therefore without informed consent. This is common through methods such as data mining techniques and online profiling (Bygrave 2002). Such methods cannot provide methods for the subject to control information and therefore the remaining alternative is regulation of minimum standards of data protection (Bygrave 2002).

Foucault & the Panopticon

In an attempt to reform the prison system of his time Bentham (1995 [1787]) developed an architectural plan for an ideal prison called the Panopticon. His ideal prison design was a ring shaped prison with a watchtower in the centre of the ring. The ring contained the cells were each prisoner would sit in individual cells. Each cell would have a window on the outer wall to allow light into the cell and a large opening, opposite the window and facing the watchtower. The walls of the cell were extended to prevent the prisoners from communicating with, or even seeing, each other. From the watchtower the guard could see everything in each cell while the use of lighting and blinds prevented the prisoners from seeing the guards and therefore they could never know if they were watched at any time. The prisoners could only act on the assumption that they could be watched at any time.

The Panopticon design is control by architecture. With a minimum of manpower and direct intervention the prisoners are immersed in total visibility and the inmates reaction must be one of self-control (Foucault 1980). The gaze of the guards is through this architecture internalised by the prisoner making the prisoner become her own guard. Through this self-policing surveillance the effects are constant and pervasive even when no actual surveillance is being carried out. As Foucault (1980) notes the Panopticon is an architectural device made into regulation.

> There is no need for arms, physical violence, material constraints. Just a gaze. An inspecting gaze, a gaze which each individual under its weight will end up by interiorising to the point that he is his own overseer, each individual thus exercising this surveillance over, and against himself. A superb formula: power exercised continuously and for what turns out to be a minimal cost. (Foucault 1980, p 155).

Since his presentation of the metaphor of the architectural device Foucault's interpretation of the Panopticon has been widely used in discussions on privacy and surveillance. The basic premise is that the awareness of potential surveillance effects the way in which the subject under potential surveillance behaves. The Bentham/Foucault Panopticon metaphor has increased in popularity with the increased use of surveillance technology both online and offline. This metaphor is however not applicable in the situation of privacy since, as explained below, the user under surveillance is unaware of the surveillance. Therefore the actor continues to behave in an open manner. The difference therefore is that the actor has no choice in the matter. The use of covert surveillance regularly considered to be a more serious interference with the individual's integrity and usually allowed only in more extreme situations (Etzioni 1999, Norris & Armstrong 1999).

Spying Technology

Spyware can be defined as surveillance technology or software, which is bundled into another piece of software and enters the 'infected' computer, and use the 'infected' computer in an unauthorised manner. Blanke (2006) writes about spyware,

> Basically, they are computer programs that are installed (or install themselves) on computers and perform activities that range from the innocuous to the criminal, but almost always negatively affect the basic use and enjoyment of the machine. (pp 1-2).

Spyware is most commonly bundled together with freeware which the user downloads and installs (Klang 2003b, 2004b). The main purpose of the spyware is to collect information, and send it to the information gatherer. Spyware, once installed on the computer, can take a wide range of activities such as: (i) Transmit information about the computer user to a third party, (ii) Lower the security by subjecting it to allowing an attacker to remotely control the infected computer, (iii) Record keystrokes to reveal passwords and other sensitive information, (iv) Enable the computer to be hijacked and used in a denial-of-service attack, and (v) Search for vulnerabilities which may be exploited by hackers (Thompson 2005).

This chapter takes a more limited view of spyware, focusing on the types of spyware that most users find objectionable. The reason for this is that most users would prefer, had they known what was happening, not to have spyware on their computers. This becomes an interesting ethical discussion since the spyware manufacturers tend to claim that the users have agreed to the spyware installed in their computers. Since there is a difference of opinion as to whether or not the spyware has been installed with or without the users consent the actual installation becomes a critical issue. What is interesting to note is the fact that spyware can be included with the users consent but without her knowledge. This is done by including spyware clauses in the end user licence agreement (EULA) which is displayed when the user begins installing the software and requires the user to agree to the terms before the software can be installed and used. The importance of contract law and the EULA will be discussed further below. The discussion on spyware is made more complex due to the lack of an agreed upon definition; this flaw seems to stem from a lack of adequate consensus with which to reach a definition. The name alone is not universal, spyware is sometime known as scumware, parasite-ware, stealware or theftware and occasionally mixed up with computer trojans, viruses and worms. This chapter uses the name spyware since it is the name, which is rapidly becoming the most accepted when describing the phenomenon.

An important additional aspect of spyware is the difficulty connected with its removal. Spyware rarely appears in the computers uninstall list and even if it can be located removal of parts of the software can sometimes affect the more traditional workings of the computer. Other complaints connected with the removal of spyware have been the issue that if not totally removed the spyware has an ability to re-install itself.

To create a better understanding of what spyware may be, five examples of spyware (Klang 2004b) will be presented in this section. The purpose of these examples is not to provide an exhaustive list, nor is it to point a finger at manufacturers or software as being extreme in any way. These examples were chosen since they are reasonably well documented and therefore serve to give the reader an example of what the software and their manufacturers are attempting to do.

The first example is Comet Systems Inc., the maker of Comet Cursor. The software allows the user to change the colour and shape of the computer cursor. The shape can change into alternative shapes such as company logos when the user visits websites connected with the service. However the software also installs a GUID (global unique identifier) and is able to follow the users online browsing habits (Klang 2004b). The effect of installing a GUID is that a computer can be identified by this number and this is the first stage in building a database of the computer users habits since the user is no longer anonymous.

The second example is Sharman Networks, the creators of Kazaa Media Desktop bundled in software that connected the users to a secondary private network called Altnet which was operated by an affiliated company called Brilliant Digital (Klang 2004b). This system works in the same way as a distributed computing project and takes advantage of the unused processing power in computers where it has been downloaded. According to the company the processing power is used to process the data gathered by the advertisers and to render video and 3-D animated advertisements. However, the network, using the software of unsuspecting Kazaa Media Desktop users without their knowledge could also be used to process large amounts of user profiles. A network such as this steals resources, and abuses the property of the unsuspecting. It also raises security concerns since it allows additional access to the user's computer.

The third example is the Napster like software called Audio Galaxy also included the spyware program from a company called VX26. The software recorded the user's movements and sent the data back to the database which was used for advertising purposes. The interesting issue about the Audio Galaxy case is that it also illustrates the temporary relationships and shifting loyalties of the different companies involved. These temporary relationships can be seen by the fact that Audio Galaxy bundled the VX2 software for a period of 34 days but no longer does so (Klang 2004b). These types of relationships will be discussed further below.

The fourth example is the Gator Corporation, which is, according to their own website, a leader in online behavioural marketing. They create, maintain and distribute software called "Gator" which acts as a digital wallet. Gator also offers users the ability to store personal data and other information which is used to fill in online forms. The advantage to the user is that they no longer need to retype all the information when presented with an online form. This software is bundled with another, called "OfferCompanion". OfferCompanion has also been bundled with peer-to-peer software such as Kazaa. The spyware, OfferCompanion, launches automatically when the user launches the browser program and when the user visits certain web sites the Gator Corporation transmit advertising pop-ups which appear on the screen in front of the desired page. The pop-ups prevent the legitimate page from being viewed in a manner which it was intended since the page is marred by advertising messages.

The fifth example concerns the interesting case of the so-called self-installing toolbar, this can be seen as a variation on the Comet Cursor. The Xupiter is an Internet Explorer toolbar program registered to a Hungarian company called Tempo Internet but has been traced to two Internet businessmen in California (Klang 2004b). Some users have even claimed that it installs itself onto the computer after only visiting certain websites. The software changes the user's startup page to xupiter.com and redirects searches on Internet search engines to xupiter.com and changes security settings. This is important since changing security setting allows more information to be gathered about the computer user. The program attempts to download updates and in certain cases downloads and launches other programs such as gambling games and causes pop-up advertising windows (Klang 2004b). Since many users are unaware that spyware has been installed onto their computers they are not aware that they should uninstall the software. However, if the user is aware that software she installed included spyware it is seldom straightforward removing the spyware. Even if the software, which carried the spyware onto the computer, is removed it does not follow that the spyware is removed.

Spyware Business Model

It is important for software manufacturers to spread their software and also to obtain financing for their work. There is a culture of not paying for goods and services online. Many, if not most, users have come to expect and demand that information, software and services are available at no cost. The traditions of no cost software have been compared with tribal gift economies (Barbook 1998) since there is a tendency to help, share and barter with property in these cultures.

The tradition of no cost software and information has developed into the copyright conflicts taking place today. Entertainment files are being transferred over peer-to-peer networks despite the fact that they are copyrighted. The entertainment industry is attempting to regain control over their traditional marketplaces by persecuting those who aid copyright infringement via technical means (Bowrey 2005). This situation has led many users to attempt to legitimise their infringing actions and call for the demise or radical change of copyright legislation. In discussing the legitimacy of infringing software copyright Nissenbaum (1995) argues both with consequential and deontological arguments that there are some specific cases where infringement is morally permissible. However, whether or not the action of copyright infringement can be justified or not the situation is such that many do not feel that they are doing anything wrong in violating another's copyright or at least they are not deterred by any such emotion.

This desire for free software has led to a loss of revenue and a need for software manufacturers to find alternative incomes. Enter the parasite economy (Cave 2001). To obtain income for their products, popular software can act as a host for other software, carrying it into the computers of users. Popular free software can create channels of revenue by offering themselves as carriers of bundled software. The spyware (or indeed any other software) which travels with the free software pays a minimal fee per download for the service. The total cost paid therefore depends upon the popularity of the downloaded software. The creators of the downloaded software claim that their actions are both legal and driven from economic necessity. Users demand free software, software manufacturers need funding to create more competitive software and marketers need to reach potential customers. Since the users obtain free software, software houses obtain a new source of income and the marketers increase their reach, then one might argue that there should not be any discussion on the evils of spyware. This is, however, an oversimplified interpretation of the situation.

Integrity

Those who are discontented with the position of spyware often evoke the arguments of the privacy and integrity debate. Lacking the international consensus of contract law these users have to argue from a rights based position which is a weaker position since they first have to prove the existence of their position and then argue that theirs is the position more worthy of concern. Online privacy has been discussed for a long time and in many different ways. The most common legal discussion tends to be whether or not there is, or there should be, a right to privacy. If this can be answered in the affirmative the question then becomes one of degree i.e., where do the limits of privacy stand?

In Europe this question has received considerable help in recent years due to the growth of the European Union, which requires the incorporation of the European human rights convention (Convention for the Protection of Human Rights and Fundamental Freedoms – Rome 1950). Prior to the incorporation of the convention into the national legislation of the member states the discussion centred on the creation of a right as opposed to a discussion of positive law. After the incorporation the main thrust of the legal discussion became a positivistic discussion on what should be included in a right to privacy.

The concept of privacy can only be placed in relation to the ability of that privacy to be invaded. Unfortunately the discussions have for a long time focused on either the voluntary submission of data or the use of cookies. Software such as spyware has not been discussed and its appearance and proliferation requires urgent action on the part of the users, software manufacturers and regulators. In the modern privacy debate an influential work is Foucault's (1979) interpretation of the Panopticon. This internalisation of supervision arises from the awareness of constant supervision, or even the threat of constant supervision, and causes the subject to behave differently. The subject must behave in a manner consistent to the fact that she may be observed at any time. This knowledge has the effect of changing the behaviour of the subject in a manner that is incompatible with the concept of human freedom.

Technological advances have brought about the change in the concept of privacy and many would claim that the new technology represents a Panopticon of sorts. While there may be certain elements of truth in this type of discussion this is not the case with spyware. This is due to the fact that the user is unaware that she may be watched and this causes her to behave in a natural and uninhibited manner. This means that tools of supervision installed in the computer through bundled software are more serious than the Panopticon metaphor. In the Panopticon the user is aware that she is being watched and has the choice to behave accordingly but this crucial difference is, in the case of spyware, that the user has no knowledge that her actions may be observed.

Leaving the Panopticon metaphor leaves us more able to understand the need for an increased discussion in the privacy debate. This new technology represents a new challenge to the level of privacy we can expect. The amount of privacy we can reasonably expect is "…a function of the practices and laws of our society and underlying normative principles" (McArthur 2001, p 127). Unfortunately the open public debate on the integrity depriving aspects of spyware has not yet developed enough which has the effect of depriving the law from a worthy basis of discussion and not developing the underlying principles to be able to meet this new challenge. In the face of this vacuum courts may be tempted to fall back upon a familiar pattern of discussion centred on contract law and this leaves the user in a weaker position.

Analysis: Actors

Despite the fundaments of contract law and despite the legality of the business models there appears a level of discontent among those afflicted by the technology. These users are not pacified by the legality of the scheme. They do not agree with the implementation of technology in this clandestine manner for the purposes of invasion of their experienced integrity. In this we can see a connection to the arguments of Habermas (1989) on the relationship between technology and power. This relationship exists in a state of constant evolution and the important issue to be discussed is one of legitimacy. The problem of legitimacy arises when the technology is driven forward in such a way as to exclude a number of users from the socio-legal discourse. Since it can be claimed that it is one of the many roles of law to legitimise actions and create a level of understanding between the citizens and those in power it is important that those who are affected by the technology, and the infrastructure it creates, have the opportunity to partake in an open discussion. When the law is used in such a manner as to silence debate by legitimising actions, which are unwelcome to the users, then one can claim that the law has been used as a pacifier and alienated the users from partaking in the debate.

While attempting to remove the nefarious software may be a complex affair there are software programs which may be useful. Software such as Ad-aware created by Lavasoft and Spybot created by PepiMK Software both can be downloaded free and be used to find and remove the unwanted software. These programs have however given rise to an interesting dilemma. They are not all too open about their methods in defining what spyware is and as such have a large amount of political power in their ability to blacklist programs. Comet Systems Inc claim that they have been unfairly targeted by Lavasoft and their business has suffered because of it (Miles 2002).

The potential of anti-spyware companies to damage the legitimate business interests is a serious threat. Marketing companies claim that they have a right to market their products, software companies need revenues from marketers to be able to provide free software. The whole process is legitimised by contract law. The question therefore may be to what extent the anti-spyware companies are, or should be, liable for their activities.

It is therefore important for the creators of anti-spyware programs to be open about their methodology and their choice of programs that their software removes. The most popular anti-spyware program is reputedly overly covert and silent about their business practice that makes any discussion on openness difficult. For those who are technically adept the whole problem of spyware is an issue of lesser importance but the majority of technology users are happily unaware of how their technology works or how to correct it if it fails to work. This is the group that needs anti-spyware software. This group is usually unaware of the choices made by the programmers of which software to define as spyware and which not to include in this category.

Anti-spyware software, once established, creates for itself the role of gatekeeper since it has the ability to choose which software is to remain on the users computers and which is not. For software developers therefore, the anti-spyware software becomes another barrier that must be respected. Some software developers have attempted to open discussions on the powerful position attained by anti-spyware companies in relation to deciding which advertising is allowed and which is not (Klang 2003b).

Another interesting reaction can be seen in the attempts of the software companies to fight back against the anti-spyware programs. The Radlight17 video playing software, once installed, attempted to remove or disable the Lavasofts Ad-aware program. This action was legitimised in the EULA

> …You are not allowed to use any third party program (e.g. Ad-aware) to uninstall application bundled with RadLight. Such programs will be removed. If you want to uninstall them, you may do so via Add/Remove in Windows' Control Panel.

The EULA text has since been amended with a text describing which types of third party software is bundled into the program and also the fact that it will create a GUID for the computer. It no longer claims the right to remove software installed in the computer. It does however openly explain that the software will be used for marketing purposes. In a text few of their customers will ever read.

Analysis: Structures

As shown in the examples in Chapter 6[25] these types of software are capable of sophisticated surveillance and they have not been introduced into the computer in an open manner. An important issue to discuss therefore is what position software such as this has in the legal system. There are valid claims being made that this is all legal and above board. Those making the claims can be found in both camps of the pro and contra spyware battle. Therefore this section will take its starting point in the examination of this claim since an accurate understanding of the legal position is beneficial to the total discussion of the software and its effects.

The right to privacy is a fundamental right protected both in international conventions[26], European Union directive[27] and national legislation. Despite these structures intended to provide regulation aimed at protecting privacy

[25] See *Theory* in *Integrity* chapter, page 117 *et seq.*

[26] See for example Article 12 of the Universal Declaration of Human Rights, Adopted and proclaimed by General Assembly resolution 217 A (III) of 10 December 1948, or Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms.

[27] Most importantly Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Also, Directive 2002/58/EC on Privacy and Electronic Communications (DPEC).

these types of software present a threat to computer user integrity. In addition to this the software user has seldom had the opportunity to provide informed consent to the software since it has not been introduced into the computer in an open manner. The computer user is often unaware of the surveillance and therefore continues to behave in an open uninhibited manner. Despite legal measures, the legal position of spyware is not clear and there are legal grounds for claiming that the software is legal.

Spyware: Legal Position

The current EU Directive on Privacy and Electronic Communications 2002/58/EC does not define what spyware is or even the scope of spyware. While there may be advantages to such an approach the result is a degree of uncertainty about what types of programs constitutes spyware. The only guide the Directive on Privacy offers is recital 24 which provides that:

> …so-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. (p 9).

This lack of definition causes the users and the regulatory structures to rely heavily upon fundamental regulatory principles. Once such principle is that of contract law, implemented in the case by the end user license agreement (EULA). In contrast certain jurisdictions have defined spyware, one such example is the State of Utah, and have received criticism for its definition as being over-inclusive, in other words including harmless or beneficial software within the scope of the spyware definition.

Since those who claim that the software is legal all tend to focus upon the EULA as a "silver bullet" in resolving the conflict then it is in the re-examination of contracts which we must base this first stage of the discussion. Therefore this section must briefly explore the regulatory structure of the EULA.

Contract theory (Furmston 1996) is taught to most law students in the form of a simplified mythical situation where two people meet. In the meeting, A makes B an offer. In our scenario A offers B the latest widget in technology for the price of 10$. B, after careful thought, agrees to the offer and the contract is formed. Formation means that legally enforceable obligations have been created. The point of formation is usually symbolically celebrated by some ceremony of, e.g., handshakes, nods or applying names on paper. This ceremonial aspect is an important issue in producing evidence that a contract actually has been formed but binding obligations can be formed without the ceremonial aspect. The whole basis of liberal contract theory is the meeting and agreement of the wills of competent individuals.

If B wishes to buy some software from her local computer store the contract is completed when she hands over her money and receives the box, containing the disk, containing the software. However, an interesting thing occurs when B gets home and tears open the shrinkwrap, opens the box and begins to install the software. Out of the box spills lots of documents written in unfriendly complex language. These amendments and additions to the contract are known as shrinkwrap contracts (Rowland & McDonald 2000). B does not need these to install the software so she proceeds to enter the disk into her computer. On the screen she receives many options all of which she must decide whether or not to agree to. One such text, which usually appears in the beginning of the installation, demands that she agree to a larger text to be able to continue. This is known as a clickwrap (Arne & Bosse 2003) and is an evolution of the shrinkwrap and has the power to regulate the contract that B has already entered into. Usually the clickwrap is seen to be more binding than the shrinkwrap since it requires positive actions from the user.

The situation is the same if B had chosen to download free software from the Internet. Supposing B had downloaded the software Kazaa to be able to share music files with all her friends. The text that precedes the installation of the program is binding. The fact that she does not read it, or if she does read it but cannot understand it does not alter the fact that it is binding. So if Kazaa has written that they intend to collect data and send it to the company for marketing purposes B cannot do anything about that – except not install the program.

Naturally the theory of contracts is a simplification used in education to teach students about the basics of law. It is not intended to be the solution or total description of reality. Nor are the challenges created by technology the only situations where flaws in the simplified model of contract theory become more evident. In any large business process there may always be difficulties in discerning when a contract was entered into and what the content of the contract was. To solve this dilemma the myth has been amended with the theories of the shrinkwrap and clickwrap licences as described briefly above. The courts have understood the necessity of these licenses and have reinforced their legality and power over the users.

At first glance the courts acceptance of these licences may seem unduly harsh. The writer of the contract is at an advantage since they have the time to create a contract which best suits their needs. Additionally the advantage is enhanced by the situation that most consumers are not legally trained and, should they read the contract, may not see the disadvantages the contract places them in. However, this situation is true of many contractual situations. Few of us bother to read the contractual terms when renting a video film or a car. There is a great deal of trust placed in the fairness of the overall system (Klang 2001), additionally we see many other people renting cars and video films without problem and therefore we assume the same will be true for us. The courts acceptance of the standard licence is based upon the needs of commerce; the courts acceptance of the shrinkwrap/clickwrap contract is based upon the knowledge that most consumers are not going to read the contractual terms that underpin every train or airplane ticket. In most cases the contracts are not unduly harsh since they have developed over time to suit the contractual situation and the courts acceptance of them is based upon commercial necessity.

It is however, important to note that this is not the same as saying that the shrink/clickwrap licence is enforceable in all situations. There are contract situations were the contracts are not enforced by the courts. In Scandinavian contract law the courts have the power to amend contracts that are unduly harsh on one of the contracting parties. This situation typically occurs when the drafter of the contract has used techniques, such as language and layout, to obfuscate the terms of the contract. Under common law the question may be one of misrepresentation since the spyware is most commonly bundled into another software product and it is not the intention of the user to download the spyware. Under U.K. law, in the case of Spurling v Bradshaw[28], Lord Denning stated that in the use of sweeping exclusion clauses it was necessary to draw the contracting parties' attention to such cases it required something startling. Denning suggested printing in red ink with a red hand pointing to it or something similarly striking which could not be missed. Arguments, such as these, show that the existence of contract is not enough to legitimize any and all content. The red hand argument can be extended for use against the bundling of spyware, especially since the spyware interferes with the peaceful enjoyment of the users' property vis-à-vis the browser and the personal computer. Today we tend to follow what is often referred to as the liberal contract theory and see contract law as an instrument for enforcing promises (Gordley 1991). This view is tempered with the fact that the contract is seen as an agreement

[28] *Spurling (J) Ltd v Bradshaw* (1956), CA. Also in *Thornton v Shoe Lane Parking* [1971] 2 QB 163.

where the wills of the contracting parties are in accord. If we are to view contract law as an enforcement mechanism then the law tends to be weighted in favour of the EULA since this is, at first glance, the contract. However, it is important to remember that the contract should represent an agreement and as such the question of what the parties knew they were agreeing to is vital to the actions of the courts in attempting to decide upon these issues.

Spyware in Court

The courts have already been made aware of spyware, however the issues that have been raised have not be concerned with the privacy aspects of the software and are therefore not helpful to understanding where the legal reasoning should be developing within this field. However, it is interesting to note that the development of spyware related case law is moving ahead in relation to trademark and copyright infringement. While this is helpful for companies hoping to maintain control over their online assets the connection of spyware to trademark and copyright tends to relegate the importance of privacy concerns to a lesser place.

The software of the Gator Corporation[29] caused pop-up advertising to appear on the screen in front of the desired page. These prevented the legitimate page from being viewed in a manner in which it was intended since the page is marred by advertising messages. This prompted 16 online news-publishing organizations to file a lawsuit[30] against Gator claiming trademark and copyright infringement, and unfair enrichment by freeloading on the reputation of the established sites. The court granted a preliminary injunction in July 2002 preventing Gator from causing pop-up advertising on the Plaintiffs websites. In February 2003 the case was settled out of court but unfortunately for the development of jurisprudence in this area the settlement is covered by confidentiality.

The US courts have, however, not been consistent. In June 2003 the court (Tedeschi 2003) granted WhenU's motion to dismiss charges of trademark infringement, unfair competition and copyright infringement. With this the company U-Haul could not prevent WhenU.com from delivering competitors' ads to visitors to U-Haul's site.

[29] Described above in *Spying Technology* page 120 *et seq.*

[30] Washington Post, Newsweek Interactive Co., LLC., *et al.* v The Gator Corporation, Civil Action 02–909-A, U.S. District Court (EDVa).

The Regulatory Approach

The American legal reaction to the problem of Spyware has been to develop the "Spyware Control and Privacy Protection Act of 2001" (hereafter The Spyware Act) intends to control spyware. The Spyware Act requires that manufacturers notify consumers when a product includes this capability, what types of information could be collected, and how to disable it. More importantly The Spyware Act makes it illegal for the programs to transmit user information back to the manufacturers unless the user enables this function and the user has given the collector access to the information. There are exceptions for validating authorized software users, providing technical support, or legal monitoring of computer activity by employers.

However, The Spyware Act has been attacked for not being consumer friendly since despite its good intentions it does not go far enough in controlling the actions of the spyware producers. The Spyware Act follows the ideas set out in the European Data Protection Directive (DPD) in that it divides personal data into two categories: sensitive and non-sensitive. Sensitive data concerns personal data surrounding the data subject's finances, medical history, sexual orientation, lifestyle, political affiliation and race.

This data cannot be collected or used without the data subjects consent. The non-sensitive data, however, is everything else and all information which can be inferred from that information. This includes any and all actions which the software can record from the web and the conclusions which can be drawn from this data. This non-sensitive data can be collected, processed and sold without the data subjects consent. While at first glance this seems to be a reasonable starting point, there is one major drawback. By collecting or recording much, or all, of the information a user obtains via the Internet several inferences can be made about the users, which pertain to their sensitive data, and therefore the division of sensitive and non-sensitive division is no longer useful.

The European legal reaction has been to develop the DPD, which has been enacted in all member states and can be used to criminalise the actions of spyware since the DPD requires that the consent of the user be obtained prior to collection of personal data. While these legislative tools are effective they have been unable to deal with the Internet-based privacy invasions due in part to the fact that the techniques required to monitor and enforce are beyond the power of single, or groups, of states. The member states of the European Union have a strong level of privacy legislation that enables a level of control of the companies dealing with personal data in their businesses. Unfortunately those dealing in personal data collection through spyware are notoriously difficult to locate and tend to shy away from establishing themselves in states where there is a strong privacy enhancing legislation.

In addition to this the Directive 2002/58/EC on Privacy and Electronic Communications (DPEC), lacks a clear definition of spyware. In addition to which, the users right to be informed in accordance with the DPD has been watered down in relation to online information about the purposes of cookies or similar devices:

> Member States shall prohibit the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user without the prior, explicit consent of the subscriber or user concerned. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network. (EU Official Journal 13 June 2002, C. 140E/121).

The weakness of the legislative approach is that it must struggle to obtain a balance of the needs and wants of the different groups in society. After this balanced approach there is the difficulty of enforcing legislation that is limited to nation states in an environment that no longer considers these boundaries to be relevant. It is not that the courts do not have the competence or jurisdiction to rule in a case but rather the question as to whom is behind the software and which corporate entities or private citizens are to be considered to be responsible for the software.

Discussion

The ethical viewpoint of the spyware maker can be summarised by the Friedman's (1993) controversial view of the sole duty of the corporation to maximise profits and benefit the shareholder. This deontological approach however is opposed by the other rule based imperative not to spy upon or cause harm to others. The question of how to resolve this conflict of ethical rules by applying the Kantian humanity principle of not treating people as a means to an end but rather as ends in themselves. If we were to apply this final Kantian principle we can arrive at the conclusion that spyware constitutes a breach of ethical conduct. However if we were to attempt to apply a utilitarian analysis of the situation the ethics of the actors becomes less clear. The inclusion of spyware in free software could be viewed as a necessary evil and the creation and supply of free software creates more happiness or utility than the evil generated. This argument is effectively reinforced by the fact that there is software which can be used to protect the individual from the harms of software. For this argument to be effective the person downloading spyware must be aware both of the consequences of her actions and the availability of counter-measures.

Since it is difficult to clearly state that spyware is inherently immoral, the position of other actors who provide the infrastructure with which the software is spread (for example those who bundle spyware with other software) is even more difficult to ascertain. Despite the difficulties it is possible to state that spyware is often an unwelcome addition to the computer and from the growing popularity anti-spyware software it is possible to surmise that many computer users believe spyware to be wrong.

One interesting question, which the spyware problem opens up, is the question of which is the best method for combating these types of issues. The problem of spyware is relatively new and relatively unknown outside technical forums or privacy forums. While many of these forums may agree that the problem is growing, it remains difficult to see which solutions should be applied to the problem. The use of anti-spyware software is at best a market solution that requires from the users knowledge of the problem and, at least, a working knowledge of where to find the solutions and how to install and use them. The level of information required by the market is therefore reasonably high, especially considering the fact that most Internet users have never even heard of spyware and, even if they had, may not appreciate the importance of defending their privacy. If the users are aware of the problem, and want to resolve it, a new question arises and this is one of understanding which software is the best for their problems. This stage is crucial since the users can download inadequate anti-spyware software or, in the worst case scenario, even more spyware.

Attempting a regulatory approach takes time and a great deal of concerted effort. Habermas argues (1989) that societies are the base for a multitude of pluralistic opinions but only a few ever come to the forefront of the public debate. In ensuring that the debate is maintained in an open environment and that the rules are created in a transparent method it is important that the basis for rules are discussed by those who are effected by them. It is also important however to note in this context that all rules should be held under constant debate (McCormick 1997). Rules should not exist in a closed space but must exist in the open under public scrutiny to avoid the creation of a representative elite whose interpretations of societies needs, or an illusion of public good, control what is developed as a social balance. The user is left therefore with problems on all sides and must therefore attempt a pragmatic approach to the problem. Not using information technology is not a viable option but what is important is that an effort is made by the users to keep up to date with the state of privacy, both technical and legislative. The user must be prepared to use both technical means to protect her own data while participating in a public discourse on the importance of better data legislation.

As has already been shown the nation state is not capable of meeting all the ills on the Internet and protecting its citizens from them but it is important that the nation state creates an environment where the individual has the ability to find information, make informed decisions concerning her privacy and, if so desired, implement technical countermeasures to protect the level of privacy required.

The case of spyware shows that users are concerned with their online privacy and expect a certain level of anonymity in their online communications. Sundström (2001) has also pointed to the importance of integrity and privacy in relation to ICT in the democratic process. This case also shows the way in which users behave when a core value upon which they rely is threatened and the regulatory structures fail to react in an adequate manner to protect them. In this case we see how a niche is created in the market for software manufacturers willing and able to provide software that will resolve or alleviate the problems experienced by the actors. The market-based solution represents the privatisation of regulation in that the regulation is implemented by the user groups through their choice to implement such software.

Conclusion

Spyware is yet another example of how privacy has become the price that computer users pay for their use of the information technology infrastructure. This time the threat comes from software bundled into free software, the problem is that the price the user pays is not one that is discussed or declared openly. The user is therefore not able to enter into an agreement on equal grounds or attempt to negotiate to achieve a better bargain. Contract law is in this scenario pushed to the limits and used as a legitimising factor for unethical business practices.

The form of regulation seen in this chapter is a blend of the *design-based* and *competition-based* (Murray & Scott 2001) forms of regulation. As this case study has shown, the lack of *hierarchical* regulation leads to an opening for *competition-based* regulation to fill this gap. In this specific case the form which *competition-based* regulation has taken is one that uses *design-based* regulation in the form of anti-spyware software.

There are alternatives for the user. She can naturally choose not to use free software but this choice requires knowledge of the integrity threatening software within the free software. Also the choice not to use free software has economic effects and may create barriers to active participation in the information technology infrastructure. There are also possibilities for the user to attempt to eradicate the unwanted software installed into the computer. These types of solutions require an awareness of the problem and a certain level of knowledge on how to find, download, install and run the necessary software. An important issue with these market-based solutions is that their fairness and objectivity have been marred by accusations of injustice and unfair treatment. On the legislative side we, once again, see an example of legislation struggling to enforce local ideas under fire from a global (or a-national) infrastructure. This is becoming a familiar pattern when the national or regional legislation attempts to deal with Internet-based technology. There is no solution to this aspect of the problem other than international legal consensus which is very hard to achieve, implement and enforce. The disruptive effects of technology upon a social balance created over time can have the subtle effect of changing that balance which was created at a prior technological balance. Technological advance demands a renewed discussion on its effects upon the users in society and on the gradual effects of technology on society. This is especially true since a market approach to resolving the issue requires that more information is made available to those who are effected by the problem. Without this information they will be unable to take a stand on whether they desire to protect themselves, and if so, in which manner.

An additional reason for the need for more public debate amongst those concerned is that they are themselves responsible for achieving a re-balancing of the socio-technical regulation. Without information and debate the process of establishing a balance between the effects of technology and the needs of society will cease to be forceful and any meaningful effects such a debate can create will be lost. The focus of regulation should be to maintain the core democratic value of integrity. Within the participatory democracy the need for integrity protection is important to ensure individual participation within the democracy. Without such assurances a supervising gaze is developed, and such a gaze becomes a mechanism of control internalised in the behaviour of the individual preventing her from participating openly and freely in the democratic process. Therefore it is important to ensure that the disruptive effects of technology in relation to integrity do not negate the positive potential of participation through technology.

The process of participating in a democracy requires privacy. The simplest example of the importance of privacy is the secrecy of the ballot box. The voting system is created in such a manner as to insure that even those closest to each other cannot be certain of how the others vote. This integrity is there to ensure democracy. While many could argue that they would not change the way they vote even if they had to do so in public the importance of integrity in democracy is, through this example, easily grasped. Therefore it is strange that when threats to online integrity appear they are not treated with equal importance. The need for integrity is fundamental for the participatory democracy to function even in the online domain and therefore the regulator should be more concerned with protecting this core democratic value than conservatively overprotecting the sanctity of contract.

7

Property

Property is intended to serve life, and no matter how much we surround it with rights and respect, it has no personal being. It is part of the earth man walks on. It is not man.

Martin Luther King

Introduction

A large part of our online interaction takes place within specialised virtual environments. One such environment carries the unwieldy acronym, the massively multiplayer online role-playing game (MMORPG) (Kelly 2004), which can be defined as any online role-playing game where a hundred or more players can play simultaneously in the same environment. MMORPG have quickly become a huge success. The games, such as Ultima Online, Asheron's Call and Everquest have evolved from single player games and text-based multi-user domains (MUD), and they have been created as a way of combining the playing advantages of single player games, strategy games and synchronous social interaction.

To play the game, the player buys the program and installs it on a computer with an Internet connection. Once the installation is complete, the player then logs on to the server and creates an account. Financing the game is done in two stages: first there is the initial fee to buy the software, and then there is a monthly cost to access the game environment. These games cannot be played without access to the game environment. Once the account has been set up, the player then creates a character from a list of choices. These choices can include certain fixed attributes, which the character will then have during the rest of the game – such as hair colour and occupation – and they also have a certain number of features that will change during the game – for example, the character's strength, agility and other vital statistics. From this point on the player enters the online environment and can perform tasks within this world. The limits of the actions of the character are limited or decided by the configurations of the program.

One peculiarity of the MMORPG is the level of interaction that is possible between the players via their online personas. The players often form teams or guilds in which they can help each other with the more difficult tasks inside the game. The guild not only provides help and tips for new players but also a sense of security, since the self-regulatory guild system ensures that the players within the same guild will not cheat each other while trading or cheat within the game to the detriment of fellow guild members. In certain games, the guild is almost a necessity for those who wish to play the game and be unhampered by other players who have managed to manipulate the program and grant their characters powers unintended by the game programmers, such as the power to destroy or kill the characters of other players.

MMORPG's are an established form of social interaction; the phenomenon has created an increased academic interest in online game studies and created several new business models for the companies that create, distribute and maintain the games. The roots of the games can be seen in the interactive worlds of MUDs (Pargman 2000) and chats (Sveningson 2001) where the creation of an online persona becomes strongly connected to the personas reputation.

The goal of this chapter is to study the assets that are created in the MMORPG with special focus on the avatar itself. The reason for this study is that there is a discrepancy between the regulatory structure, which in this case is the MMORPG controller, and the actor, which in this chapter is represented by the player. The fundamental difference of opinion between these two groups concerns the property rights in that which is created online in these virtual environments. The structural regulation formed by contract favours the regulatory structure, many actors disapprove of this balance, and argue that the value created in MMORPG belongs to the actor who actively works to create added value. *This chapter therefore will look at the way in which new environments, such as MMORPGs, challenge existing established principles in property and attempt to re-interpret them to better suit their new environment.*

This case deals with the core democratic value of property (Harris 1996). This case examines the frontiers of intellectual property in that it looks at the conflict that appears in the creation of intellectual property in online environments. The basic disagreement surrounds the ownership of artefacts within massively multiplayer online role playing games (MMORPG). From the traditional point of view these environments are created and controlled by private organisations and the users are regulated by contractual agreement with the private organisation. Among the users there has been a growing belief in that they own their online characters and any artefacts they find within the world. This opinion is widespread among the players but is contrary to the contract. This case shows that there is a growing re-appraisal or negotiation on the way in which intellectual property originating in online environments should be understood. This entails a re-evaluation of the role and concept of property being driven by the users of MMORPG. This is tantamount to a grassroots revolution to see a user-driven re-appraisal of one of the core values in democracy being negotiated in this manner.

Theory

The concept of property is neither static nor easy to define. On one level there is the simple concept of *mine* that every child develops and understands (and every parent attempts to temper with the concept of sharing) on the other hand property is all about exclusive access and not having to share. In addition to this there are discrepancies between what we consider to be ours and what the law protects. Many of our ideas of what can become, and what is, property are founded in the technological standards of the age. Once it becomes technologically viable to do something the law is required to take it into consideration and attempt to incorporate the technologically possible into the property regime.

The development of digital technologies has led to the transfer of much of our creative material from traditional into digital storage formats. This format offers substantial economic and logistical advantages however it also creates an ease in which the products can be duplicated and transferred without permission. These new advantages are testing the boundaries of property regulation. Bringing into question previously resolved social agreements on the limits of property ownership in cultural material and demanding of the legislator a re-appraisal of the values that need to be protected.

Marx (1978 [1844], p 26) defined property, as "…the right of man to property is the right to enjoy his possessions and dispose of the same arbitrarily without regard for other men, independently, from society, the right of selfishness." Whether or not we agree with this property theory is deceptively easy. Property today implies exclusive privilege of the thing in question. Despite the difficulties in attributing property rights to intangible objects, the legal institutions of copyright and patents have been created to create exclusive property–like relationships and grant property rights on certain symbols, images, and intangible matter. This has led to the expansion of property to encompass a larger sphere. That which is owned is no longer simply the item itself but the privileges which it provides to the owner (Harris 1996). One of the most heated areas of conflict within this discussion is the conflict between private property and public domain or the commons (Ostrom 1999). These concepts will be discussed in the next section before we apply them to the digital domain.

The concept of property often is related to the legal relationships between persons in relation to things. These things may be tangible such as real estate or pencils or they may be intangible such as stocks, patents, or software. As in many other areas, the protection offered by the law, and the way in which it is offered varies greatly. The law in relation to property exists in every legal system but the scope and manner in which protection is created and enforced depends very much on the culture, both where and when, in which the legal system was created and developed (Harris 1996).

Common amongst the concept of property law is that it deals with the accumulation, protection, use, and limitation of wealth and therefore has serious repercussions on many other aspects of society. A characteristic of the core European legal systems is the predominance of private ownership. Western legal systems regard individual ownership as the norm, derogations from which must be explained. The legal concept of property in the West is characterized by a tendency to agglomerate in a single legal person, preferably the one who is currently in possession of the thing in question, the exclusive right to possess, privilege to use, and power to convey the thing.

Property is not often seen as a static condition but rather is viewed as a relationship between a person (or persons) who owns, the things that are owned, and actions affected by ownership. The word ownership is not especially clear since it seems to denote a single relationship to that which is owned. In reality ownership is a collection, or bundle, of rights that complement each other and grant to the owner the authority to legitimately enforce conditions. Stated more simply, ownership allows the owner to enjoy, that which is owned and prevent others from similarly enjoying that which is owned.

In addition to this, the owner may grant others the right to enjoy, that which is owned. This permission may be connected to conditions and fees. Under the law today most tangible things may be owned, but there are exceptions (for example hazardous goods, narcotics, wild animals, important waterways) which limit full property rights through specific rules. Intangibles are more complicated under the law. This is not due to any lack of historical or traditional intangible ownership (Sherman & Bently 1999) but is due to the focus on the concept of possession.

Scarcity, Distribution & Justification

The exclusivity of property is one of its salient factors and the interaction between private property and the commons has become one of the more discussed questions within technology law of our day (Boyle 2003) For most people the commons is very strongly connected with the idea of tragedy. Even without ever having read Hardin's (1968) article the idea that commons are a wasteful form of property is something we almost intuitively believe to be true. Hardin's view was that when property was in the hands of a collective group, each individual would act in a manner to maximise her own utility. The result of this, in Hardin's metaphor, was that the pasture owned by all would eventually become over-grazed. The commons could only lead to ruin of the property, or as Hardin puts it:

> Ruin is the destination towards which all men rush, each pursuing his own best interest in a society that believes in the freedom of the commons.

Hardin's position is not without historical predecessors. This line of thought contends that the externality costs are not considered when individuals strive to maximise their own utility. Since theoretically all actors will strive to maximise the optimal short-term strategy is to strive to maximise and therefore the pasture will be lost. Hardin's critics maintain that his theory is flawed since the context within which the commons is located is not considered (Ostrom 1999, Shiva 2002). The high level of social cohesion and trust among the actors ensure that the see beyond the long-term goals. The concept that each actor has only the maximisation of personal utility in mind is also a point that is seen as being a simplistic view of humankind.

The disappearance of the European commons has been called the process of inclosure or enclosure and took place mainly between the 15th and 19th centuries (Gonner 1912). The enclosure movements were partly legitimised by philosophers such as Locke, who believed that idle nature was wasteful and that property could be created by adding labour to wasteland. Property occurred since "...every man has a Property in his own Person. This no Body has any Right to but himself. The Labour of his Body, and the Work of his Hands, we may say, are properly his" (Locke 1960 [1690], p 287-288).

With this the stage was set for the commoditisation of nature. "Whatsoever then he removes out of the State of Nature hath provided, and left it in, he has mixed his Labour with, and joined to it something that is his own, and thereby makes it his Property" (Locke 1960 [1690], p 288). This latter accommodating view on property creation has been used to legitimise the creation of new property rights in both tangibles and intangibles (Hughes 1988).

Recently there has been an awakening of interest in the commons among lawyers working in technology related law. The most active proponent of the concept, Lawrence Lessig, equates the commons with access to infrastructures

> Central park…an extraordinary resource of peacefulness in the center of a city that is anything but; an escape, and refuge, that anyone can take (take, or use) without the permission of anyone else. The public streets…on no one's schedule but your own, you can enter the public streets, and go in any direction you wish. (Lessig 1999a, p 2).

The public domain, according to Lessig, must not only be protected but it must also be created. It is created when people share what they own.

> …we are not interested only in talking about a public domain or in getting legislators to help build a public domain. Our aim is to build a movement of consumers and producers of content…who help build the public domain and, by their work, demonstrate the importance of the public domain to other creativity. (Lessig 2004, pp 283-284).

While the commons may be a notoriously vague term (Boyle 2003) consisting of ideas such as property owned by a group, common access to another's property and un-owned property (wasteland). The term is positively crystal clear in relation to the concept of the public domain. In frustration at not being able to define it clearly the public domain is often referred to as that which is not protected by intellectual property. In other words the term lacks an adequate definition but is often defined by what intellectual property is not. The public domain is our collective culture. It is what makes us who we are and it is the font from which most creative work is collected. The definition of the public domain as that which is not property diminishes its fundamental importance and maintains the myth, or "charming notion" (Litman 1990), that intellectual property is created without context. When the creator removes something from the public domain and presents it as her own the claim is based upon the idea that that which has been created is an original work. It is important that we do not forget that the actual legal interpretation of the criteria of originality is that it is not plagiarism (Litman 1990). While the courts need a baseline from which to award property it is difficult to understand why everything short of verbatim copying can be seen as property.

Social institutions cannot be accepted as they are but always require justification, in the institution of property this is even more acute since the results of the implementation of property may at times be morally objectionable (Waldron 1999). In part justification can be the most efficient management of limited resources as seen above in the tragedy of commons (Hardin 1968). Beyond the criticism presented earlier against Hardin it is important to recognise that the utilitarian argument for property does not address what will be done with those who are not benefiting from the property and indeed how should conflicting needs be addressed Hardin (1986) exemplified with the use of grazing but what of the needs for other groups what would happen if a motorway needed to be built on the grazing land? The utilitarian arguments of Hardin therefore do not always address the needs of all groups.

An issue, which needs to be discussed and regularly reappraised, is the question of the distribution of property since this has a deep impact upon the individuals ability to participate within a social context and a democracy (Harris 1996, Rawls 1999, Waldron 1999). For example political developments may cause a need for reappraisal as seen in the large-scale land redistribution conducted in Mexico and New Zealand (Waldron 1999). Among the innovative modern theories of redistribution we find the Coase (1960) theorem that, ignoring the primary justifications of initial distribution, attempts to settle an efficient distribution of property based upon an economic foundation of utility. Whilst the Coase theorem is innovative the main arguments for property distribution can still be divided into three approaches: The Humean, the Rousseauian and the Lockean (Waldron 1999) these will be briefly reviewed here.

The Humean approach takes its starting point from the premise that people will fight over resources and the distribution of property at any time will "…be arbitrary, driven by force, cunning and luck" (Waldron 1999, p 17). This arbitrary distribution of property based upon power may, at times, become stable and conflict can then subside, to the benefit of society:

> I observe, that it will be for my interest to leave another in the possession of his goods, provided he will act in the same manner in regard to me. He is sensible of a like interest in the regulation of his conduct. When this common sense of interest is mutually express'd, and is known to both, it produces a suitable resolution and behaviour. (Hume 1978 [1739], p 490).

Therefore property distribution becomes legitimised by the mutual recognition of each other's interests in their own property. The point Hume is making is that there is no real advantage to be made in disputing inequalities in property distribution. The real advantages will be made when everyone can rely on the status quo and not have to actively defend their property. For Hume the basic need for justification is not justice but to provide a stable foundation upon which society can build (Waldron 1999).

The Rousseauian differs from the Humean in that where Hume means that society benefits from the legitimisation of status quo Rousseau (1997 [1762]) places the will of the people and the social contract first. Therefore through the social contract the state becomes the expression of the will of the people and therefore if necessary the state has the power to redistribute property if this benefits the people. This redistribution has been criticised for being arbitrary and against freedom (Nozick 1974), however Rawls (1999) is more positive and argues that property distribution cannot be valued in isolation from the context where it is situated and therefore it would not produce the arbitrary results Nozick fears.

Finally we have the Lockean approach to property distribution. Locke (1960 [1690]) disagreed of state regulation on the grounds that the individual was the best judge of what she needed and to Locke there was nothing wrong with the individual using initiative to take what was necessary. Locke espouses occupancy theory (Waldon 1999) in that the legitimisation of ownership comes from the individual who has worked for the property.

> …every man has a Property in his own Person. This no Body has any Right to but himself. The Labour of his Body, and the Work of his Hands, we may say, are properly his. Whatsoever then he removes out of the State of Nature hath provided, and left it in, he has mixed his Labour with, and joined to it something that is his own, and thereby makes it his Property. (Locke 1960 [1690], pp 287-288).

This theory is controversial but has its supporters and has been accepted in particular in relation to intellectual property (Nozick 1974). Therefore once the principal theories and causes of property justification and distribution have been briefly viewed we can proceed to the implementation of this case.

Analysis: Actors

The online character is often seen as a reflection of the offline self and is in literature referred to as the avatar since it is a manifestation of the self in this online world. Avatar is a Sanskrit word that refers to the incarnation of God, but is more commonly used to mean a manifestation of the self. While the initial creation of an avatar is merely a list of choices, which then generates a character by use of sophisticated algorithms, many players tend to develop deeper relationships to the avatars they use. The MMORPG not only involves playing in an online environment but there is also a strong aspect of online cooperation and communication. This cooperation and communication can even be seen as a crucial aspect of the online game, since the successful completion of many situations in which the player will find herself are not possible to complete with only one player. The game also requires that the avatar collects a steady stream of artefacts, which are more and more powerful; without these more powerful artefacts the player will have a difficult time proceeding in the game. The online collaboration also makes the MMORPG a more socially oriented game than any of the computer game predecessors. The online environments are created as complete worlds with their own topologies and cosmologies, which are often reasonably coherent within the confines of the game. For a discussion on the importance, growth and future of MMORPGs, see, for example, Keighley (2002), Kosak (2002) and Krantz (2002).

The development of an avatar from an unskilled, low-level character to a level of skill and strength within the virtual environment requires, above all, a great deal of time and commitment from the player. The more one plays the greater the skill of the avatar. With the improvement of skills comes the greater accumulation of wealth (either in currency or in goods), and with all this follows an improved social standing both within the game and also within any guild the player belongs to or even in any external offline gathering where two or more players meet.

The avatar is therefore not only the physical representation of self within the online environment but also a social being within its own social circle and a corresponding position that follows this social position. Finally, the avatar is an investment. The time spent creating a powerful avatar can be seen as an investment within a social group, but it can also be seen as an investment in monetary terms as well. The fact that MMORPGs have internal economies has been mentioned briefly earlier. Everquest's virtual world 'Norrath', if compared with offline economies, has a gross national product per capita of US$2,266, which makes it more economically sound than China (Castronova 2001). The currencies of online games have been (and some still are) more valuable than the currencies in offline environments.

Outside the game the online currency traded in relation to offline currency, and the avatars themselves and the artefacts they possess can be seen as being economic assets. Trade in these assets has been carried out both within and outside the virtual environment. Trading the in-game assets within the game has almost always taken the form of bartering since no offline money has changed hands.

But this is not the only trade that has been taking place. Much of the trade has been carried out in other, non-gaming, virtual environments such as the online virtual marketplaces like eBay and Yahoo!. The practice of selling artefacts and avatars on online auctions has been seen as a natural part of the game for the players, even though those who buy powerful characters do lack a certain amount of social cachet and are often considered inferior players. This is much the same attitude that old money has towards the nouveau riche.

In 2000, a wizard sold, by online auction, the "Cloak of Flames" he had managed to obtain after successfully vanquishing Lord Nagafen of Norrath. The cloak was sold on eBay for over US$1,000. Others have sold their avatars for prices reaching the thousand-dollar mark and above (Sandoval 2000). It is interesting to note that the virtual world is not free from sexism; male avatars usually fetch higher prices than female avatars (Castronova 2003). In 2001, this practice was stopped by the auction houses. Their rationale for stopping the auctions in virtual merchandise and avatars was their policy of cancelling auctions that may violate intellectual property rights (Sandoval 2001). This issue was quick to spark a debate about who owned the products of the game (Carter 2002, Taylor 2002b, Klang 2004c). Most players felt that they had acquired proprietary rights over their avatars. This right arises, according to the players, not from the actual payment of the software or the monthly subscription fee. The players feel that they have a right to their avatars and the merchandise they collect because of the time they invest in the game (Carter 2002). The legal questions that arise are natural. First, what is it that is being traded? And, second, if that which is being traded can be seen as being property, then to whom does it belong and, finally, which rights do they have over it? The dispute begins with the first question.

Most players who want to trade their avatars claim that they are selling their time while the platform owners[31] claim that they are selling the game manufacturers' own intellectual property. When it comes to artefacts found or bartered within the virtual environment, the defences are the same but the arguments of the players tend to be much weaker.

[31] This term is used to define the group in control of the virtual environment.

If we were only concerned with the law 'as it is', then legal philosophy would never evolve and the needs of the people would never be met. The validity and scope of the end user license agreement (EULA) might easily end this debate, bringing all other complaints to an end. But attempting to end a discussion by simply referring to the fact that the current solution is in line with the law is neither a fruitful nor an interesting discussion. Also, it must be remembered that the EULA can be interpreted by the courts and it is they who will fill it with meaning via their interpretation and understanding of what the EULA really is. Without an active discussion on the role of the EULA, the courts will not have much material with which to interpret the EULA. There is also a final question that must always be posed: What is it that regulation should be? And in this discussion the role of the users is crucial. This issue is too important to be answered less rigorously than it deserves with a condescending remark to read the end user licence agreement.

While positive law (i.e. the written law and the decisions of the courts) is an important tool of the lawyer, it has often come into conflict with the moral rights and obligations of the citizens. In classical terms this is the conflict between positive and natural law. Both the age and the content can be illustrated in the Greek tragedy of Sophocles where Antigone disobeyed King Creon's command and buried her dead brother. When Creon asks her if she broke the law she replies:

> Yes; for it was not Zeus that had published me that edict; not such are the laws set among men by the justice who dwells with the gods below; nor deemed I that thy decrees were of such force, that a mortal could override the unwritten and unfailing statutes of heaven. For their life is not of today or yesterday, but from all time, and no man knows when they were first put forth. (Sophocles 1912 [ca 442 BCE]).

The conflict in the tragedy is the fact that there are worldly laws and there are laws that must be followed since they have a greater standing and supersede the laws of men. Today it is not the laws of any god which one can use to argue a higher obligation and therefore a diminished need to follow positive law. But this does not mean that positive laws take precedence. Today we tend to discuss the rights of individuals as being important enough to stand above written laws enforced within the borders of a single state.

The question is, therefore, can there be a right to ones own avatar? The initial response to a question such as this is that no such right exists; but this is a much too short-sighted answer since rights tend to evolve over time.

The fact that there is no such right now does not mean it cannot evolve. And also the fact that we claim something to be a right does not mean that it will be enforceable – for example, the American Declaration of Independence (1776) declared all men to be equal but did not prevent slavery.

Avatar as Property

What would be the basis of the right to ones own avatar? The first such basis must be found in the discussion of what an avatar is. If we return to the older understanding of the term, we find that in Hinduism it is the incarnation of a deity in a human or animal form. It commonly refers to the ten appearances of Vishnu, who appears to counteract some particular evil in the world. Or, as Lord Krishna tells Arjuna in the Bhagavadgita:

> Whenever there is a decline of righteousness and rise of unrighteousness then I send forth Myself. For the protection of the good, for the destruction of the wicked, and for the establishment of righteousness, I come into being from age to age. (Johnson 1994, Chapter 4).

Within the game avatars are cyborgs, that is to say a combination of the actor and the machine represented in a virtual space (Balkin 2004). Lastowka and Hunter (2004) even consider the possibility that cyborgs have rights since they are representations of humans, with rights, acting in a social context. These contexts often develop community norms that regulate conduct within these contexts. The regulated norms are often controlled and regulated both by the other players, through their avatars, and the platform owners (Balkin 2004).

The Reputation Aspect

While this is an interesting background it may not be applicable here since we are not deities taking on human form – even though in certain role-playing games some may argue against me. One thing that the avatar is, however, is the manifestation of my self in a virtual environment. My self is not only my appearance, even though this is not without weight, but my self is also the sum of my actions. This last point is usually summed up as reputation (Gambetta 1988, Luhmann 1988) and, indeed, the avatar is the focal point of my reputation within the virtual environment.

As in the real world, my reputation is a valuable asset, which I use and abuse at my discretion, but it is not something I can fully control since it is the sum of other people's opinions of me that make up my reputation (Gambetta 1988, Luhmann 1988). If the avatar is a part of my reputation, or if the avatar is the bearer of my reputation within a virtual world, then should it not be protected in the same way as my offline reputation and be part of my assets to be dealt with as I see fit? Human reputation is protected to some extent in most, if not all, jurisdictions and is even protected in Article 12 of the Universal Declaration of Human Rights[32] and Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms. The protection of reputation is therefore a human right, and, in much the same way as the government has an obligation to protect their citizens other rights, there is also an obligation to protect the reputation of its citizens.

The problem is, of course, that the rise of the MMORPG and virtual environments in general has not received the amount of attention they deserve. There is a tendency to look upon these environments as being unimportant and mere playthings not requiring legal protection outside the scope of the protection of the intellectual property of the software manufacturer. Reputation is a key aspect of all virtual environments and will require a more serious legal protection than previously envisaged.

The Speech Aspect

Another important function fulfilled by the avatar is the mode in which one expresses oneself within this world. While there is a difference between expressing oneself and obtaining a right to protected freedom of expression (Schauer 1982), in these environments the full control of ones avatar is essential for the right to control ones speech. It is hardly necessary to point out the massive amount of work that has been done on the importance of free speech in an open society. Yet it is important to underscore the fact that most legislation for the protection of speech only protects the speaker from governmental involvement or persecution.[33]

[32] Conventions are often used to create and defend human rights. E.g. Universal Declaration of Human Rights, Adopted and proclaimed by General Assembly resolution 217 A (III) of 10 December 1948. Article 12: No one shall be subjected…to attacks upon his honour and reputation.

Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No. 11, Rome, 4.XI.1950. Article 10 – Freedom of expression. (1) Everyone has the right to freedom of expression…The exercise of these freedoms…may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society…for the protection of the reputation or rights of others.

[33] Ibid.

Considering the technological realities of the day and the rapid advances in technological development it is an open question as to whether the right to speech will be limited to protection from the involvement of governmental actions. But the question of human rights may one day create the right to ones avatar. But will these rights 'to be left alone' and to 'free expression' also entail a right to treat the avatar as personal property that may be traded? The right to ones own avatar should be an absolute right for a human person since any interference with the right will quickly limit the efficiency with which the avatar can be used in exercising these rights. Therefore, the rights should include a full right to dispose of ones avatar as one feels fit.

The Property Aspect

And, finally, we reach the aspect of property. This is where most arguments on the rights of avatars usually end up. In this case, I would like to take a slightly different approach. I would like to take the starting point of a non EULA-regulated environment. In other words, I would like to explore who owns the avatar if there is no EULA to weigh the arguments so heavily in the favour of the manufacturers.

To be able to discuss this in more depth, we must return to the creation of the avatar. Since the avatar is created out of a, more or less, complex series of settings, the actual avatar cannot be seen as anything other than the output of an equation or programming function. However, the user then has the option of naming the avatar, and this act of providing the avatar with a unique name does entail a certain amount of separate intellectual investment in the avatar.

In the same way as trademarks are protected, so can the avatar be protected. While the act of naming does entail a certain activity that could make the avatar less likely to be a result of the programming, it is still a weak link upon which to claim ownership. An interesting argument can, however, be found in the works of Locke (1960 [1690]) when he writes that the result of an individuals labour should belong to the individual.

If we see the newly created avatar as coming from the state of nature, it is devoid of personality and does not noticeably differ from many other avatars (except in name). The player's use of the avatar can be seen as enjoining the state of nature with ones own labour and, as such, the product of these actions, in this case a more powerful and socially adept avatar, should belong to the player since he is the one who has created it.

The purpose of this section is to attempt to seek a rationale for the right to ones own avatar. The law of intellectual property has reached an interesting point today since in many situations there has been a reversal of position from its origins. Originally, only a limited number of things were protected and the use of most intellectual property was unregulated. Today we see that the situation is the opposite, since the default situation is that most usages of intellectual property are regulated and what is left is only a small area of rights (Lessig 1999). When it comes to the ownership of the avatar, the situation is clearly in the favour of the software manufacturers, but this should not prevent others from finding arguments with which to attempt to rebalance the scales.

Analysis: Structures

While many discussions on the issue of digital property tend to gravitate around the concept of intellectual property, there is a very important issue to be resolved before we can enter into that arena and this is the question of whether or not the property (intellectual or otherwise) belongs to those who wish to sell it.

To be able to answer this, we must look at how the property came into the hands of those who wish to sell it. The first stage is actually a simple contract. And while there is still no actual international consensus on which requirements must be fulfilled for there to be a contract, most jurisdictions agree upon a simple formula when attempting to explain contract law. This is usually referred to as the offer-acceptance model. The idea is that the contract is a reflection of the will of the parties to be bound by contract. Formally, this occurs when one party makes an offer that the other accepts (Furmston 1996).

Leaving aside the differences of opinion as to whether offers are binding (e.g. in Nordic law) or not, whether there needs to be consideration (common law) or not, (civil law) the simple model sketched above is the basis of contract law. In the case of the MMORPG buyer, the first stage of the contract is that he purchases the software and then installs it onto a computer. The buyer then logs onto the site and enters into an agreement to pay a fixed sum each month to access the online game.

However, there is a small part that is usually ignored by the buyer in the rush to commence use of the new game. When the actual installation of the program begins it is usually interrupted by several questions, which the experienced computer user tends to agree to without a second glance. The questions involve technical settings such as where the program shall be located and whether a shortcut shall be placed on the desktop and so on.

Among these questions the EULA (for more on EULA see Chapter 7) makes its appearance. It is usually in the form of a box where the buyer must click on the 'I Agree' icon to be able to install the program onto the computer. The text box containing the licence agreement is not especially interesting and the text is rarely reader friendly. A friendly interpretation of the scenario is that the buyer and manufacturer are in general agreement of what can be done with the software, so the buyer tends to agree to the terms without much ado. In reality the terms are quite harsh. There is no option to negotiate on any of them. The situation is all or nothing. If the user does not wish to agree then the software cannot be installed and attempting to return an opened software CD to a vendor is a harrowing experience.

So the position of the buyer is either to agree, or to lose the money already spent and to not be able to play the game that was bought. What is the position of these agreements in the law? Much has been written on this question (Furmston 1996, Gomulkiewicz & Williamson 1996). The question is usually dealt with theoretically and seen as: the actual terms that appear after the purchase of the CD should not be part of the contract and cannot be binding. This is usually because it is not seen as fair that one contracting part can put himself in a better position after the deal has been done. However, the fact is that the shrinkwrap licence and the clickwrap licence have become standard practice and have been regularly enforced in courts in several jurisdictions.

Therefore this chapter could be at an end here. The EULA is seen as being binding by the courts and, therefore, the situation under the law is clear: if the EULA states that the avatars and artefacts within the MMORPG are the property of the software house and may not be sold, then this is binding to the user. If we were to remain here, the question would not be complex, and to many this is the complete answer of the discussion. This may be regrettable since the many players feel that the situation is not equitable, but it is legal.

Therefore, the question should be posed: Is there a rationale for increasing the scope of protection for the players and should this mean that they have greater rights of which the law should take notice?

The Limits of EULA

Simply because EULAs have been enforced by the courts does not mean that legal systems are prepared to enforce all their terms in all situations. The EULA is an important document since it does more clearly state the obligation of the purchaser or user of the software. The courts apply these licences since they generally reflect the trade practices that are currently in use today. But it is important to remember that these trade practices are not fixed in stone and also the courts still often have the power to interpret these practices in favour of the purchaser should a need to do so arise.

The EULA does not live in a vacuum and comes from a context known to lawyers as adhesion contracts. These are contract terms that are part of the contract without being actually included in the contract text or that have not been discussed during the negotiation. These adhesion contracts are not unusual nor something to be feared (Gomulkiewicz & Williamson 1996). For example, airline tickets are bought without consulting the mass of rules that apply – in this case, the adhesion contract simplifies the negotiating process by standardizing the terms involved.

It is important to remember however, that the adhesion contract does limit the scope of rights available to the parties and as such must be treated with some care. Software companies wishing to ensure that their EULA is applicable should ensure a certain amount of transparency and information in the process of presentation of the EULA. This entails such steps as: (i) making the EULA visible and enabling the user to study the terms in a reasonably easy manner; (ii) any limitation to the rights of the software user should be included as highlighted warnings; (iii) the language must be such as to be comprehendible to the average reader, meaning that a limited number of legalese and unclear terms should be used; (iv) it should be possible for the users to return to the EULA for future reference; (v) uncommon or onerous terms should be highlighted – inclusion of especially harsh terms should even require that the users acknowledge their awareness of the harsher terms (Brown 2002).

As we can see, there is a common thread in all this and that is the act of creating clarity and agreement between the buyer and the seller. Unfortunately, the craft of drafting software contracts and the inclination of those who draft them has moved away from clarity. This has led to the increasing disparity between the contracting parties. The more this trend continues and the more the parties are mismatched in legal power the more likely it will be for the courts to find EULAs to be inequitable.

Looking at EULAs today, we can see that many of the basic rules – which were created to ensure that adhesion contracts are not unduly onerous and surprising to one of the parties – are being ignored. Even a cursory survey among users will show that they do not read the contract terms. Those who read them find them confusing and, as the current situation with avatars shows, they are not in line with what the ordinary user feels to be correct.

The sections of the EULA that particularly limit the rights of the user are not more clearly displayed and as such it is possible for the parties to have an increasingly mismatched concept of their rights and obligations. All these factors create a new scenario where it may be that the courts will eventually limit the power of the EULA. This does not mean that the EULA will not be a very important document in guiding the rights and obligations of all involved, but the lack of transparency and clarity has led to an opening for the courts wishing to curtail the absolute freedoms created by EULAs. This situation becomes even more poignant when the parties involved are mismatched, such as a large software house and an individual consumer.

While there are openings for these kinds of interpretations, the courts have not yet shown a willingness to move in this direction. The American legislators have, however, proven to be more forthright, and in the UCITA (Uniform Computer Information Transactions Act) they legitimized the shrinkwrap licence, creating an even stronger position for the EULA than it had already held (Crotty 2002). The position of the EULA is strong in law and it has yet to be challenged in the manner discussed within this chapter. Until serious challenges to the EULA occur, it will maintain its current strength and must be taken as a starting point in any legal analysis of virtual property.

The whole issue of selling both artefacts and avatars recently came to a head when Blacksnow Interactive sued Mythic Entertainment for unfair business practices and interference with prospective business advantage. Mythic Entertainment is the computer game developer that developed and runs the MMORPG *Dark Age of Camelot*. Blacksnow Interactive specialized in "farming" the online game *Dark Age of Camelot*. Blacksnow's business model consisted of employing low-wage Mexican workers to work three shifts per day in the MMORPG. The work consisted of collecting valuables within the game. The valuables were later sold in online auctions.

In the beginning of 2002, Mythic terminated Blacksnows game accounts and contacted auction sites and requested that they stop dealing in copyrighted material – sites like eBay complied. Mythics actions led Blacksnow to file charges that Mythic was behaving in an anti-competitive manner and was attempting to "exert monopoly-like control over uncopyrightable material".

On 10 May the same year, the District Court of California[34] found that the end user licence agreement (EULA)[35] was valid in this dispute and that, according to the terms of the licence; the dispute was to be settled by arbitration. Since arbitration is a private affair, the terms of the resolution of the conflict are not public knowledge and one can only point out the Blacksnow Interactive no longer trades in artefacts from any online games.

The enforcement of the EULA has led to the demise in large-scale trade in avatars and artefacts. But the interesting issue with the EULA is how enforceable is it and how is it that it can control the activities of the user?

Discussion

Democracy and property theories stem from the 17th century works of philosophers such as Locke and Hume who both argued that the purpose of government was to protect life, liberty and property. The discussions on the distribution and justification of property have been active ever since. The basic premise being that if there were structures to protect property then productive labour would not be worthwhile since there is no way of knowing if someone would simply come and take your property away. Private property ensures that the individual can participate freely and with a degree of autonomy within the democracy. Therefore to ensure the survival of the community private property is necessary and there must be a reliable structure that protects it (Harrison 1995).

The question, which arises within this case, is not whether property is, or is not, a vital component of a democracy but rather when property becomes the private property of an individual – which claim can one use to claim the exclusive right to something? Harris (1996) points to the core of the controversy surrounding property:

> Private property is controversial for the same reason that it is commonly prized. It emphasizes the individuality of the property-holder. A property institution at least confers some private domain over some scarce things, so that the separateness of persons is made evident in the face of collective decision-making. (p 165).

Within the framework of this case the claims are based either upon the concept that labour grants property. This theory, based upon Lockean

[34] *Blacksnow Interactive, et al. v. Mythic Entertainment, Inc.* (2002) SA CV 02-112 GLT (ANx), 10 May.

[35] For more on the EULA see *Spyware: Legal Position* page 127 *et seq.*

thought, is appealing in that it confers a level of recognition onto the individual who worked for or made the property. As this chapter has shown the dispute revolves around the understanding of who developed the property and therefore who can call it theirs. The actors claim that the artefacts found within the virtual environment belong to them since they have struggled and worked hard to find them (Taylor 2002b, Klang 2004c) while the environment providers point both to the fact that the environment is the result of programming and entry into the environment is controlled by contract and therefore the can be no property within the environment which does not belong to them.

Today, the computer software manufacturers have the power and the ability to close down the accounts of any users who are in violation of the EULA. This means that buying or selling an avatar could result in the termination of ones whole account. To many the termination of an account in a computer game does not seem like a harsh punishment. Some would even claim that the players should join the real world instead of spending their time online. This, however, is a very short sighted approach. We are presently drawing up the future of the legal status of avatars, and, at present, the status is that they are to an ever-greater extent falling under the ownership of the software manufacturers. If the situation were only relevant to online games, this would maybe be less important to the larger community; but this is not so.

The growth of MMORPGs has shown that they are here to stay and that they will continue to grow. Another future trend is the development of mobile platforms that allow access to virtual environments. The future will bring a much easier access to virtual environments and maybe even the development of more avatars for more diverse roles.

The more dependent we become on our avatars the more necessary it becomes that they are seen by the law as being an integral extension of the human body in the virtual environment, since they will be the way in which we express ourselves and the way in which others perceive us in the future. This is a development that we must begin to take seriously. Whether or not this requires the creation of a new right, as in the right to ones own avatar, remains to be seen. But what should be understood is that, even without the separate right, the avatar must start to be perceived as the extension of body. This extension of body and rights therein does not affect the software manufacturer. A question that is rarely raised is: For what purpose does the software manufacturer claim to need the rights of ownership in my avatar? Instead of the users needing to explain the rationale for what is an easily understandable reaction, it would be interesting to hear the rationale from the software manufacturers.

The Blacksnow incident has led many to believe that there is not much point in arguing any more. The courts have determined the fate of the avatars, and with legislation like UCITA the situation seems very bleak indeed. But the situation where a company for business purposes cultivated avatars for the express purpose of selling them should not be the reason why no rights can be given to the avatars of private individuals.

Attempting to view the online activities in Humean, Roussean and Lockean terms can further our understanding of the distribution and justification of online property ownership. According to the Humean approach property was taken by whatever means necessary and the best one could hope for was a period of stability where society could develop an acceptance of the status quo in property ownership. This approach would legitimise the role of the platform controllers since they have the power to close of the individual's access to the game. This approach does not disallow that individuals may continue in their attempts to sell online material. The actions of the legal system would not support them since the role of the structure is to maintain the status quo of power. Using Rousseau provides an interesting opening discussion for applying changes to the power relations involved in this discussion. Rousseau allowed for the possibility of property transfer if this was compatible with the will of the majority. This becomes problematic when attempting to define the majority. Is the majority the online game players, society at large, or the game owners? The Lockean approach has been put forward as a support for the position of the player. Here the user invests time and energy into creating something which then can be transferred. We can see clear comparisons to the concept of the fruits of one's labour argument posited by Locke. Therefore both actors and structures can rely on traditional philosophical arguments to support their moral positions. Modern property theory, as exemplified by Coase (1960) would argue for the distribution of property which offers the most in terms of economic returns. In this scenario the most probable conclusion is in favour of the platform owners since allowing the individual to profit from the fruits of her online labour may have a long-term negative effect on the economy of the game as a whole (Castronova 2001).

This conflict of interests concerns that which Balkin (2004) called the freedom to play and the freedom to design. However Balkin's freedom to design entails a large degree of control rather than design. This control takes place to a large extent, as we have seen, through the EULA. However this focus should not exclude the element of social creation and control which takes place among the actors within the virtual environments. The focus of this case has been on the commercialisation of items created or found within the environment and since much of this commercialisation takes place beyond the confines of the game internal community norms become a weak form of social control. However there are examples of this (Balkin 2004). The actors' ability to play and to claim property within the game is experienced by the actors as an important factor the ability of self-regulation and democratic participation among users. While the control exercised by the EULA is understood to be hierarchical and inaccessible from the users point-of-view. The freedom or influence that the actor retains is the ability to leave the community however this cannot be a democratically acceptable alternative.

Conclusion

The MMORPG and similar online environments are providing new places of social interaction and within these places we can see new discussions arising on social issues that have previously been settled. Therefore, in this way, the virtual environments are disruptive in that they demand that we re-interpret established social institutions such as property. The forms of regulation most evident in this chapter are the *design-based* and the *hierarchical* forms of regulation (Murray & Scott 2001). The *design-based* regulation is seen in the way in which the software making up the MMORPG environment can be changed to suit the regulatory needs of the platform owners. This is used together with the application of the EULA as a form of *hierarchical* regulation, which is supported by the courts through the implementation of contract law.

The controllers of these environments have traditionally held the high ground in particular since they have the overall control of the software created environment and are therefore able to implement changes in the software that regulate the behaviour of the actors. The actors, on the other hand, have begun to accept as a rule that the avatar and the artefacts within the game belong to them (Taylor 2002b, Klang 2004c). They have established a strong social practice within their online communities that is proving hard to regulate completely.

The negotiation between the parties has inevitably led to conflicts and attempts to regulate and circumvent such regulation. While the controllers have been reasonably successful in regulating certain types of economic activity, in particular organised attempts to find and sell artefacts, they have been unsuccessful in others (Castronova 2001). This lack of success can probably be seen as the result of the negotiation between the regulators and actors where the regulatory strategies (regulation through code, law, social practice etc) have been an overall failure. One example of the way in which the actors can be said to have managed to redefine the way in which property in this case is viewed is the recent opening of an official online auction site for Everquest, organised and run by Sony.

The rights of actors in virtual environments have to a large extent been explored in online gaming environments however these rules and regulatory procedures are equally applicable in the growing number of virtual environments where actors participate. These include, but are not limited to, online distance learning environments (Svensson 2002), local government (Ranerup 2000) and the corporate intranet (Stenmark 2002). The democratic implications of the regulation of property within these environments will continue to have far reaching implications on the way in which democratic participation is carried out and developed.

With the increase of online interaction follows a heightened interest in the way in which the products of our time therein are shared. This is a relatively new form of social interaction with great potential however a great deal of this potential as a tool for interaction, collaboration and creation will not be able to be used unless there is an equitable method of sharing that which is created in online environments. The present day disruptive effects of interaction via virtual environments have begun to demonstrate the inadequacies in present day property regulation since it tends to discriminate against online participation. To be able to develop online participation to its capacity this must be satisfactorily remedied.

8

Access

The value systems of those with access to power and of those far removed from such access cannot be the same. The viewpoint of the privileged is unlike that of the underprivileged.

Aung San Suu Kyi

Introduction

Another core value in a democracy is the right of access to the social and democratic infrastructure (Åström 2004). The study in case five demonstrates the way in which this right can be problematised within the digital environment. The case concerns the present day distinction between the development rationales for software. The traditional form of software (erroneously referred to as proprietary software) production is based upon an economic rationale. In other words the motivation to make software is to make economic profit from the activity. The last 25 years have seen the growth of politically motivated software development. The latter is an attempt to build a digital infrastructure that grants the user a greater amount of freedom. Through policy documents and technological decisions there is a state bias towards the use of economically developed software. This bias discriminates against the ideologically motivated software developed in society and in certain cases this bias can result in state subvention of individual products, to the detriment of others.

The previous chapter discussed the legal position of property created within online virtual environments. This chapter will study a related problem to software as property – the rights of users to access technological environments. The software contained in most computers can be defined as being proprietary. The term proprietary is misleading but the term has become established and therefore must be recognized. Proprietary refers to the fact that the thing that is proprietary has an owner (a proprietor). Therefore proprietary software is software that belongs to someone. In the case of software property rights are established through copyright. The person or persons who create software have a copyright in their software and are therefore the owners. Even if they choose to give their property away at no cost they remain the copyright holders (in most cases). Therefore all software is, in reality, proprietary.

The term proprietary does not really refer to software which someone has property rights in since almost all software would then be proprietary and the term would lack meaning. The term proprietary means such property where the owner intends to enforce such rights as are granted to him or her by copyright law. The term proprietary software only becomes relevant in relation to such property where the owner does not intend to enforce such property rights as are granted by copyright law.

Free Software, as defined by the Free Software Foundation, is software that can be used, copied, studied, modified and redistributed almost without restriction. Freedom from such restrictions is central to the concept of "Free Software", such that the opposite of Free Software is proprietary software, and not software that is sold for profit, such as commercial software. Free Software may sometimes be known as libre software, FLOSS, or incorrectly as open source software (more on this term later).

To most outsiders the ethics of software is not something usually considered. To most proficient computer users with a passing interest in this question the ethics of software is recognized as one of the fundamental questions in the digital rights area. To most of the latter, terms such as Free Software, open source, and their derivatives (FLOSS, FOSS, Software Freedom) are interchangeable. Choosing one over the other is a matter of taste rather than politics. However, to most insiders the question is not one of taste. There is a fundamental difference between the two areas even if they share a similar root. Free Software is not the same as open source. The two groups differ in their fundamental philosophical approach to software and its importance to society as a whole. This chapter examines the two groups' differing philosophies and explores how their actions have affected software development, access to fundamental software infrastructure and the development of the concept of freedom.

This chapter studies the role of Free Software as a disruptive technology. The disruptive nature of Free Software lies not in its technological development or in the manner in which it is produced, even though the latter has received a great deal of attention (Ljungberg 2000, Williams 2002).

The disruptive nature of Free Software lies in the goal to create an information infrastructure which is freely available (i.e. at no cost) and which the users are free to use in the manner in which they themselves choose. This openly altruistic goal stands in contrast to the traditional incentives for software development.

The disruptive force of this technology was not created by technological means but rather by the express goals of the project founders. These goals have been subsequently enacted in through legal means. In an attempt to free the dependence upon the regulatory structures created by proprietary software the creators of Free Software have taken it upon themselves to create their own software and effectively circumvent the need to be reliant upon proprietary software and its regulatory structures.

This chapter therefore studies the creation of an information infrastructure with the express political goal of being freely available for everyone who wants it, to be used in any way the users desire.

Theory

The philosopher Habermas (1989) is often associated with the term public sphere, which he describes as the realm of conversation and discussion by private individuals on matters of public interest. These conversations and discussions range from the private personal conversations to the open dialogue in the public press. No matter if the topic is personal or public, appreciative or critical, Habermas' posits that the key feature of the public sphere is universal access. This means that entry and exit to the arena of the public sphere should be without constraints and once within the public sphere the communication is free from constraints. Therefore the participants must be free to enter and to render independent judgments and criticisms in the manner that they choose (Habermas 1974).

Habermas' (1989) work on the public sphere is his thesis that under the post-feudal developments of capitalism and the liberal state, the public sphere became a critical in the interaction between society and the state. The fundamental aspect of Habermas' public sphere was its separation from the power of the state and market forces (Habermas 1974). To function, this public sphere was to be freely accessible by all citizens and public debate was to be uncontrolled in both content and format. A well functioning public sphere is, to Habermas, essential to the function of democratic societies. To Habermas the role of the public sphere is primarily a form of public communication and he posits that this role has been under a prolonged decline. This is, to a large extent, due to the commercialisation and privatisation of the public sphere to such an extent that it is unable to serve its function and through this there is a diminishing of democratic communication. Brill (1989) criticises this concept of the diminishing public domain. He argues that there cannot be a slow demise of public sphere communication, as envisaged by Habermas and others, since the public activism and pathos of the public sphere never existed. According to Brill this image of the public sphere is an over-romanticised view of its liveliness and profundity. Yet despite this criticism Brill (1989) acknowledges the importance of open access to the public sphere.

The components of the access to public sphere include (i) physical access, (ii) social access, (iii) access to discussions, and (iv) access to information. (Carr *et al* 1992). These points may be summarised as the ability to participate within the discussion in any form, for the public sphere to be an effective and productive part of a participatory democracy there should be no limitations to access to it. Once the importance of universal access has been established the question of affordance (Norman 1990) must be approached. An affordance is a property of an object, or a feature of the immediate environment, that indicates how to interface with that object or feature. Latour (1992) offers an illustrative example when he discusses the open door and sees that it affords movement across the threshold (Latour 1992). What is important to recognise is that the affordance is a design feature and therefore must be added or assisted. When discussing the physical public spaces in cities Gehl (1994) notes that a number of Scandinavian cities have, through design choices, actively created a public culture where little or none previously existed. The same applies to software. Affordance in software that ensure or support universal access must be designed and supported.

Castells (1996) has posited an alternative approach to the tangible elements of the public sphere. He argues that the urban physical arena of the public sphere is on the verge of becoming an irrelevant. Despite its importance Castells (1996) argues in the past the information technology revolution is moving the public sphere from the physical places within the industrial cities and exchanging their importance with the information networks and network nodes. The elites within this new system will be those who control the networks rather than the physical spaces.

Even in the network society access remains the democratic key. Castells (2001) argues that Internet access is the first step towards overcoming inequality and establishing democracy. This becomes even more apparent in societies where many important social and political activities are mediated by

ICT and the Internet. Castells (2001) realises the importance of equal access to technology as a first step to develop an inclusive society. He recognises that equal access alone will not provide automatic solutions. Equal access to the arena must include social access as well as access to discussions and information.

Mode and Purpose of Production

Classical economics recognises three factors of production: land or natural resources, labour and capital goods (or means of production). While this division remains a rough one, it is still used since no major theory has substantially altered the foundation assumptions of either Marxist or Neoclassical economic theories. Upon entering the post-fordist information age it became clear that communication is an element of production. This change occurs with the commodification of information and its metamorphoses into a necessary part of production. The recognition of this process is described by Williams (1980a):

> As a matter of general theory it is useful to recognize that means of communication are themselves means of production…themselves always socially produced and reproduced…they are not only forms but means of production, since communication and its material means are intrinsic to all distinctively human forms of labour and social organization, thus constituting indispensable elements of both the productive forces and of the social relations of production. (p 50).

If this argument is carried to its conclusion in the context of this case study we can see that programming is the production of an artefact manifested in computer code. The production of this artefact through forms of intellectual labour should be seen as part of the development of both Base (economics) and Superstructure (ideology) (Williams 1980b).

The lines between the factors of production have never been watertight and yet they have become particularly unclear when applied to the forces of production of software. The programmer is the natural resource, the labourer and the means of production. The product that is produced is, like all artefacts (Winner 1985) a product and a manifestation of ideology. In addition to this the software is the base upon which we communicate within an Internet-based society it is the infrastructure of the advanced participatory democracy and as such it should be under constant surveillance to ensure its impartiality.

In *The Cathedral and The Bazaar* (Raymond 1999) the author presents one of the most persistent metaphors software development. The Cathedral represents the commercial model for software development. It is a pregnant imagery of hierarchy, high walls, high priests and secret rites which are all geared to the official release of the final product. Once the product is released it remains under the control of the Cathedral in the sense that only limited forms of use are permitted. Adaptation, exploration and dissemination are not permitted without authorisation.

The Bazaar represents the opposite of this. In Raymond's metaphor it is a flat structure were everyone seems to be in movement. The goal is to release the product early, release it often and allow the user to become part of the production process. To enable this the user is supplied with the tools and the permissions to adapt, explore and disseminate the software without needing additional permission.

Whether a Cathedral ever is so rigid or a Bazaar is ever so free is not important. The important point is that Raymond (1999) is describing two opposing modes of production not fordism and post-fordism but the main difference in the goal of this production methodology is political. The commercial method of production, the Cathedral, is a process developed to manufacture software for profit. The main goal of the Cathedral is not to make software but to make a profit. The alternative model, the Bazaar, has a different goal. The goal is to develop political software. Political in the sense that the software being developed is freely available and it is unhampered by commercial goals. Naturally actors within the Bazaar frequently have commercial interests but the software being developed is left uncontrolled. The rationale for this is that the software is intended to constitute the infrastructural base in society and therefore the lead developers have taken the (political) decision to make the software free.

The Freedom Debate

The formalisation of FSF's philosophy is most clearly stated in the GPL in which the preamble states: "The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change Free Software — to make sure the software is free for all its users." More specifically the freedom envisioned by FSF and formalized in the GPL concerns the so–called four freedoms, which are the freedom to:

a) run the program, for any purpose (freedom 0).

b) study how the program works, and adapt it to your needs (freedom 1). Access to the source code is a precondition for this.

c) redistribute copies so you can help your neighbor (freedom 2).

d) improve the program, and release your improvements to the public, so that the whole community benefits (freedom 3). Access to the source code is a precondition for this.

The Free Software Definition establishes criteria for a program to be considered "free". There is an interesting clarification about the concept of freedom so that the reader will not be confused. Readers are asked to think of "free" in terms of free speech rather than "free beer". Aside from being a rather unique metaphor in the debate on freedom, the free speech/free beer dichotomy adequately captures the conflicts involved in the term "free" in relation to computer software.

The importance of freedom, its attainment and preservation, has been the topic of discussion in every society. However the definitions and contents of freedom vary over time and place. The Stoics' discussions on freedom, for example, are very reminiscent of present day discussion on determinism and free will (Bobzien 2001). Today an accepted systemisation of freedom into negative and positive freedoms, with its roots in Kantian (2003 [1781]) thought, is a popular theoretical construct. The concepts of negative and positive freedom were developed by Berlin (2002 [1969]). Negative freedom is commonly seen as the absence of barriers or constraints that prevent actors from carrying out their wishes or desires. Positive freedom deals with the existence of enabling factors that create the ability for the actor to carry our desires. An alternative approach is to look at negative freedom as external forces on the actor while positive freedom concerns the internal forces affecting the actor.

In terms of state actions the liberal view is one of negative freedom and minimal state interference while those who argue for positive freedom understand that the removal of barriers is not enough to create freedom. Active positive freedom in social terms can be seen when individual freedom is achieved by actively participating in the decision–making processes of society. In its best form, the rules of society are then a reflection of the general will, based upon self–determination. Members of such a society are free only to the extent that they participate in the creation of society (Gauthier 1986).

Those who argue for positive freedom point to the fact that the removal of barriers is too simplistic to create freedom. For example anyone born in the United States can become president. Those who subscribe to negative freedom will point to the fact that there are few or no barriers, while those who argue for positive freedom would point out that despite this lack of barriers no president has been female, openly gay, or from a non-white minority. In other words, the removal of formal barriers is a necessary pre-condition but does not de facto create a larger freedom of action for the individual.

Positive freedom, on the other hand, is criticised for its authoritarian tendencies since it requires the paternalism of other actors to provide for the encouragement of the concept of freedom in others. Additionally, positive freedom carries with it a paradox when dealing with an oppressed minority. No matter how much the minority participates in the decision–making process it will remain oppressed and cannot be seen as free.

An issue, which we have not yet dealt with here, is the role of the actor's desire. In other words, is it the actor or the surroundings that decides whether the situation is free or unfree? Prison is the symbol of lack of freedom. Are perfectly content inmates unfree if all their desires can be fulfilled? The prisoners are, relatively speaking, content and therefore do not suffer from their lack of freedom. Those who espouse positive freedom would therefore conclude that these prisoners are free. Some argue that freedom cannot be limited to what one wants to do but must also include what one might want to do.

In attempting to understand this form of free will, which includes what one might want to do in the future, it is important therefore to understand the actors' motives. Christman (1991) uses the example of women raised in cultures where women are subservient to men. A woman's desire to conform in such a society may be her own desire or it may be a role from which she cannot rebel. Positive freedom theorists would argue that the woman is unfree since her views were formed in an oppressive environment. Most theorists would consider that if the desire to conform is her own, then forcing an alternative view of freedom upon her would not increase her individual sense of freedom (Saul 2003).

There is an alternative approach to this binary definition. We have noted the "freedom to" (positive) and "freedom from" (negative) approach to understanding notions of freedom. Another way of looking at freedom is the so–called triadic model (MacCullum 1967) which states "A (Agent) is (or is not) free from B (Obstacle) to achieve, be, or become C (Goal)." The triadic model was important in showing the error in attempting to distinguish between freedom as the absence of constraint and freedom as the possibility of choice.

In recent years some have argued that freedom is a social relation (Kristjánsson 1996, Kramer 2003) by which they argue that there is a difference in being unable to do certain things and being unfree. Being unable to do things due to natural causes (men cannot give birth, blind cannot see) is not being unfree. However this view of looking at freedom or lack of freedom as dependent upon human acts is troublesome in relation to computer software. The underlying assumption is that non–social causes of a lack of freedom fall outside the scope of interest of philosophers, becoming merely an engineering problem.

However if we ignore discussing notions of freedom in relation to software, we seriously create risks for the future by creating an unfree infrastructure that potentially could be a major hindrance. Future users hence run the risk of being unable to contemplate a scenario where this lost freedom is even an option. This is much the same problem that Orwell (1990) presented where the only meaning of free is to be free from something. Therefore a dog could be free of fleas but the concept of human freedom is incomprehensible. Democratic freedom should not be limited to the possibility of doing things but it should guarantee the possibility of providing the possibility of carrying out acts once a rational well-informed decision has been reached.

Analysis: Actors

Writing about the importance of software is difficult without resorting to what seems to be empty hyperbole. However it is important to point out that software is rapidly becoming one of the most fundamental building blocks of human interaction and activity. Authors such as Negroponte (1996), Mitchell (1996), Castells (1996), and Balkin (1998) have tried to help us understand the way in which software is changing most aspects of our lives. Despite the work these authors there is a common misconception that software is a complex component which in some sense "lives" within computer hardware. By confining software to the inner workings of the computer most non–technical software users are unaware of the extent to which software permeates their lives.

Moglen (1999) writes about computers being under our social skin but this seems to imply that there are computers everywhere. To most people the computer is still a very specific artefact which only affects their lives in specific, controllable situations. Talking less about the computers and more about software may help bring about an understanding of the omnipresence of software. Also, like most other things that surround us, this software belongs to someone. The software that fills our homes and our lives is, in almost all cases, the property of someone else and therefore we are dependent upon the property of others for our everyday lives to a much greater extent that we may previously have imagined.

It was in part to counteract this that Richard Stallman wrote his original announcement for the GNU project in 1983. He wrote "Starting this Thanksgiving I am going to write a complete Unix–compatible software system called GNU (for Gnu's Not Unix), and give it away free to everyone who can use it". In 1985 Stallman launched the Free Software Foundation (FSF), an organisation whose goals it is to promote the computer users' right to use, study, copy, modify, and redistribute computer programs.

The term "Free Software" includes a philosophy, an understanding that software is an important building block in the information society and that the control of this infrastructure needs to remains accessible to all. This egalitarian principle demands that software remain outside the control of those who would limit its usage and only provide this necessary infrastructure at a price. "Free Software" refers not to price but to freedom and it is a deliberately confrontational term (Raymond 1999), an attitude designed to provoke actors with commercial interests in proprietary software.

Stallman was to become the ideological father and leader of the Free Software movement and through this, one of the fundamental ideologists for open source. His views on software were dominant during 1983–1996, after which the focus on ideologically–correct software creation shifted to creating good software (Williams 2002). No longer was it necessary for software to be free to be considered good.

"Open source" was proposed as an alternative to "Free Software". The purpose of launching the term was an attempt to promote open source as a software development model acceptable to corporate developers, those who had been reluctant to adopt a methodology connected to the moniker "Free Software". The definitions of open source were taken from the Debian Free Software Guidelines and adapted during June 1997 in relation to suggestions made during an e–mail conference. After revisions the definition was adopted by the Open Source Initiative (OSI) in February 1998.

Despite the ideological differences between the Free Software and open source movements, Free Software and open source software are most clearly defined by the licences that are approved by the respective organisation (either FSF or OSI). While the purpose of this chapter is to look at the freedom debate, it is important to remain clear that both FSF and OSI refer to the same types of software products and licenses.

In his attempts to establish a software commons Stallman pushed for the creation of a freedom with limitations. While these limitations may be necessary for the creation of the commons they are most definitely limitations. This establishes the paradox at the heart of the Free Software debate which is then confused with notions of free. The use of the word free however is important to those within the FSF since it provides positive reinforcement for the ultimate goal of a commons.

However the OSI have not necessarily chosen a better approach. By abandoning the established path laid out by Stallman, OSI may have appeased commercial interests but they have muddied the philosophical waters of the free/open software movement. Both groups (FSF and OSI) have suffered. Any gain, which may have been achieved by enticing economic cooperation, has occurred at the expense of the original notion of software freedom. While there may now be an increase in open source software, there are fewer debates over some basic philosophical issues. In translating this debate into terms, which are easily comprehensible to commercial actors, we have lost the most important element of the debate — who should own the most fundamental elements of our infrastructure?

Critics of the term “Free Software” argue that the term has many weaknesses and that these weaknesses prevent the movement from gaining the widespread acceptance it both needs and deserves. Their primary concern is over the misleading meanings in the word “free”. The word, according to them, in relation to software means “at no cost”. Despite the free speech/free beer clarification, the term “Free Software” equally applies to all software available at no cost, such as Microsoft Explorer. However both the Free Software Foundation and the Open Source Initiative agree that the Explorer browser is not free in that its code is not widely available.

The problem therefore arises when one attempts to define what Free Software is to the world at large. In many cases computer users have not reflected upon the ownership of software. In relation to software such as Web browsers most computer users tend to consider such software as being free since it is freely available at no cost. In some cases there is no cost but the use of the software is either limited or connected with non–monetary payment (see, for example, Eudora Mail or Opera web browser sponsored mode). The many different financing models of computer software lead to a confusing diversity of software business models all that have the effect of obfuscating the concept of monetary cost for software users.

The accusations of ambiguity have led the FSF to publicise additional material both defending their view and terminology as well as critiquing the

OSI for their lack of precision and for confusing the users (Stallman 2002). The choice of certain users within the Free Software community to start using the term open source was seen as a serious threat to the philosophical basis of Free Software. In 1998 Stallman (2002) wrote:

> The Free Software movement and the Open Source movement are today separate movements with different views and goals, although we can and do work together on some practical projects. (p 55).

The rift between the movements was therefore not so great that they could not cooperate on certain projects but it was serious enough that they no longer could identify ideologically with each other. Both movements are in agreement upon their common enemy that they see as proprietary software. Therefore they share a common enemy but a fundamental difference in how they define themselves and both groups believe it to be important to protect their identity despite the fact that they share a common background. Stallman (2002) continues:

> We are not against the Open Source movement, but we don't want to be lumped in with them. We acknowledge that they have contributed to our community, but we created this community, and we want people to know this. We want people to associate our achievements with our values and our philosophy, not with theirs. We want to be heard, not obscured behind a group with different views. (p 56).

The OSI organisation and terminology was created to meet the needs both of those developers who were disenchanted with the view that software needed to be ideologically pure as opposed to functional and of those developers who were attempting to entice more traditional software manufacturers to join the Free Software/Open Source movements. However, Stallman understood the OSI to be a weakening of a strong moral position in the debate; he appealed to developers not to accept this easy compromise (Williams 2002). Despite Stallman's warnings, the growth and development — both economic and political — of open source has been massive. The creation of the OSI has entailed the creation of an umbrella organisation that has attempted to subsume the FSF. Despite this, the FSF and the GPL still remain the more stringent and philosophically coherent organisation and license.

Political Goals Make Political Artefacts

Within the human rights tradition, it is almost taken for granted that the concept of property is a fundamental part of human freedom.[36] However

[36] Universal Declaration of Human Rights, articles 2 and 17.

the concept of property does not always easily co–exist with freedom. Anarchists, such as Proudhon (1994 [1840]), claim that all property is theft, meaning both that property is a prerequisite for theft and the accumulation of property amounts to theft since it deprives others.

In law, the concept of property (for more on property see Chapter 7) refers to the legal relationships between persons in relation to things. These things may be tangible such as real estate or pencils or they may be intangible such as stocks, patents, or software. As in many other areas, the protection offered by the law and the way in which it is offered varies greatly. The law in relation to property exists in every legal system but the scope and manner in which protection is created and enforced depends very much on the culture, both where and when, in which the legal system was created.

Common amongst the concept of property law is that it deals with the accumulation, protection, use, and limitation of wealth and therefore has serious repercussions on many other aspects of society. A characteristic of the core European legal systems is the predominance of private ownership. Western legal systems regard individual ownership as the norm, derogations from which must be explained. The legal concept of property in the West is characterized by a tendency to agglomerate in a single legal person, preferably the one who is currently in possession of the thing in question, the exclusive right to possess, privilege to use, and power to convey the thing.

As discussed earlier in chapter seven property is not a static condition but should be understood as a relationship between the person (or persons) who owns, that which is owned, and actions affected by ownership. The concept of ownership refers to a bundle of rights that overlap each other and grant the owner the authority to legitimately enforce conditions.

In addition to this, the owner may grant others the right to enjoy that which is owned. This permission may be connected to conditions and fees. Under the law today most tangible things may be owned, but there are exceptions (for example hazardous goods, narcotics, wild animals, important waterways) that limit full property rights through specific rules. Intangibles are more complicated under the law. This is not due to any lack of historical or traditional intangible ownership (Sherman & Bently 1999) but is due to the focus on the concept of possession. Despite this, today the concepts of property have been extended to cover many forms of intangibles. These intangible include software, even though this extension is not without its critics. Moglen (1999) noted that treating software as property has the effect of creating bad software.

Property theory is deceptively easy. Property today implies exclusive privilege of the thing in question. Despite the difficulties in attributing property rights to intangible objects, the legal institutes of copyright and patents have been created to create exclusive property–like relationships and grant property rights on certain symbols, images, and intangible matter. This has led to the expansion of property to encompass a larger sphere. That which is owned is no longer simply the item itself but the privileges that it provides to the owner (Harris 1996).

Copyright prevents the use of a copyrightable object without permission. That which is copyrighted cannot be reproduced in any form. Copyright does not only ensure the owner has exclusive rights to enjoy a property but also ensures that the property cannot be re–created by anyone else — even if this recreation does not diminish the copyright holder's enjoyment. This sentiment was criticised by Thomas Jefferson (1903 [1813]) when he wrote:

> If nature has made any one thing less susceptible than all others of exclusive property, it is the action of the thinking power called an idea, which an individual may exclusively possess as long as he keeps it to himself; but the moment it is divulged, it forces itself into the possession of every one, and the receiver cannot dispossess himself of it. Its peculiar character, too, is that no one possesses the less, because every other possesses the whole of it. He who receives an idea from me, receives instruction himself without lessening mine; as he who lights his taper at mine, receives light without darkening me. That ideas should freely spread from one to another over the globe, for the moral and mutual instruction of man, and improvement of his condition, seems to have been peculiarly and benevolently designed by nature, when she made them, like fire, expansible over all space, without lessening their density in any point, and like the air in which we breathe, move, and have our physical being, incapable of confinement or exclusive appropriation. Inventions then cannot, in nature, be a subject of property. (p 333).

Intellectual property moves beyond control of the physical object that is in itself only the manifestation of that which is protected. Intellectual property controls the way in which property may be used insomuch as it controls all forms of use, even those that do not enrich or harm the original owner. In relation to software this problem becomes more acute since it does not take into consideration the needs of stakeholders such as users and other developers.

The western view of property has led to an increase in the privatisation of commodities, which traditionally were held in a commons. Natural resources necessary for the survival of all within a society have become privatised. An example of this can be seen in the most basic of commodities: water. Traditional and older legal sources hold access to water to be a common right; with the development of more efficient technology, water has become a commodity (Shiva 2002).

The quest of the Free Software Foundation is to create a software commons. This is not about the recreation of something that was free but is now lost but instead the realisation that software is becoming an essential element of the modern world. To lose control of software and to become dependent on the private property of others is tantamount to the loss of water rights, becoming dependent upon the goodwill of others.

The disappearance of the European commons occurred during the 17th century with the enclosure movements. These movements were legitimised by philosophies and property theories such as those put forward by Locke (1960 [1690]), whose view that idle nature was wasteful and the adding of labour to land was enough to create property. With this the stage was set for the commodifiction of nature. Philosopher such as Locke have since then been used to legitimise the creation of new property rights in both tangibles and intangibles.[37]

Today the concept of commons is associated with inefficient and wasteful usage of property - Hardin (1968) goes so far as to ask us to view the commons as a tragic waste of resources. The commons, from Hardin's perspective, are pastures, free for all to use, where cattle graze freely. Under economic theory, individual cattle owners will all strive to maximise their own stock and this will lead to the destruction of the pastures. Hardin sees the commons as a place without rules (legal or social) where all actors strive to maximise their own economic wealth. However, for Hardin's tragedy to occur several assumptions about the commons must be made (Shiva 2002).

Hardin assumes that all human interaction is based upon competition and not cooperation and that property held in commons is unregulated. Communities dependent upon the commons do not have social regulations and that group ownership is an inferior solution.

Analysis: Structures

The structures of interest in this case are two sets of structures. The reason for describing them as two separate regulatory structures is that they both regulate different areas of this disruptive form of software development and dissemination and are controlled by different groups. The first regulatory structures are the licensing agreements under which the Free Software is

[37] For more on property justification see *Scarcity, Distribution & Justification* page 142 *et seq.*

disseminated. This regulatory structure is politics made manifest and since it is set down in a more permanent form and accepted as such it is an actor created form of regulatory structure (Giddens 1986). The second form of structure, which will be briefly discussed here, is the manner in which technology policies are used within state organisations and the way in which such policies form a regulatory bias against political software in favour of commercial software.

Licensing freedom

Licenses are a form of contract, often seen as standard form contracts not requiring parties to actively read and agree with each detail to be valid and enforceable. Licenses are commonly used to grant the licensee the freedom or permission to do something, which without the existence of the license would be wrongful or illegal. Licenses trace their origins in property where the license amounts to permission to enter the land owned by another; additionally they could also grant permission to hunt or remove items from the property. Bare or gratuitous licenses are revocable at the pleasure of the licensor (i.e., the owner of the property who grants the permission). Contractual licenses may be coupled with an interest and may through this interest grant the licensee the ability to enforce the license should the licensor attempt to revoke it. This ability depends upon the terms of the license.[38]

When looking at software licenses it may be of interest to notice the licenses for software often fall into different types: proprietary, academic, reciprocal, standards, and content licenses (Rosen 2004). Proprietary licenses are possibly the most restrictive of all licenses and are commonly used in most commercial software when the source code is not made available. No distribution is permitted for original or derivative works, no license is granted for the user to view, attempt to view, or recreate the code. The term proprietary license is however not exact and variations on what is permitted regularly occur. Despite this, the term has come to reflect the antithesis of software freedom. Academic licenses recognize that many Free Software/open source projects were developed within academia where the main drive was to spread their use. Therefore the users were granted full freedom, provided that they attributed the original to a given academic organisation. The reciprocal license allows the users to use and modify the software provided that all derivatives grant the same freedom to its future

[38] For more on licensing see *Spyware: Legal Position* page 127 *et seq.*

users.[39] Standards licenses attempt to develop and maintain industry standards and require that deviations from industry standards be made public. Content licenses are concerned with ensuring that copyrightable subject matter be made freely available.

The concept of Free Software as envisioned by the Free Software Foundation was not created in a vacuum. The General Public License (GPL) was based upon the concept of reciprocity. The goal of forcing developers to maintain the same amount of freedom has had the effect of creating "free" software that enables future users to continue to develop and expand the amount of software available.

Section 2b of the GPL (version 2) reads "You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License." This means that any software created from the GPL must continue to be offered under the same terms. Moglen (1999) maintains that this clause ensures users always have the best available software. Critics claim that this means that widespread commercial development cannot take place, nor will commercial companies dare to use any part of GPL software in their products. The latter critique has led the GPL to be seen as largely anti–commercial.

Rosen (2004) defines reciprocity as the "…mutual interchange of favors or privileges. Something is reciprocal when it is performed, experienced, or felt on both sides." Both sides of the GPL (licensor and licensee) both use the GPL. However it is interesting to note that the GPL constricts the user since any derivative works must be licensed under the same terms. In a sense the developer is forced to contribute to the commons.[40] The contributor does not contribute freely. If all developers wanted to contribute in this manner to the commons they would not be doing so freely.

The license therefore is a fundamental element of the creation of a commons where software is available. The goal, as stated by Stallman in his original announcement, is to create and expand a software commons. The expansion of the commons is, however, not compatible with the terminology of freedom used both in the name of the organisation and in

[39] Those who dislike the practice term this the viral effect while those who support it prefer the term the vaccination effect.

[40] Alternatively not spreading it at all.

the rhetoric it espouses. The freedom created by the GPL has limitations in relation to price (§2b), patents (§7) and authorship (§10). While many of these limitations are not experienced as limitations since they are part of the Free Software developer's ethos it is important to note that they are limitations. In discussing freedom, we must be careful about confusing freedom with happiness. An unfree person may be happy as easily as a free person is unhappy.

Technology Policies

FOSS is often hailed as being a panacea to especially in reports on its benefits to developing nations three advantages are often cited (Ghosh *et al* 2002), these are low barriers to entry, its advantages as a training system and its role as de facto standard. Often these claims are undisputed when they are applied to developing nations. However there has been a great deal of resistance when attempting to claim the benefits of FOSS to the developed nations of the world (Rejås 2006). The need for commercially developed software to maintain and increase market share leads to a harsh competition for the presentation of facts surrounding software costs.

There are a growing number of national and regional organisations that are becoming interested in promoting the dissemination of FOSS within their organisations. These efforts have often met with resistance and regulators have come to realise that if the implementation of FOSS within governmental bodies is to succeed there is a need to create policies which are either neutral to, or positively discriminate, FOSS. The motivations for such policies vary however the motivation of the Danish Board of Technology (2002) is indicative

> Ordinary market conditions for standard software will tend towards a very small number of suppliers or a monopoly. It will only be possible to achieve competition in such a situation by taking political decisions that assist new market participants in entering the market. (p 5).

The need to be more active towards the promotion of FOSS is not only the economic and market inequalities faced by those who wish to promote FOSS within government. The existing legacy systems are entrenched within the information system environments formal organisation and mindset of the organisations therefore implementing software based upon a new ideology demands an active effort.

When approaching FOSS on a policy level Ghosh *et al* (2002) have identified four approaches (i) Mandating FOSS, (ii) Preferring FOSS, (iii) Mandating Open Standards, and (iv) Best Value. Mandating FOSS is the most radical approach and it has been partially carried out in Brazil and Thailand. Preferring FOSS is much less radical and is easier and less risky to implement. The approach, which has been implemented in South Africa, is flexible and allows case-by-case evaluations to be made. One of the main advantages of mandating open standards is that organisations with such policies can avoid seller lock-ins and path dependencies (David 2000, Hanseth *et al* 1996) enforced by closed standards. This approach breaks the regulatory power of standards and allows the evaluation of new systems. This latter approach has been adopted by the Commonwealth of Massachusetts (USA) and is favoured by the EU. The least harsh policy approach is the best value policy that focuses on the economic calculations presented by sellers and attempts to meet them openly and objectively without prejudice to previous experience.

Sweden has yet to take specific policy decisions but has conducted studies and arrived at the conclusion that the best approach for Sweden would be the use of open standards (Statskontoret 2004). While the Norwegian approach has been much more specific and they have stated that proprietary formats will no longer be acceptable in communication between citizens and government. The eNorway 2009 report states: “Public sector agencies shall apply open standards in their ICT and information systems. Non-adherence to this must be well-founded” and the main goal is that by 2009, “all new ICT and information systems in the public sector shall use open standards” (Ministry of Modernisation 2005).

Discussion

Politically motivated production such as FOSS presents a disruptive mode of software production. Traditional assumptions on the method, motivation and organisation of the production of software are questioned and in this sense the technology represented by FOSS is disruptive. In addition to this FOSS represents many of the core values in the participatory democracy since its ideology, mode of development and product are based on openness and transparency.

The ideological attitudes, which underpin the production of artefacts within a society, are a key element in forming the outcome of these products. Therefore when the ideological base of production is changes it is not surprising that the outcome will also change. Changing the ideological base and creating a disruptive force to change the products does not automatically amount to the acceptance of the new products. Fortier (2001) wrote:

> As the technology continues to evolve rapidly, new technical, organizational, political and legal tools will be needed to bypass and confront the restrictions and agendas on hardware, software and information flows that dominant groups and state authorities are now successfully imposing. (p 106).

The artefacts, which have been produced, need to overcome a long list of resistance to implementation such as lock-in effects and path dependencies (David 2000, Hanseth *et al* 1996), buyer/user tradition or habit, organisational inertia and political strategies. Many governmental organisations have realised the value of FOSS and are attempting to develop strategies to counteract the resistance by implementing policies with goals stretching from the recommending to making FOSS a basic requirement. The commonly cited rationales for governmental interest in FOSS is economic however there are a growing development within policy discussion to go beyond economics and refer to the ideological values inherent in the application of FOSS within government.

The openness with which our political systems are operated is one of the most important instruments of control within a participatory democracy. Sweden has a long tradition of openness through its Offentlighetsprincipen (Freedom of Information) which guarantees citizens access to government information similar instruments whereby actors are legitimised to control the regulatory structures exist in other states but they usually take similar forms since without access to information control is ephemeral. Similar systems of control are being discussed and implemented within the EU as a method for ensuring democratic control.

The importance of the ability to review the activities of public authorities must not be underestimated. The fact that this ability is seldom practiced by the broader public is not important. This regulatory tool works to ensure that public authorities conform to the rules is twofold. Firstly, the fact that people may look goes some way in assuring public administrations self-regulate in a Foucauldian manner (1980) since they are unaware when they may be watched. Secondly there are groups that take an active interest in implementing these rights. Special interest groups and journalists actively use the principles of openness to review the activities of public authority.

As we have previously stated in this work the basic communications infrastructure today is built in computer code. Since it is computer code that creates the infrastructure it is also the underlying principles that form the products and in turn the products form the way in which we interpret and interact with reality (Winner 1985, Latour 1992). Therefore there is a growing public interest in being able to have the ability to control the way in which computer based public decisions are made. This is particularly relevant in situations where legal rules are interpreted through the logical parameters and software code of computer programs – in other words in areas were the public decision making process has become automated (Magnusson Sjöberg 1992).

When applying a functional equivalent approach to the principles of openness there is need to see the basis and methodologies involved in decision making and resource use within public authorities. Therefore, to ensure that the possibility for public review of government activity remains relevant, it is important that policy decisions not be encoded in closed formats and proprietary software.

The Norwegian policy position (above) shows an attempt by public authorities to rid itself proprietary standards and it is presented in a manner which reflects a political and ideological approach to the fundamental understanding of the information infrastructure (Hanseth 1996). The declaration that communications between state and citizen within a participatory democracy illustrate a desire for an open unfettered and non-discriminatory channel of communication which enables a increased access to the information infrastructure controlled by public authorities.

The effects of a lack of political will to efficiently create policies for open standards can be illustrated with an example of a non-critical system based upon non-open standards. The Swedish public service television broadcaster - Sveriges Television (SVT) and the public service radio broadcaster – Sveriges Radio (SR) are separate companies owned by a foundation and entirely funded by licence fees. To ensure impartiality within the public service advertising is not permitted. Due to the position of SVT and SR they contain a wealth of archival material, which is constantly being updated. There has been a great deal of interest in harnessing the communicative power of ICT both in allowing access to archival material and making news and other content accessible online.

In their attempts to achieve this goal the public service in Sweden has chosen to use non-open standards and effectively locked-in themselves and their users to the commercial formats. This creates a discriminatory effect against alternative formats. This technical policy has a far-reaching regulatory effect. The actions of the public service in Sweden are one of marketing and promoting commercial products to the end users, the viewers and listeners. To be able to obtain access to the information infrastructure stored and created by the Swedish public service, the user must use software, which has been developed with a commercial goal and is prevented from using ideologically developed software.

Conclusion

In this case study we have seen that the disruptive effect of technology can have its roots in the development ideology behind the software development. This ideology carries through and affects the finished product, which in turn has effects on the social structures in which the software is implemented. The way in which the software affects the social structures of the environment in which it is implemented created new patterns of use among those dependent upon the information infrastructure. The two forms of regulation seen in this chapter are *community-based* and *design-based* (Murray & Scott 2001) regulation. The *community-based* regulators can be seen in the force of the policy decisions and mindsets of those making technology investments while the design-based regulators are the effects of the lock-in and path dependencies caused by the installed software base. While these may seem to be "soft" regulators in comparison with markets and hierarchies they remain surprisingly resilient and difficult to overcome (Hanseth *et al* 1996).

This case study has concerned itself with the two main ideological software development paradigms – the commercial model and the free model, where the free model represents a disruptive approach to traditional software development. Within FOSS, Stallman's position in the freedom debate arises from a realisation about the necessity of a software commons. However Stallman shares Hardin's flawed views of the commons. The position that freedom is good may be acceptable but freedom cannot be enforced and limited in the way in which the FSF attempts to do. Since users are controlled by the GPL and they are reliant on licenses any freedom that they may have or experience is on the whole illusory. True freedom would allow all to do as they pleased. However, Stallman shares Hardin's view that uncontrolled freedom inevitably leads to ruin. Therefore the commons he creates is not a free one. It offers only limited freedom maintained and controlled by an elite.[41] However this control is not absolute since the individual developer creating the software has the choice to use the license or not.

[41] The GPL is controlled by an elite since only a limited number have the power to affect changes to the GPL.

The way in which we interact in a participatory democracy controls the manner in which the democracy is shaped and develops. Therefore the ability to freely access the infrastructure of communication and interaction in a democracy is vital. This freedom must include the freedom to access in the way one chooses and through the equipment of ones own choice. These decisions are often removed from the traditional discussions of democracy since they are seen as being merely of a technical nature. However as this case, and this thesis, has shown this is to gravely underestimate the importance of technology and the ability of the actors. As the simple example of public service broadcasting in Sweden illustrated, this issue illustrates the root of this thesis: technical regulation is the regulation of democracy.

9

Autonomy

Self-determination, the autonomy of the individual, asserts itself in the right to race his automobile, to handle his power tools, to buy a gun, to communicate to mass audiences his opinion, no matter how ignorant, how aggressive, it may be.

Herbert Marcuse

Introduction

The final core democratic value studied in this work is autonomy (Harrison 1995). In study six the control and censorship of online information is studied. The study looks at the more blatant forms of information control carried out by governments who use technical and social means to openly limit information flows. In addition to this the study also looks at the more subtle forms of controlling online information. The latter are more commonly implemented within less openly repressive governments and can be seen as a delegation of regulatory practices to the service provider. The rationale for the limitation of online communications can be seen in the re-occurring moral panics (Thompson 1998) surrounding technology. Structural regulation of communications through the persistence of paternalistic information policies results in the loss of user autonomy in relation to the online environment. This in turn results in the discrimination of the online communications medium.

Freedom of expression is often pointed to as being a fundamental building block in a democracy (Dahl 1998); therefore the ability to communicate is the basis upon which the democracy is built. This position has been uncontested by most nations for a long time. For most individuals actually communicating with a larger group of people was not practical. Traditional avenues into mass communication are not available to most individuals.

With the advent of ICT the cost of mass communication plummeted. With the growing use of the technology the state position on freedom of communication has been put to the test and many nations are failing this test and not only the ones who traditionally did not support free speech.

Censorship is often a matter of perspectives. The legitimising motivations behind controlling flows of information often lie in paternalistic desires to protect weaker individuals whether they are children or adults. The problem of perspectives is one of cultural relativism in the sense that "we" limit access to information in an effort to defend important cultural values, social stability or avoid harmful content. "They", on the other hand, maliciously prevent individuals from accessing information in an attempt to protect and maintain their own power and position (Esler 2005).

The purpose of this chapter is to present censorship theory and practice in relation to the debate of Internet regulation. The chapter will also present the results of some empirical censorship research and look at the growing anti-censorship movement.

Theory

The concept of autonomy refers to the individual's capacity for self-regulating in practice this includes elements of self-esteem, self-awareness, self-acceptance, self-responsibility, and self-assertion. Against the value of autonomy there are various forms of social paternalism, regulatory structures and outside intervention.

Autonomy is accepted as a core democratic value and it is often argued that in the absence of a compelling evidence to the contrary, everyone should be treated as the best judge of his or her own good or interests (Scanlon 1977, Dahl 1998). Dahl's motivation for defending this point of view is based upon two arguments. First, individuals are the best judges and defenders of their own interests due to epistemic and motivational reasons. In other words, not only do they have the greatest interest in this work but they are also in the unique position of being best able to judge what is best for them. Second is the argument for the interest in self-determination since this involves allowing the actor to be active in following the regulation of his own choosing. This latter argument has a moral strength and also includes a large measure of self-development since it includes the ability to make autonomous decisions, being personally responsible for the outcomes and it requires that the actor engage in free and open discussions with others and thus increases the level of participation in social and regulatory decisions.

The importance of autonomy can be seen in the role and responsibility of the individual to take part in public life and participating actively in the democratic decision making process. Without the ability or inclination to autonomy and self-rule the individual must rely on the technocratic expert (Giddens 1990, Beck 1992) and this reliance undoes the fundament of the participatory democracy. Contemporary philosophical discussions often concern themselves with autonomy in both its theoretical approach and public policy applications (Taylor 1999b). One important area of practical autonomy has been the field of medical ethics where recent changes in the field of patient autonomy have redefined many fundamental medical practices in general and patient doctor communication in particular (Dworkin 1988).

Taylor (1999b) posits two reasons for the central role autonomy plays in contemporary debates. Firstly autonomy becomes the way in which "we structure the world around us" and therefore it becomes fundamental to our understanding of the world and our place within it. Taylor's second reason builds upon the recognition that contemporary western society is morally pluralistic and therefore autonomy becomes the way in which society can ensure that certain groups do not attempt to impose their moral or political views on others. Taylor concludes that this latter argument "…will also, of course, fit well with views that hold pluralism _as such_ to be a good in itself."

In attempting to define the concept of autonomy we are often presented with the problem that the term is used in a manner of ways. Dworkin reflects (1988) that the concept of autonomy is…

> …used sometimes as an equivalent of liberty (positive or negative in Berlin's terminology), sometimes as equivalent to self-rule or sovereignty, sometimes as identical to freedom of the will... It is identified with self-assertion, with critical reflection, with freedom from obligation, with absence of external causation, with knowledge of one's own interests. (p 6).

Dworkin (1988) qualifies the concept of autonomy by listing six criteria which a "satisfactory theory of autonomy" should include (logical consistency, empirical possibility, value conditions, ideological neutrality, normative relevance and judgmental relevance). Autonomy is a complex term and it is possible, according to Dworkin (1988) that no concept of autonomy is rigorous enough to satisfy them all. Dworkin concludes that the abstract concept of autonomy is not one single concept but rather a collective concept of several versions of the idea.

Autonomy can be further problematised by the basic concept of someone being in charge of her life. It is enough, using this argument, that the autonomous person is self-directing or self-governing. In such a limited understanding of autonomy, as a person who acts in accordance with her preferences, does not do justice to the concept (Taylor 1999b). Taylor (1999b) gives the example of the bank teller who under duress gives the banks money to the armed bank robber. This act, in accordance to the person's preferences, is not autonomous. If this was an adequate definition states could coerce their citizens while maintaining the resemblance of autonomy by letting them act according to preferences. One such way of doing this is providing Internet access and the semblance of choice while filtering out unacceptable material before it reaches the user. Therefore acting according to preferences is a too narrow description of autonomy.

Taylor (1999b) presents the concept of autonomy in part as "a person's desire is autonomous if she decides to treat it as being giving her a reason to act, and if she is satisfied with this decision." However he continues, that this may be an incomplete decision since "…person's desires--and their decisions about their desires, and even their feelings of satisfaction concerning them--are susceptible to manipulation." The problem of manipulation must be taken very seriously and can include both the external limitations of choice, the use of marketing and the rewarding of conditioned desires. Therefore it is important to establish the criteria required for an act to be autonomous. Scanlon (1977) pointed out the importance defining criteria for autonomous acts when he argued that autonomous acts in accordance to a persons desire are very similar to being autonomous under coercion. Therefore to be able to discuss what makes a person's acts autonomous one must be able to deal with the autonomy of a person's desire. It is tempting to understand the autonomous act as an act which flows from autonomous desire. Acts are not autonomous simply because they emanate from autonomous desires (Taylor 1999b). Acts under duress or acts where the desire or context has been manipulated cannot be autonomous – even if they in some cases may be perceived as such by the actor.

The main requirement for individual autonomy to be implemented is the ability to communicate. This ability should not be understood to be a one-sided form of communication but it must also include the right and ability to freely receive information. Without the ability to receive information the ability to make decision based upon the facts cannot take place and therefore there will be no real autonomy. To this end the freedom of access to information must occur without the involvement of government since any such involvement affects the information received.

The history of censorship is long and tangled however there are two philosophers which should be addressed in the theory of censorship and these are Milton and Mill. In 1643 the English Parliament issued a law aimed at bringing publishing under government control by creating a number of official censors to whom authors would submit their work for approval prior to publication. In response to this Milton (1979 [1644]) wrote and published his speech Areopagitica without presenting it to the censors, it is unlicensed, unregistered, and without name of printer or publisher. The book carries this maxim on the front page

> This is true liberty, when free-born men,
>
> Having to advise the public, may speak free,
>
> Which he who can, and will, deserves high praise;
>
> Who neither can, nor will, may hold his peace:
>
> What can be juster in a state than this?

Milton's (1979 [1644]) text remains the classic statement of the arguments against censorship, particularly in the form of previous restraint. Milton conceded that criminal prosecutions might, perhaps even should, follow upon the publication of certain writings. He insisted, however, that such works must not be suppressed before publication.

The second work of importance (chronologically) to this all to brief look at censorship theory is *On Liberty* by Mill (1980 [1859]). In this work Mill presented four arguments for allowing free speech and censorship:

1. Perhaps the opinion we would suppress is true
2. Perhaps the opinion we would suppress is partly true
3. We need the false opinion in order to make sure the true opinion is not held as a mere uncontested prejudice
4. We need the false opinion in order to bring home to ourselves the meaning of the true opinion

The basic premise of Mill's argument is that only through discussion could truth emerge and therefore both the individual and society would benefit when many participated in open discussions. The purpose of Mill's arguments were derived from his belief that if there was enough discussion the truth would eventually emerge and therefore it was fundamentally wrong to prevent the expression of ideas even if these ideas were wrong.

Analysis: Actors

In an early work on Internet censorship Varlejs (1998) discussed which actors were carrying out Internet censorship and for which purposes. Listing actors involved in censorship as governments, academic institutions, religious groups, corporations, media and libraries Varlejs (1998) notes that these actors censor different types of information, for different methods and motivate it through different reasons. However the end result was that online censorship was a common feature.

The concept of censorship is most often concerned with activities carried out by the censor after the text has been written but prior to its dissemination. This limitation however fails to take into account both the self-censorship often carried out by those who are too intimidated by threat of legal sanction or social exclusion. Nor does it take into account the activities of a state after the information has been widely disseminated. These two areas are important methods of information control since they act in concert to limit information flows within a society.

The focus of this work is on Internet content and the limitation or control of the free flow of information it is important to be aware of the technologies of information control available to the controller. The first important difference between the traditional censor and Internet-based censorship is that the information in question has usually already been disseminated. Therefore the focus is not on what may be disseminated but rather how to prevent groups from accessing this information. The main process involved in this activity is one of filtering. The term is aptly chosen since the activity involves allowing the free flow of acceptable material while preventing the harmful content from being accessed.

The evasion of censorship has always been a popular topic. One can almost see this as an escalating race of technology. For every move the censor carries out to implement new forms of censorship technologies and techniques there is a rapid move towards new and better forms of hidden communication. The advent of the Internet has increased the amount of cheap international communications being carried out. The race to censor and to beat the censor has been going on for some time but it is still in its infancy.

More or less comprehensive information on how to avoid or evade censorship is easily found online. Much of this information also focuses on the use of pseudonyms and maintaining a level of secrecy to ensure that if communications are intercepted the communicants will not be able to be identified and punished. There are, naturally, two sides to these arguments. The use of such techniques by those who cause harm is abhorrent while the use of these techniques by those who bravely fight for freedom is praiseworthy. However the question then becomes one of degree and definition. Which user causes harm and which users are actually praiseworthy? Much of the activities we deplore today were historically acceptable and vice versa. There is no reason to think that these decisions have been, or ever will be fixed.

Therefore censorship becomes a point of view. Those who are against and those who are for are solely demonstrating differences of opinion and it is only serendipity that puts us on one side of the barrier or the other. This argument from cultural relativism is not an adequate argument to prevent activity on both sides of the fence. Since the concept of censorship can be taken as a point of view several actors have been moving towards creating technical anti-censorship devices. The object of these is to help avoid state censorship without being detected. One example of such a system is Freenet.

Freenet (Clarke & Sandberg 2005) is software designed to enable the publication and retrieval of Internet-based information without fear of censorship and distributed at no cost. This is done by creating a completely decentralised network where information about publishers and consumers of information is anonymous and not stored. The advantages of decentralisation is that no single point controls the network and the advantage of anonymity is that users can depend on the network for communications without fear of advance censorship or post-publishing reprisals. In addition to being encrypted communications are routed through several nodes to make tracking the information requester more complex. According to the project site the software has been downloaded several million times and used in countries with comprehensive censorship systems.

In addition to the development of technical anti-censorship technologies there have been social actions developed to help with censorship evasion. These have taken the form of publications with the activist as a target audience. The goal is to provide readily available information about censorship and how to avoid or mitigate its effects.

The online civil rights organisation Electronic Freedom Frontier (EFF) has produced a guide to ensuring blogging safety which is aimed at ensuring that those who create online information do not meet with negative consequences from employers or state censors. Their advice includes (EFF

2005) using pseudonyms and limiting the use of identifiable information, promoting the use of anonymizing technologies, using ping servers to publish information then quickly removing it (the effect is that the information remains on other servers but not on the publishers site), limiting audiences through password protected sites, avoiding being included in search engines and registering domain names anonymously.

The EFF has a strong reputation for civil liberties work and has been active online since 1990. They have a large audience and deal with a wide range of issues pertaining to online civil liberties. Their motivations for producing such documents are to ensure that the individual can act autonomously in providing and receiving information without fear of outside coercion. They write:

> …we offer a few simple precautions to help you maintain control of your personal privacy so that you can express yourself without facing unjust retaliation. If followed correctly, these protections can save you from embarrassment or just plain weirdness in from of your friends and coworkers. (EFF 2005).

The underlying belief is therefore that the individual should have the choice to publish information but this choice or desire is limited by the potential threats the individual faces if such activities are carried out. The EFF publishes several documents of this nature on their website ranging from legal to technical advice intended to empower the individual and provide tools to ensure individual informed choice. In addition, documents such as this, also fulfil a political purpose by sustaining and contributing to a larger debate on online freedom.

Providing censorship circumvention advice is not limited to organisations. Individuals such as Freerk (2005) maintain sites which describe different forms of online censorship methods and also discusses technologies and provides techniques for circumventing censorship. Freerk is more focused on local censorship (schools, libraries etc) however also discusses circumvention of state censorship. The work is a "tutorial on how to bypass Internet Censorship using Proxies, Shells, JAP" and is intended to be a way in which "to beat the filtering in schools, countries or companies (blocked ports e.t.c)." Freerk (2005) provides no motivation for providing this information.

While the EFF takes the civil liberties stance and individual actors provide information without attempting to place their work in a larger ideological context there have also been moves from traditional (non-Internet) organisations to help circumvent online censorship. One such organisation is Reporters Sans Frontiers (Reporters without borders – RSF). This French organisation focuses on freedom of the press but has also developed an interest in protecting a larger group, namely the non-professional reporter using the Internet to publish and disseminate information online. To this end RSF have published the *Handbook for Bloggers and Cyber-Dissidents* (Pain 2005), an anthology which includes introductory texts on information activism with information on topics such as how to get started, which are the best tools and what ethics bloggers should have. In addition to this the handbook gives example cases of what bloggers have been able to achieve before offering concrete advice on anonymous blogging (Zuckerman 2005) and censorship circumvention (Villeneuve 2005).

Zuckerman (2005) discusses social safety precautions similar to those seen above (EFF 2005) i.e. using pseudonyms, public computers and anonymous proxies before moving on to the more advanced precautions such as union-routing and using anonymous blog services involving encryption, re-routing and anonymous re-mailers. The main point Zuckerman (2005) is attempting to make is that anonymity is possible however for each step there is a cost in time or learning required to be able to use the tools. The trade-off therefore becomes a factor of risk evaluation, knowledge and time. Depending upon the risk being undertaken it may become worthwhile to invest time and energy in learning to use the available tools. Villeneuve's (2005) focus is on circumventing online filters, therefore after a brief introduction to filtering he presents a spectrum of circumventing technologies and a methodology for the user in determining the right balance between the users needs and capacities. The results of such an evaluation determine the course of action and the focus needed for developing circumvention methods and avoiding detection. The choice of circumvention method will be based upon factors, such as, number of users, bandwidth availability, point of access, levels of expertise and the risks being undertaken. Once this has been determined Villenueve (2005) presents an array of web-based circumventors, circumvention through proxy servers, tunnelling and the wide-scale anonymous communications systems.

These examples of instructional texts for activists are by no means exhaustive. Their purpose is to be indicative and demonstrate that the regulatory activities of the censors is being met as a challenge and this has created an interest among actors to aid each other in the evasion of censorship in online environments.

Analysis: Structures

Internet content filtering is the process of preventing user access to information on the Internet. Most filtering systems focus on access to the World Wide Web by software placed between the user and her Internet connection (Zittrain & Edelman 2003). For the most part filtering is dependent upon one of three techniques. However the different techniques can be used in combination to achieve the desired effect. The processes are known as *blacklisting, whitelisting* and *content analysis*. Blacklisting refers to the process whereby lists of unacceptable websites are collected. Once the filtering software is installed the software will first check to make sure any website requested does not occur on the list of websites collected on the blacklist.

Filter	Function
Filter Types	The standalone filter - an all-in-one package supplied by a single vendor. A standalone filter makes all filtering decisions; although there may be a facility to let some users override decisions or ban more sites. The protocol-based filter – provides alternative types of rating systems (e.g. from the American Civil Liberties Union or the Family Research Council) and lets users choose between them.
Filtering Mechanisms	A rating mechanism that makes value judgments categorizing a web site's content. A filtering mechanism which grants access to a web site only after comparison with lists of allowed/disallowed web sites or words
Filtering Techniques	Blocking - uses particular router combinations to deny access to specific Internet Protocol (IP) addresses or services that run on specific port numbers Content analysis - the controlling of information based on the analysis of specific keywords within web pages or URLs. 'Parsing mechanisms' sift through these keywords and block access accordingly. Web sites with forbidden keywords or other specified criteria are blocked from the user

Table 6: Internet Filters adapted from Hamilton (2004).

The use of blacklists entails handing over power and decision making capacity to another agent. Commercial blacklisting products have received a fair amount of criticism for their tendencies to overblock, i.e. to block more access to more information than necessary. A recent study found that in school blocking software "for every web page correctly blocked as advertised, one or more was blocked incorrectly" this was seen as the result of the Children's Internet Protection Act (CIPA) which requires all schools and libraries who receive federal funds or discounts to install and use a technology for blocking visual depictions that are obscene, child pornography or harmful to minors (EFF & OPG 2003). Blacklisting is a commonly used method in many countries. In the UK Operation Cleanfeed (Anonymous 2004, Fagelman 2004) is an attempt among broadband suppliers to self-regulate by blocking access to child-pornography. This project has inspired similar action in Norway and debate in Sweden on the responsibility of the ISP (Eneman 2005).

Blacklisting raises many questions and fears. To avoid creating an interest in the information which is intended to be controlled publicity surrounding the lists is kept to a minimum. It is important to ensure that blacklisting is not used as a methodology to prevent access to acceptable material. The question therefore becomes: If blacklisting is to be used as a legitimate form of information control how can the controlled society ensure that the material being blocked is correct. Blacklisting also creates the need for constant vigilance since the censor is required to keep the blacklists up to date and in line with the growing sources of information to be blocked. This is a daunting, if not impossible, task.

Whitelisting is also, as the name indicates, a process of allowing access to material which has been checked in advance. Instead of creating lists of unacceptable material, whitelisting entails the creation of acceptable material. Users are therefore only permitted access to that which has been approved in advance. This method is infinitely more cost efficient in terms of limiting user access to unwanted information. It also is prone to overblocking, in other words the efficient use of whitelists prevent users from accessing too large amounts of information and thus mitigating the potential of the communications technology.

Seen as a hindrance to access information whitelisting is a much more serious impediment to the free flow of information. If looked at benignly the concept is based upon trust. The information one is allowed to access is in some form “officially approved” by the censor and therefore is reliable, non-harmful and will not lead to negative consequences.

The third form of filtering is content analysis. The concept behind this system is to avoid predefined lists (irrespective of whether they are black or white) and to focus on the actual content of what is viewed. Content analysis works by setting predefined characteristics of the material, which is to be avoided, and allowing software to scan the information for this content prior to delivering it to the user.

If the software is programmed to recognise sexually explicit language and the user attempts to view a page which such content, access to the page will be denied. This system has obvious appeal since it avoids the pitfalls of white & blacklisting (most of over and underblocking respectively). However, the system brings with it problems of its own. Content analysis is not a substitute for understanding information in context. If keywords are used then sites, which have no connection with the words, may be inadvertently affected. For example the city of Scunthorpe has been blocked since the word contains within it a four-letter word. Swedish blocking sites have inadvertently blocked Spanish sites containing the word hora (hour) because the term means prostitute in Swedish. Other content analysis systems intended to block sexually explicit images have been based upon the large amounts of skin-coloured pixels in such images. However these systems have been known to block close up pictures of a non-sexual nature (such as head shots) since the bulk of the image consists of skin-coloured pixels.

State of the art filtering software usually attempt to use a mixture of these three systems and also include a level of human activity to "teach" the filters what to block and what to accept. However as these examples have shown there is no such thing as a system which will not either over- or underblock. Therefore systems will always be either tools of conscious and inadvertent censorship or less than 100% efficient.

In a study conducted by Deibert & Villeneuve (2005) they show online censorship activities being carried out by 22 states. They divide these censorship activities into three categories (1) comprehensive censorship, (2) distributed censorship, and (3) limited censorship. Comprehensive entails a large-scale censorship activity, distributed censorship refers to a significant amount of censorship being carried out, and usually the actual act of censorship is delegated to the ISP. Limited censorship refers to, as the name implies, small amounts of censorship.

While there is a great deal of concern about the states who traditionally censor the Internet such as China, Cuba, Myanmar & Turkey etc there are other states which appear on the list which are traditionally not understood to be censorship states. Such states include the USA, France and Germany. These states rarely receive the same amount of bad publicity for their censorship since it is commonly understood that these states are for freedom of information. However it is easy to see how this stance becomes problematic since even these states censor access to information online.

There seems to be two main approaches among States implementing comprehensive censorship practices. Myanmar and Cuba limit access to Internet by ensuring that only limited numbers of individuals can go online and even those who can may only see approved material – the rest is filtered (Deibert & Villeneuve 2005). China, Saudi Arabia and Turkey are more permissive when it comes to allowing individual's access to the Internet but the content they are allowed to view is heavily filtered (Deibert & Villeneuve 2005). Additionally these countries attempt to register those who access the Internet through Internet Cafés.

Among those who are less ambitious in their filtering activities we find that ISP's, or in the case of the USA libraries, are required to filter different types of content in an effort to protect certain cultural values. Often the filtering is heavily focused on, but not limited to, preventing pornography. The filtering of dissident and human rights sites follows this in a close second place (Deibert & Villeneuve 2005). Those who filter least, according to Deibert & Villeneuve (2005) are countries like France where courts have ordered Yahoo! to block access to Nazi auction sites, Germany in which certain states require ISPs to block Nazi sites and Jordan which blocks the site of arabtimes.com at a national level (Deibert & Villeneuve 2005).

What Deibert & Villeneuve's (2005) study clearly shows is that it has become increasingly difficult to speak of censorship in terms of them and us. Many states, traditionally accepted as pro-free-speech, censor to a lesser or greater degree. That the more traditionally censorship-friendly states such as: Turkey, Cuba and China filter information is not a great surprise. It is important in all these cases to remember that no matter how well planned and organised the system of censorship is – there is no such thing as a perfect system.

Privatised Censorship

While much of the censorship being carried out can be relatively easily understood in terms of a central power controlling the flows of information in the attempt to achieve certain political goals, not all Internet censorship follows this pattern. Two main areas of concern, which fall into the category of private censorship, are the role of the Internet Service Provider (ISP) and legislation with a chilling effect (Boyle 1996).

Censorship by ISP can take many forms, but most generally fall into one of two categories. Either the censorship is carried out as part of a governmental recommendation or requirement or the censorship is undertaken as part of corporate policy – which may in turn be a part of industry self-regulation or simply an individual corporation policy. One example of such as policy is the *Public Pledge of Self-Regulation & Professional Ethics for China Internet Industry*, which states that the principles of self-regulation and the Internet industry's professional ethics include "…patriotic observance of law, equitableness, trustworthiness and honesty" (Article 3). These duties are further expanded in Article 9 of the Public Pledge, which states:

> We Internet information service providers pledge to abide by the state regulations on Internet information service management conscientiously and shall fulfill the following disciplinary obligations in respect of Internet information service:
>
> 1. Refraining from producing, posting or disseminating pernicious information that may jeopardize state security and disrupt social stability, contravene laws and regulations and spread superstition and obscenity. Monitor the information publicized by users on websites according to law and remove the harmful information promptly;
>
> 2. Refraining from establishing links to the websites that contain harmful information so as to ensure that the content of the network information is lawful and healthy;
>
> …
>
> 4. Encouraging people to use the Internet in an ethical way, to enhance the Internet ethical sense and reject the spread of harmful information on the Internet.
>
> 5. If the Internet service provider discovers information which is inconsistent with the law on its website, it will remove it.

The public pledge is written as a one-sided declaration from the corporate actor. This creates the image that the corporate actor has the choice to refrain from signing the document, declaring support for it or implementing it in any manner. However, the non-implementation of the document is understood to bring with it additional difficulties for companies intending to enter the Chinese Internet market. Therefore companies follow the *Public Pledge*, which results in the inspecting and monitoring of national and international sites and blocking access to harmful content as stated by Article 10 of the *Public Pledge.*

> We…pledge to inspect and monitor information on domestic and foreign websites…and refuse access to those websites that disseminate harmful information. (Article 10).

In the case of China many companies are eager to take part in what promises to be a large and potentially profitable market. Therefore many companies are prepared to sign the Public Pledge to gain access to the

Chinese market, among the more notable signatories is the company Yahoo!.

In a recent case at the Changsha Intermediate People's Court of Hunan Province Yahoo! provided information that classified documents where sent via a Yahoo! email account to be posted online on the "Democracy Forum" which was then reposted "…on other foreign web sites such as…'China Democracy & Justice Party"' (Changsha 2005). The court verdict includes the information provided by Yahoo!:

> Account holder information furnished by Yahoo Holdings (Hong Kong) Ltd., which confirms that for IP address 218.76.8.201 at 11:32:17 p.m. on Aprl 20, 2004, the corresponding user information was as follows: user telephone number: 0731-4376362 located at the Contemporary Business News office in Hunan; address: 2F, Building 88, Jianxiang New Village, Kaifu Disrict, Changsha. (Changsha 2005).

The information, which was sent by the account holder was "…the text of an internal message which the authorities had sent to his newspaper warning journalists of the dangers of social destabilisation and risks resulting from the return of certain dissidents on the 15th anniversary of the Tiananmen Square massacre." (RSF 2005). The defendant was sentenced to 10 years imprisonment and two years subsequent deprivation of political rights for illegally providing state secrets to foreign entities (Changsha 2005).

According to RSF (2006) Yahoo! has actively helped jail cyberdissidents by providing Chinese courts with evidence. In a case in 2003 an ex-civil servant from Dazhou was sentenced to eight years in prison in December 10, 2003 for "inciting subversion" the case relied on information provided by Yahoo!. In an article the RSF (2006) call for Yahoo! to provide a list of all cyberdissidents it has provided data on. The RSF are particularly interested in the 81 dissidents whose release they are campaigning for. Paradoxically, when Yahoo! was compelled by the French Courts to prevent access of French Internet users to auction sites for Nazi memorabilia Yahoo! argued that such censorship was unconstitutional (Reidenberg 2001, Vick 2005).

In January 2006 Google launched a local version of its online search engine for China (Google.cn). This version will block "subversive" content from the Chinese users and therefore help Chinese officials to filter Internet content. Especially since to large degree today any website not listed by search-engines has little chance of being found by users. This addition to the Chinese censorship technology has the effect that even sites which are not caught by the Chinese firewalls (Zittrain & Edelman 2003) can now be excluded since they are not part of the material that can be found when using the search engine. Google made several statements in response to the protests over their actions.

> …by launching Google.cn, our website for the People's Republic of China. In order to do so, we have agreed to remove certain sensitive information from our search results. We know that many people are upset about this decision, and frankly, we understand their point of view. This wasn't an easy choice, but in the end, we believe the course of action we've chosen will prove to be the right one.
>
> Launching a Google domain that restricts information in any way isn't a step we took lightly. For several years, we've debated whether entering the Chinese market at this point in history could be consistent with our mission and values….We ultimately reached our decision by asking ourselves which course would most effectively further Google's mission to organize the world's information and make it universally useful and accessible. Or, put simply: how can we provide the greatest access to information to the greatest number of people? (McLaughlin 2006).

The threat to the participatory democracy presented by the privatised censorship of the service providers should not be underestimated. Today the online search engines have become the de facto standard for finding online information and online navigation. However these search engines are not a form of public good. Many consider the search engine as a technology and as such neutral. However this view omits the fact that the technology exists in a corporate context with a duty to create profit (Friedman 1993 [1970]). Despite the search engines role as fundamental infrastructure they are driven by profit motives and therefore no obligation to ensure equal access to information. The effects of privatised censorship are that a greater amount of information becomes unavailable. Once the opposing views are made unavailable what remains online is a form of consensus of opinion. This makes it even more difficult for anyone harbouring an opposing view to speak out. In addition to this the harm of privatised censorship is made more grave by the fact that there is little or no information about the censorship rules, therefore the ordinary user cannot be aware of what is censored and therefore cannot realise when she should attempt to circumvent the censorship.

Another example of voluntary self-regulation can be seen in the UK Project Cleanfeed Initiative (Anonymous 2004, Fagelman 2004). This project involves the largest broadband provider in the UK and entails a process of filtering to prevent access to child pornography sites. These actions have led other countries to follow suit or to discuss similar action (Eneman 2005). Often these forms of self-regulation are an attempt to anticipate actual state legislation in the field.

The second category of private censorship is the case of regulation with so called chilling effects, in other words the stated purpose of the regulation is not to limit a certain action (such as free speech) but has that as a negative side effect. This may sometimes fall outside the strict definition of censorship, however the effect of legislation, which prevents the ability of communication, it results in the lessened flows of free information. While it is important to mention this topic here, due to space constraints it is not possible to give the topic the attention it truly deserves. Many different bodies of legislative rules may affect the way in which communication is carried out. Those that are most common are privacy (Taylor 2002a), defamation (Dent & Kenyon 2004), copyrights (Heins 2003) and trademarks (Dogan & Lemley 2004). The importance of bringing up the topic of the chilling effects of legislation is to underline the difficulties that the communicator faces. The problem is not in the rules but in their interpretation and implementation. When taken at face value the regulations do not vary greatly. However their implementation can easily be implemented in such a manner as to entirely prevent or cause a chilling effect on the actors.

Discussion

Once again (see chapter 8) the concept of the public sphere must be addressed. To briefly recap the concept as developed by Habermas (1989) the public sphere is the realm of interaction and discussion by private individuals on matters of public interest. The key feature of the public sphere is universal access which means that there shall be no control or manipulation of the individual's ability to enter or exit the public sphere. The autonomous individual must be able to freely participate and communicate to be able to be considered an autonomous individual (Habermas 1974).

As presented earlier in this work the components defining access to public sphere include (i) physical access, (ii) social access, (iii) access to discussions, and (iv) access to information (Carr *et al* 1992). Castells (1996) presents the idea that the public sphere has, to all intents and purposes, moved from the physical world to the network. Therefore it is important to look to those writers who claim that the Internet is the public sphere and then to attempt to understand whether or not the same rules apply to the autonomous participant.

Part of the criticism towards Habermas' idea of the public sphere is that during the period upon which his study was based a large part of the population was excluded from entry into the public sphere. The sphere was dominated by white, property owning males and western ideals (Schuler 2000). A discussion within the Computer Science discipline, which is directed at alleviating this problem, has come to be known as the digital divide. Within this field there is an idea that technology can provide the means for leveling the playing field and allowing previously communications-weak actors access to the public sphere. With this access they have the opportunity of fulfilling the goal to becoming autonomous. However if this level of autonomy is to be reached there is a need for the individuals to have an unrestricted, and therefore unbiased, access to this public sphere. This is not the case since many individuals access to the Internet is effected by state interference (Boas & Kalathil 2003, Zittrain & Edelman 2002, 2003).

For the control and limitation of information ICT is a disruptive technology. The studies seen in this chapter have shown that many countries are prepared to move directly to regulate citizen communication. This regulation has created a reaction from the actors in that they are creating technical and social systems aimed at circumventing or mitigating the effects of Internet censorship.

The interaction between the regulatory structure and the actor can be understood as a series of actions and reactions. The first stage is the implementation of ICT as a form of communication. At an early stage this is uncontroversial since the number of users is relatively low and social control can be maintained. The increased dissemination of communications technology leads to a perceived threat of what this communications can entail. Real or imagined threats create a need to protect certain values such as local culture and citizens; decrease foreign influence; protect political stability; maintain security, protect secrets, morals and religion (Varlejs 1998).

Certain actors will perceive the censorship as paternalistic and a threat to their autonomy and therefore strive to counteract it in some form. It is at this stage we can see the development of a clear interaction between the regulatory structure and the disaffected actor. Actors will actively counteract the regulatory structure and force it to maintain a high level of vigilance to enable it to function. The effect will be a constant move to develop socio-technical systems of more adequate policing and intervention.

This is the continued negotiation between regulation and technology. This may deal with the adaptation of social behaviour (or implementation of technologies) to coincide with regulation or attempts to evade the effects/sanctions prescribed by regulation or the behaviour of following the wording of the legislation while ignoring its substance. These negotiated socio-technical solutions attempt to either circumvent regulation completely or at least to cushion its effects.

One of the direct effects of the terror attacks of 9/11 has been the direct limitation of online civil liberties. Since then several governments have moved to implement and extend anti-terror regulation. Hamilton (2003) defines three main areas were these activities are taking place (1) the creation of a data retention structure, both at national levels and also through international co-operation. This entails the mandatory requirement that Internet Service Providers (ISP) store all user data for specific periods of time. (2) Online surveillance – regulation in this area is making surveillance technically possible and formally easier. (3) Direct censorship – on the grounds that "terrorists should not be able freely access sensitive information…" (Hamilton 2004, p 185).

Conclusion

ICT carries with it many promises for democracy. Early voices hailed it as the ultimate tool of freedom. However technology is also being implemented to limit the scope of freedom of expression among ICT users. The theoretical approach to the concept of regulating Internet is developing from a polarised into a nuanced understanding of the complexity of Internet regulation.

In this case we see three regulators interacting to control user access to information. These are *design-based*, *community-based* and *hierarchical* regulators. The design-based regulators refer to the filtering software employed to block user access, the community-based regulators are the "soft" voluntary policy documents which corporate entities choose to enforce while the *hierarchical* regulators are the legal actions with both intended and unintended consequences.

The present situation is one where many parties are conducting the regulation of online communications – the states are attempting to maintain traditional control structures while users are helping each other communicate and circumvent controls that prevent communication. The most efficient state strategy remains one of controlling access to the technology in general and open communication via the Internet in particular.

The issue is one of user autonomy in online environments. The ability to act without coercion or manipulation is vital to democratic participation. This is true even in the online environment. By implementing direct control over Internet content through online content filtering or implementing regulations through industry codes of conducts which require such filtering to be carried out by private actors directly impacts online autonomy. The same can be said of the actions of search engines such as the case of Google.cn, mentioned above, since removing information from the search engines effectively makes the information invisible to the larger public. If the information is not available through search engines it is, for all intents and purposes, not there at all. Without the ability to locate and gather information the individual cannot acquire the adequate information necessary to make autonomous decisions based upon the facts. Therefore through manipulation the public information sphere cannot function.

In addition to this there is a large degree of coercion evident in the examples of search engines and other ISP's facilitating for regulators by providing evidence of technology use. Without the ability to use the technology necessary to enter the public sphere users cannot participate as autonomous individuals in the public sphere. This therefore creates a system of imbalance where the online technological world is discriminated against.

The promise of efficient communications and the development of the Internet into a public sphere without the limitations inherent in Habermas' model have quickly been proven to be false hopes. Reactions to censorship have caused many to both protest and react towards the threats against online autonomy. These reactions come both in technical solutions and in attempts to educate users on the importance of security and risk awareness to prevent autonomy loss.

This chapter has presented a brief overview of censorship and regulation theory. It has identified the roles of some of the main actors involved in the online censorship discourse. ICT has become a disruptive technology with an un-stabilising effect on the status quo of state controlled information flows. In response to this, states have reacted to ensure that the balance of power remains in their favour. In the meantime the user-based response ensures that state activity will not be unhampered nor take place outside the sphere of public knowledge. This chapter has also addressed the role of censorship conducted by private actors (Internet Service Providers) showing how their regulatory actions present a serious threat to the online autonomy and the participatory democracy.

10

Discussion

Our Age of Anxiety is, in great part, the result of trying to do today's jobs with yesterday's tools.

Marshall McLuhan

The purpose of studying the democratic effects of the regulation of disruptive technology is not to provide a list of woes. The purpose is rather to provide a body of work from which positive implications can be drawn. It is important neither to neglect nor to belittle these consequences. In those cases where the unintended effects are small one should consider the cumulative effect upon democracy of several small consequences.

To these ends the data collected in the cases in this work have been collected into multiple case studies. This allows an in-depth examination of a single area of interest. This approach provides a systematic way of looking at the phenomena of regulation of Internet-based behaviour by collecting and analyzing data, reporting results and providing conclusions. The end result of this work, through the use of multiple case studies is to arrive at an understanding of the studied phenomena.

The contributions of this work are aimed at the e-democracy, regulation and disruptive technology research fields, in particular to the specific discussions on the role, methods and effects of regulation disruptive technology and its effects on e-democracy. The topic of the regulation of Internet-based activity is growing in importance, as is the field of e-democracy, this is due in part to the growth of online interaction in addition to participation mediated by other forms of technology. To understand how the regulation of technology affects the regulation of IT-based participatory democracy this thesis has studied the regulatory activities of the regulator and the reactions of those being regulated. The driving force is the understanding of the effect of technological change upon social institutions. This work examines the technological challenges to central social institutions and shows that the technological change has far outpaced the evolution of the social concepts in these areas; a result is that technology can be viewed as being a disruptive force in society. The understanding of the concept of disruption within this work is important. Disruption is a force of change in society. Change is a semi-autonomous driving force in society brought about by disruption. Change is semi-autonomous since it rarely can be ignored or avoided. It is however only semi-autonomous since it is driven by technical, social, political, etc developments for which we are responsible (Winner 1978). Therefore, disruption is a motor of change, change is what pushes, or pulls, society forward.

However the understanding of the role of ICT in the development of society is anything but straightforward. Almost in direct opposition to Winner (1978) Beniger puts forward the self-described "unfashionable opinion" in 1986 that there was nothing fundamentally new about ICT. It was only a logical continuation of the "control revolution" (Beniger 1986). This revolution is

> …a complex of rapid changes in the technological and economic arrangements by which information is collected, stored, processed, and communicated, and through which formal or programmed decisions might effect societal control. From its origins in the last decades of the nineteenth century, the Control Revolution has continued unabated, and recently it has been accelerated by the development of microprocessing technologies. (Beniger 1986, p 427).

Understood in this manner the changes being experienced are not unexpected but merely a progression for a complex society's need to control its environments. Therefore it is not technology that develops but society and with it a need for more suitable technology. Beniger's (1986) answer remains centralisation and control through bureaucracy. An advantage of Beniger's approach is that society should not need to treat new technology any differently from existing technology.

McLuhan (1964) criticised approaches such as Beniger's (1986) as being rear-view mirror approaches to understanding technology. This is the attempt to understand the future by looking at the past. Such approaches would claim that the light bulb is simply a better candle or a car is simply a better horse-and-carriage. The rear-view mirror approach fails to take into consideration the social changes brought about by the technology. Even if we can see similarities between the old and the new, the sheer scale of adoption of Internet-based technology ensures that even if the differences between old and new were small – these differences are magnified through the scale of use in society.

In an attempt to bring about social debate on the democratic impact of technological advances Winner (1986) sees a need for the creation of wider discussion arenas that would be employed prior to the development of technological systems. The discussion of technological merits would no longer be focused solely on the economically profitable or technologically expedient but would include democratic considerations.

Winner (1986) argues for this view since technological systems create and form social orders that constitute the limits that facilitate and control the way in which social behaviour may take place. From this position Winner (1986) puts forward the thought that since technical systems play an important role in social life they should be studied not only by technicians.

> What I am suggesting is a process of technological change disciplined by the political wisdom of democracy. It would require qualities of judiciousness in the populace that have rarely been applied to the judgement of instrumental/functional affairs. It would, presumably, produce results sometimes much different from those recommended by the rules of technical and economic efficiency. Other social and political norms, articulated by a democratic process, would gain renewed prominence. Faced with any proposal for a new technological system, citizens or their representatives would examine the social contract implied by building that system in a particular form. They would ask, How well do proposed conditions match our best sense of who we are and what we want society to be? Who gains and who loses power in the proposed change? Are the conditions produced by the change compatible with equality, social justice, and the common good?. (Winner 1986, p 55).

As attractive as this proposal may be it is dependent upon a relatively planned approach to technological development where the parties may gather and decide to build a technological system. This planned approach to technological development does not take into account the manner in which innovation is understood to function in the present state of communication and organisation (von Hippel 2005). It does not take into account that technological advance can be incremental and disruptive at the same time.

The definition of disruptive ICT adhered to in this work is a technical development of the technological base that has a radical and pervasive impact on the use of the technology in social interaction (Lyytinen & Rose 2003b). This neither is, or is not, a form of technological determinism.

Technical change regularly affects the way in which we behave and, in some cases, leaves actors with little choice for free choice. This is not the same as saying that there is no level of human choice or control on the changes brought about by technology. While Lyytinen and Rose (2003a) refer to the effects of disruptive technology by using the metaphor of the earthquake they are referring to the human perception of the changes as they occur. Once a technological change has taken place and begun to disseminate in society the changes felt by the members in that society may be akin to an earthquake. This is not to say that technological change occurs without human awareness of the change. Even in situations where humans have ignored or underestimated the impact of a new technology, this should not be understood to be a force beyond their control albeit that the change might be experienced as such (Winner 1978).

A much more complex issue is the level of understanding which we can have about the impact of technological change and the unintended consequences of such change (Beck 1992, Kallinikos 2005, Rolland 2002, Tenner 1997). This not only includes the future development of technology by developers but also the knowledge of how users will adopt and change their technology in the future.

This thesis explores an issue close to the problem of unintended consequences of technological change. This thesis explores how attempts to regulate disruptive technology affect Internet-based participatory democracy. This may be seen as the study of the unintended consequences of attempts to regulate disruptive technology and the anti-democratic consequences of such regulation. It is anti-democratic in the sense of not adequately promoting or supporting the active role of the citizen within a democracy.

This work began by reviewing alternative regulatory theory from Fuller (1964) to Murray (2006). The main point of this review was to show that the simplistic model of command and control regulation (Black 2002) has never been an adequate metaphor with which to explain the regulation of complex environments. With the beginning of the discussion on the regulation of Internet-based activities the command and control model has received additional critics. This work has therefore taken the definition of regulation as the enterprise of subjecting human conduct to the governance of external controls whether state or non-state, intended or unintended (Fuller 1964, Baldwin *et al* 1998). The advantage of this definition is that it recognises that there is more than one regulatory structure in place simultaneously. The more obvious drawback of this model, from the point of view of the potential regulator, is that it opens regulation to a larger degree of complexity. This complexity is commonly referred to as a polycentric (Fuller 1964) model of regulation since it is regulation originating from many sources. Therefore this thesis presents the development of traditional regulatory theory from the traditional ideological origins of command and control regulation to the more subtle and complex regulatory structures, which regulatory theorists understand regulation to be at present.

Regulation of the online world brings with it additional complexity due to the ease in which certain regulatory regimes can be circumvented (Johnson & Post 1996). Another important difference is the malleability of the physical rules where regulation takes place. Since the online environment is created by code the fundamental rules and laws that govern it can be more easily adapted to suit the purpose of the regulator or the actor. This is because the online world not only is influenced by the regulatory modalities (Murray & Scott 2001, Murray 2006) of *hierarchy*, *competition* and *community* but is also highly susceptible to *design-based* regulation. This flexibility brings additional challenges to the task of regulation and to regulatory theorists attempting to apply their knowledge to this environment. At the centre of online regulatory theory are the debates between Lessig (1999) and his critics such as Murray (2006). As described in the section on regulating technology (page 30 *et seq*), Lessig was the first to deliver a book-length application of regulatory theory to the online environment. Today most regulatory theorists agree that his theories are showing serious logical flaws.

Regulation has, on several occasions, as the case studies in this work have shown, led to a regulatory over-reaction when dealing with disruptive technology. As explained in the outset of this work the concept of regulatory over-reaction is the measure of whether a technology has been regulated or overregulated. Whether a technology is adequately regulated, or not, will depend upon the democratic effects of the regulation. If the implemented regulation tends to not only regulate undesirable behaviour but regularly criminalises or frustrates many types of legitimate behaviour, causes a negative democratic effect, then the situation is one of overregulation.

The specific contribution of this thesis is the development of an expanded understanding of the way in which we regulate disruptive technology. This understanding helps us to better regulate that which is new and which threatens that which is established. The results of such a study can then be applied to all domains where regulation of disruptive technology may occur.

The Murray approach to the regulation of Internet-based activity provides a lens with which we can study this type of regulation. His approach should be understood as an application of adapted structuration theory (DeSanctis & Poole 1994, Giddens 1984, Orlikowski 2000, Orlikowski & Robey 1991) with its interest in the interaction between actors, structures and technology. The case studies conducted within the framework of this work take as their theoretical starting point the regulatory model expounded above. They show the complexity of the regulation of Internet-based activities and the interaction between the regulatory structures and the actors that it attempts to regulate.

The Cases

The six case studies presented in this work have investigated different, but interconnected, contemporary phenomena. The use of the multiple case studies has enabled the study of these seemingly different but interconnected phenomena. The common ground between these cases is their ability to illustrate and bring forward the way in which disruptive technology is regulated within the IT-based participatory democracy and the effects of such regulation on the latter.

	Regulator	Effect on Actor	Democratic Effect
Participation	Hierarchical	Unable to fully participate	Loss of opposing voice
Communication	Hierarchical Design	Limited forms of communication	Loss of alternate communications forms
Integrity	Design Competition	Diminished incentive to participate since actor must protect herself	Uncertainty & insecurity among participants
Property	Design Hierarchical	Diminished incentive to participate due to property "loss"	Uncertainty among participants
Access	Design Community	Excluded from access to infrastructure	Rule of incumbent
Autonomy	Design Hierarchical Community	Non-autonomous actor	Loss of opposition & Incumbent rule

Table 7: Democratic Core Value, Regulatory Modality and Effects

Table 7 provides an overview of the cases with a focus on the regulatory elements based upon the Lessigian (1999) modalities of regulation: architecture, law, markets and norms. These have been further developed by Murray and Scott (2001) and in Murray (2006) to the more adequate terms *design-based* control, *hierarchical* control, *competition-based* control and *community-based* control.[42] In these studies the regulator is to be understood in the broadest terms, as Fuller (1964) described i.e. regulation is every force or external controls exerted upon those to be regulated. The regulatory modalities need little further elucidation beyond the Lessig-Murray discussion,[43] but a brief overview may assist the reader at this stage. *Design-based* control refers to software, *hierarchical* control refers to the actions of legislation and courts, *competition-based* control refers to solutions which arise when actors rise to meet consumer demand and *community-based* control refer to the social rules which arise in different contexts some of which are codified in written form.

The first case entitled *Participation* (online civil disobedience, Chapter 4) studied the way in which participation in civil disobedience was being conducted in online environments. The disruptive effects discussed here are the use of Internet-based technologies for the purpose of civil disobedience practices. The results show a definite lack of "space" in which acts of civil disobedience can occur. This lack of "space" leads to a discrimination of ICT as a medium of communication in the form of civil disobedience. This in turn leads to a lessening of the use of ICT for democratic participation.

The case refers to both the conflicts between regulatory structures and the actors' activities and the internal conflicts between the actors. As the case shows, the present trend in regulation by states is the move towards the criminalisation of all activities that these specific actors consider to be legitimate forms of civil disobedience. The main democratic issue at stake here is the concept of participation that is being severely threatened through hierarchically based regulation and the re-interpretation of essentially nuisance acts into acts of terrorism (CDT & EFF 2003, Akdeniz 2005).

What makes up the regulatory structures of the environment in this case is the right to define the actions of the actors. While the actors argue for their actions in terms of civil disobedience and the right to protest, the regulatory structure uses its right of interpretation to define the actions as criminal,

[42] For more on this see section *Regulating Technology* page 30 *et seq.*

[43] Ibid.

bordering on terrorism. The effects of such interpretative control are to remove the effective right to communicate by ensuring that there is no place within Internet-based communication for such activities.

Such a reaction to the acceptability of civil disobedience creates an uneven level between what is permissible online compared to what is permissible offline. With the application of the concept of functional equivalency, as described in the section *Theoretical Focus* (page 38 *et seq*), it becomes apparent that online communication is not being treated in a manner equivalent to the regulatory structure that is applied to offline communication. The lack of tolerance towards online protest forms seriously hampers the development of democratic interaction in the online environment. This is made possible, to a large extent, by the lack of public space when dealing with online environments. The offline world contains many traditionally acceptable public spaces where communication may take place in a more-or-less unhampered manner. However since online communication is wholly dependent upon contractual relations (for example between the user and the ISP) the common street corners can easily be regulated and therefore the ability to participate in social interaction without fear of reprisal is limited in comparison to offline interaction.

The use of *hierarchical* controls as regulation leads to the prohibition of all forms of online disobedience irrespective of motives, costs and possible damages. Such a blanket prohibition has the effect of making online disobedience impossible and as such, removes the technical realm beyond the means of the would-be technical disobedient. These actions create a discrimination against the online behaviour in so much as behaviour, which would be socially acceptable offline, becomes impossible online. This creates a diminished ability to use technology to criticise incumbent power and therefore it leads to the lessening of the democratic potential of the Internet.

The second case entitled *Communication* (viruses, Chapter 5) in some ways follows in the footsteps of the previous case in that it explores a phenomenon that tends to be generally condemned. The purpose of this study is to explore the role of structural regulation vis-à-vis computer viruses. The general regulatory trend is to criminalise the computer virus in all forms despite the lack of an adequate definition of the concept. By criminalising and providing harsh penalties for those who create or spread computer viruses the regulatory structure intends to create a better online environment for the users. Since the concept of the computer virus is a relatively unexplored area such legislation carries with it negative side effects on the right to communicate.

The validity of this paternalistic (Lessig 1999, Murray 2006) approach of general criminalisation without paying attention to the possible positive uses of virus-like software is questioned in this case. This therefore decreases the level of freedom of expression within the online environment as the regulatory structures have demanded that no positive communication can come in the form of virus-like software. The case study shows that there are a number of non-harmful uses for virus-like software and that the regulatory structures threaten to make these uses into criminal acts and therefore seriously hampering the communication rights of those involved in such activities.

By presenting legitimate uses of computer viruses the case shows that the blanket criminalization of viruses negatively affects the freedom of communication for those actors who are involved in the making of legitimate viruses. Such regulation therefore prevents users from using the equipment in their possession and thus constitutes a limitation of the freedom to act.

Even in this case a large part of the regulatory structure is concerned with the interpretation of a term or metaphor. This interpretation carries with it serious consequences for the IT-based participatory democracy and yet it is not seen as a democratic question but rather as a technical question. By referring to the discussion as a technical rather than a democratic one the larger popular debate is avoided (Beck 1992, Giddens 1990, Kallinikos 2005). Despite attempts to regulate the virus, it remains badly defined and subject to the interpretation of the regulator. This creates an uncertain situation for users hoping to use harmless or helpful viruses. Once again what is created is an imbalance between the freedoms that exist in the online and offline worlds were the online world is being discriminated against. This discrimination is subsequently being enforced by the uneasy dependence the user has upon the service provider. Using a functional equivalency approach to analyze the situation with computer viruses, we see that the regulatory structure overreaches itself by attempting to regulate software instead of attempting to regulate harmful behaviour carried out with the aid of software.

The regulatory modalities of communication are the *hierarchical* control mechanisms that, in many jurisdictions, act as a blanket prohibition against viruses irrespective of their potential damage or political content. In addition to this there is a secondary regulation through *design-based* controls and *competition-based* controls in that the software intended to prevent harmful viruses from damaging computer equipment does not attempt to discriminate between harmful or harmless viruses. The effect of the regulation of viruses through the *hierarchical* controls and *design-based* controls is a limitation of the modes of communication for the actor. This in turn may create less communication within the participatory democracy. This lessening of communication is particularly important since it entails the loss of alternative forms of communication, which therefore means that permissible communication within a participatory democracy becomes more uniform, which lessens the possibility of innovation as innovation comes not from conventional usage but from exploring unconventional sources (von Hippel 2005). Additionally the area of online communication is therefore discriminated against through the structures preference of the offline forms of communication.

The third case entitled *Integrity* (spyware, Chapter 6) begins the study of the relationship between the users and their equipment. The ability to participate in a democracy by using technology requires that the users can trust the technological infrastructure upon which they depend (Klang 2001, Awad & Fitzgerald 2005). It is important to note that even though we are part of a technological society (Balkin 1998, Castells 1996, Mitchell 1996, Negroponte 1996) this does not mean that the users in this society are able to understand how the technology works. Therefore the users are required to rely upon technical experts that provide their technology and the regulators that provide the environment within which they move. Spyware, and indeed every form of covert surveillance, threaten the actors' integrity and through this, actors' ability to freely participate in the participatory democracy without fear of being observed.

The conflict demonstrated in the integrity case represents the conflict that occurs when user trust in technology is compromised by a new threat created by a disruptive technology. The technology in this case is such that it compromises the infrastructural trust (Klang 2001, Awad & Fitzgerald 2005) upon which communication within the IT-based participatory democracy depends. The conflict arises from the interpretation of the software involved. While actors who dislike the effects of spyware attempt to discuss the phenomenon in relation to privacy regulation, found in human rights documents. The regulatory structures find it difficult to apply the more abstract privacy terminology and arguments found in human rights documents and national legislation and are more comfortable with applying contract law. This choice of the structural regulation favours the manufacturers and operators of spyware and therefore leaves concerned actors without adequate protection.

This creates a surveillance society where the user internalises the surveillance (Foucault 1979) and controls her own actions. This restricts the freedom of action within the online environment, as the actor is never aware of the privacy of her actions. In an attempt to counteract what the actors perceive as the failure of the regulatory structure to protect privacy values a *competition-based* solution has arisen. This solution takes the form of both software and social solutions. The software consists of programs that counteract spyware by removing the threatening software from the system. The social solutions consist of online discussions aimed at determining whether a piece of software should be understood to be spyware.

These *competition-based* solutions provide an example of actor-driven regulation that arises when the regulatory structures controlled by the state fail to provide the actors with the protection they perceive to need. The development of actor-controlled regulation is based upon technological solutions, as opposed to the political regulation of the state, since these are the tools that are at the actor's disposal. The efficiency of software tools as a form of regulation is due to the malleability of the software environment. By installing technological means at each computer regulation of a kind can be achieved.

The case also illustrates an important aspect of the surveillance theory that claims that individuals under surveillance will adapt their behaviour to reflect the fact that they are potentially being watched (Foucault 1979). The development here is that most of the users under surveillance are unaware of it and therefore do not change their behaviour.

The modalities of regulation observed in this study are *competition-based* and *design-based* control. The importance of competition as a regulatory modality arises from the weakness or inefficiency of other forms of regulation. The perceived need of users for integrity protecting mechanisms have created a wide market for these products, which now appear both as stand alone software and are being incorporated in larger software packages such as operating systems or anti-virus software. This *competition-based* regulation is however inefficient without the additional modality of *design-based* control. Here the software-based threats of software are counteracted by the software-based solutions of anti-spyware software. Through this consumer demand the regulation of spyware is affected by the wider implementation of anti-spyware software that changes the conditions for the producers of these products. The lack of concern with integrity issues from the part of the more established regulators leads to this need for individuals to protect themselves that in turn makes open participation more arduous. This in turn decreases the incentive and interest to participate in online activities. The uncertainty surrounding integrity protection is a serious concern for online participation in democracy since anything, which negatively affects the will to participate within the democratic public sphere directly, affects the democracy.

The fourth case entitled *Property* (MMORPG, Chapter 7) studies the importance of property in a democracy. Without the ability to be assured that an individual's property is adequately protected there will be a low level of trust and interaction. This study looks at the role of the users' perceptions of property in online environments. This study takes its starting point from the growing phenomenon of large-scale online role-playing games, the so-called MMORPG. The growth and popularity of these online environments are responsible for bringing into focus specific online/offline relationships. The ability to interact with others in online environments has challenged many of the assumptions we hold about our social dealings with others. The purpose of this case study was to describe the early process of a social re-evaluation of assumptions created in the offline world.

The case deals with the creation of property and value in the virtual environment. At first glance, applying traditional tools, assigning property rights to that which is created within virtual environments is perfectly straightforward. Since the virtual environment is a created world each aspect of it is the basis of human decision. There is no real natural evolution. Therefore the basic control and design of the virtual environment rests firmly in the hands of those who create or permit others to use the environment.

From the point of view of those who create and provide the online environment the permissions and rights of the users are regulated by the contractual obligations that exist between the users and the controllers. In this way the controller takes the role of the structural regulator. This position is reinforced by (1) the physical control of the virtual environment, (2) actor access to it and (3) supported by the legal system in the offline world. However, those being regulated are questioning this straightforward position. Actors within MMORPG are claiming that the time and effort applied in the virtual environment grants them property rights in the fruits of their labour. They argue that the control of the environment does not grant the regulator the automatic right to that which is created within the environment.

The economic and philosophical importance of this debate should not be underestimated because what is happening does not occur in the "real" world. The economic value created within a virtual environment is akin to the economic value created on a stock exchange, both are intangible values created by speculation. There have been several studies carried out in the economics of virtual environments (Castronova 2001, 2003) and some speculative investments within online environments have become news in the offline environment. One such example is the purchase of an island within an online virtual environment. The island was purchased for $26 500 as an investment for the purpose of property development (Krotoski 2005). Beyond the economics of this phenomenon the question of property in virtual environments has wider implications for online interaction.

The question concerns the right to create and enforce rules in relation to those who are affected by the rules created. At present the rule making and enforcing processes favour the status quo, which in this case is the creator and/or maintainer of the virtual environment. The question arising from this autocratic approach is what degree of freedom could the users of the environment obtain. If we take our starting point from the users there is evidence that they are dissatisfied with some aspects of the autocratic approach.

Whereas there are few who would argue that there are no grounds for the maintainers right to control her property, the question is one of the level of this control when a conflict of interest between the controller and the user occurs. At this stage the controller points to the contractual relationship that creates the users rights to enter the environment. This relationship takes the appearance of a social contract (Gauthier 1986) and many similar arguments for and against the social contract can be seen mirrored in the discussions between the controller and the users. One point stands out more clearly than others. While there is a right for the controller to maintain and control her property, if the property is used for social interaction an argument based upon the concept of participatory democracy can be made in the relation to the rules and regulations which affect the participants (Pateman 1970). The fact that the users were required to enter into a contractual relationship prior to joining the virtual environment does not prohibit them from attempting to re-negotiate the terms of the original agreement.

This re-negotiation is one-sided since there is no arena for negotiation where the controllers and users meet and freely interact. At the same time interaction within the environment among peers creates social rules and accepted common practices. This behaviour also additionally reinforces the acceptability of these practices (Pargman 2000). The rules created within the virtual environments, among the users are strong since they are internalised by the users. When these rules come into conflict with the controller's regulations the users tend to feel morally less obliged to follow the controller's rules and attempt to circumvent the controller's rules. This therefore creates a situation of re-negotiation. The controller must either attempt to more stringently enforce the rules and take the costs of such enforcement or attempt to meet the desires of the users.

This case has shown the movement within virtual online environment that are causing a re-interpretation of the understanding of virtual property. This re-interpretation causes those involved to use a mixture of technical measures and philosophical arguments in an attempt to establish and prove their standpoints. The traditional legal infrastructure is occasionally used to reinforce a position, however this is not done on a large scale. In this case study we can see that a core social value is being re-evaluated and re-interpreted to suit a new environment and that this discussion is taking place outside the traditional channels for such development. It is also interesting to note that the groups conducting this process are to a large degree those who are most affected by the regulation of property. The re-negotiations being carried out by these groups are then being brought into the more mainstream process of social understanding or creation of the term (or value) of property.

In the property case the modalities of regulation are *hierarchical* control and *design-based* control. Attempting to redefine the manner in which property is understood is complex and demands a re-appraisal of the traditional understanding of property. Without this the result is that legal regulation protects the status quo. This regulation is enhanced by the control elements inherent in the virtual environment and these are the ability to exclude users or items that have not been created or transferred in accordance with the platform owner's regulation. Therefore regulation by *design-based* control is a powerful tool in online environments. The result is a disincentive to interact within online virtual environments and a lack of ability to actively control individual property rights. The lack of certainty in this area therefore is a disincentive that negatively impacts democratic participation in online environments.

The fifth case entitled *Access* (software, Chapter 8) deals with the conflicts arising from two different forms of production ideologies (commercial and non-commercial software production ideologies) and the ways in which these ideologies are embraced or rejected by public authorities. Instead of relegating the discussion of software standards to a technical realm this study explores democratic roles inherent in the choices involved in software standards and their relevance to democratic participation. The choices of government bodies to implement a software standard carry with them democratic implications. This is particularly true if such choices have the effect of granting exclusive rights to proprietary software standards. The question of whether to adopt certain types of proprietary software standards and software packages therefore are more than technical decisions – they are decisions that directly effect the freedom to communicate and therefore play an important role in democratic participation.

The question of concern is the manner in which communication between the regulatory structure and the actor can be conducted. In this case study, the regulatory structure is represented by the technical standards and policy decisions adopted by state organisations. There technical choices have a direct effect upon the way in which the actors, represented by the clients of the organisations, communicate with the state.

In addition to creating barriers to free communication the choice of proprietary standards by government also creates the situation where the state actively becomes the advocate for a specific companies products and therefore disadvantages those citizens who wish to participate, but wish to use alternative products in their participation in the democratic process. In cases where the technology controller is a private organisation the actor or customer has a choice to refuse to communicate, however in the case of the state few actors are able to makes such a choice.

Within the case study on access the regulatory modalities are community-based and *design-based* controls. The *community-based* controls take the form of buyer habit and policy, which create a barrier to the acceptance of alternatives to commercially produced software. The *design-based* controls regulators function by the use of proprietary standards. Since the software need not be compatible with each other commercial producers can create path dependencies and lock-in effects (David 2000, Hanseth *et al* 1996) to limit the use of alternative software packages either as complements or as replacements to existing software. The regulation in this manner has serious implications within a participatory democracy since the participants are unable to participate in the manner of their own choosing but must do so in limited forms. In addition to this the limitation of forms of interaction also lead to a reduction of innovative experimentation (von Hippel 2005). The result becomes the non-questioning acceptance of the incumbent's position and role within the democracy.

The sixth case entitled *Autonomy* (censorship, Chapter 9) deals with the control of online information and the effects of such control on actor autonomy and democratic participation. On the one side we see the actions of states attempting to maintain control over the Internet-based communications by employing a wide range of technical and social means. This structural regulation is intended to control the information access and dissemination of the actors within their control. These are usually defined by the physical borders of the real-world jurisdictions. The limitations imposed on the actors' freedom to communicate lead the actors to take counter measures to ensure that they maintain the ability to communicate.

This case presents censorship measures employed by the regulatory structures and views them in accordance to censorship theory. In addition to this the case also studies the methods with which the actors attempt to circumvent the limitations placed on their communication by employing counter-censorship technologies. While the foundation of the forms of censorship and counter-censorship are based in technological measures, this case also shows that social control plays a large part in the way in which information is controlled. This case presents an example of the difficulties with regulating disruptive technologies in that the attempts to regulate are often circumvented by implementing more technology. This amounts to a technological regulatory arms race between those involved where the regulatory structure is constantly involved in implementing more technology to ensure that the regulatory structure is not eroded by those who wish to evade it.

The regulatory modalities seen in this case are *community-based*, *design-based* and *hierarchical* control. The use of software to control the amount of information that is available to groups of users is a widespread practice (Deibert & Villeneuve 2005). This is in turn compounded by the threat of traditional legal force exercised against those who make information available to others. These two modalities are powerful regulators when used in combination in this manner however the regulation is made all the more extreme with the use of *community-based* controls. As the use of the Chinese *Public Pledge* example illustrates, companies eager to enter into the Chinese Internet market actively ensure the implementation of *community-based* controls as described in the document. Corporate limitation of online information includes any and all information that the other regulatory modalities may or may not include in their regulation. Therefore by including a private regulatory actor and giving guidelines the Chinese state has enabled the regulation of online behaviour to a much harsher degree and at a much cheaper cost than possible with the modalities of *design-based* and *hierarchical* control.

Since all online communication depends upon relationships with corporations the potential regulatory power of these institutions must not be underestimated. The loss of the ability to find online information is devastating to the autonomy of the individual since it becomes impossible for her to be able to make autonomous decisions without access to the facts. The effects on participatory democracy are, if this process goes too far, the negation of democracy since without the information necessary autonomous decisions cannot be made and without autonomous decisions by individuals being made there cannot be a rule by the people and therefore no democracy.

Understanding Disruptive Technology

This work began with a simple definition of technology as both the purposeful activity and results of the transformation or manipulation of natural resources and environments in order to satisfy human needs or goals (Kroes 1998). To this we can add the words of Hughes (2004, p 1):

> Technology is messy and complex. It is difficult to define and to understand. In its variety, it is full of contradictions, laden with human folly, saved by occasional benign deeds, rich with unintended consequences. Yet today most people in the industrialized world reduce technology's complexity, ignore its contradictions, and see it as little more than gadgets and as a handmaiden of commercial capitalism and the military.

Hughes not only views technology as complex but he brings the additional idea that it is often simplified or purposefully misunderstood. This simplification is important since it obfuscates our understanding of technology by demanding that technology either be simple so that everyone can understand it or else it is too complex and must be left to the experts (Beck 1992). While a technological result may seem complex most technologies develop through incremental steps (Kallinikos 2002). These steps are less innovative than they at first may seem since they need to encompass requirements such as technological compatibility and interoperability (Hanseth 2000, Hughes 1987, Kallinikos 2002, Kling 1992).

Despite these incremental steps and the need for technology to be able to interact with earlier technology the concept of disruptive technology has been recognised. The concept of disruptive technology within this work has taken as its starting point the conceptual and terminological developments carried out primarily by Lyytinen and Rose (2003a, 2003b).

Amongst their criteria for disruptive technology (Lyytinen and Rose 2003a, 2003b), which they have based upon the analysis of several studies, we find, firstly radical changes in technical performance "pushed" by developers (as opposed to "pulled" by user demand) followed by rapidly increasing adoption and finally the overwhelming of metaphors. This latter element is consistent with the idea of the metaphor as a conceptual construction (Lakoff & Johnson 1980) in that they form our understanding of the technology around us. The cumulative social and organisational effect of these criteria have been described by Lyytinen and Rose (2003a & 2003b) as an earthquake.

The disruptive technology described by Lyytinen and Rose (2003a & 2003b) is focused on the development and innovation of technology even if the effects are described in their earthquake metaphor. The result is a description of disruptive technology which functions within the confines of organisational theory but is less exact when attempting to apply beyond the confines of the organisational setting.

The studies presented within this work have all been carried out beyond the confines of the organisation. From these settings certain adaptations need to be made to our understanding of disruptive technology in order to better understand its nature.

Radical Technological Change: Lyytinen and Rose write that disruptive technology requires the rapid development of new technology. When studying this claim in this work we notice that this is both true and false. On a general level the interconnectedness of information systems is not a new phenomenon. What is new is the scale and variety of participation and participants. In each of the different studies presented in this work the problem stems not wholly from the use of innovative technology but rather from the innovative use of technology (e.g. *cases property/MMORPG, access/software*).

Rapidly increasing adoption: As the studies in this work have shown rapidly increasing adoption is not a necessary requirement for a disruptive technology. On the one hand mass-adoption of new technology amounts to a disruptive technology since it is noticeable, but a less widely adopted technology can also be seen as being disruptive (e.g. cases *participation/disobedience, communication/virus*). The innovation lays not so much in the technology but rather in its adoption. This can be either the sheer scale of users or the innovative use of technology that makes the technological interaction radically different from the past.

Overwhelming of metaphors: The final stage is the triumph of new mental models over their predecessors. This final stage is problematic not only because such a process is difficult to measure outside the organisational boundary but also because it also requires there to be a grand or superior metaphor to overwhelm. In particular beyond the organisational barrier it is difficult to find such grand metaphors (Lakoff 2004).

To Lyytinen and Rose (2003a, 2003b) the effect of disruptive technology is the unstoppable earthquake. The idea being similar to Christensen's (1997) that not acknowledging, or fighting, technological innovation will inevitably lead to the downfall of the organisation. If this is seen at the level of state regulation (e.g. case *autonomy/censorship*) this conclusion is not necessarily true. The negative effects of preventing or regulating disruptive technology cannot be conclusively proven. But, as argued here, from the perspective of autonomy striving against disruptive technology by attempting to regulate it counteracts the autonomy of the individual and through this negatively affects the democratic participation.

Disruptive Technology Regulation

Pateman (1970) expounds the goal of participatory democratic theory as the attempt to include the maximum participation from the public. This participation is not limited to policies (decisions) but also the development of the social and political capacities of the individuals involved in the process. Participatory democratic theory takes its starting point from two important assumptions. Firstly, that people are capable of understanding, expressing, and finding solutions for their problems. Secondly, effective solutions require the participation of the people who will be affected by them, without necessarily being dependent on authorities and experts (Oppenheimer 1971, Giddens 1990, Beck 1992).

Changes in the technological infrastructure, the cultural environment and the regulatory system are constantly with us. The whole concept of social evolution and progress is the measurement of these types of changes (Latour 1991). Society should therefore have learnt to accept, or even welcome, change. Unfortunately this is rarely so. Change is rarely welcomed since it creates a level of uncertainty for those involved and uncertainty is not an aspect society welcomes. Despite the social resistance to change society has long dealt with major and minor changes in technology, society and regulation without the need for further deliberation on the manner in which this change should be accepted and incorporated into the social infrastructure.

The alternative environments, such as the Internet, have the advantage that they offer their inhabitants (for the want of a better word) the possibility to interact in ways that are not limited by the traditional social structures existing within, and enforced by, the nation state. The creation and regulation of a society is often explained in grand theoretical terms. To the unsuspecting reader it may seem that the designers and maintainers of the social order have a theoretical framework to which they apply their methods and actions.

In the world of engineering and project management there are definitely both theories espoused and methodological approaches praised. However, in this realm researchers have become more aware of the actual process of creation and management. It does not follow the lofty processes of theory and design but rather tends to be a constant process of tinkering, amending and short term fixes. This involves the re-combination of individual application elements into new arrangements, a process of "bricolage" (Ciborra 1992) leading to the invention of new applications riding the existing infrastructure. Engineers have also been required to understand the difference between espoused theories and what actually takes place (Argyris & Schön 1974). Within social design the complexity of the problem allows for too many variables and the success or failure of a project is hard to predict or explain. The same is often true of technical design but there is an easier unit of measurement in the actual concept of failure. If the finished product does not meet its design specifications there is a strong supposition that something has gone wrong. This connection between design and finished product is not easily made in social design. The realisation to be faced is that the regulator must grow accustomed to having less control over a complex reality.

Internet technology allows, to a much greater degree, attempts to practically implement abstract ideas (e.g. *Participation*, *Communication*, *Integrity*, *Access* and *Autonomy*) related to democracy. By making such a thing technically possible, this thesis shows that, the focus of regulatory discussion turns to whether the practical implementation of these abstract ideas is a desirable thing. Such abstract philosophical ideas pre-date Internet-based technology and have to a large degree never needed to be implemented since it was impossible or impracticable. Therefore the technological changes are presently challenging our grand theories of democracy – through empirical study. The removal of the technological limitations therefore is bringing a re-examination of the democratic values. This thesis has observed the role of the regulator. While it cannot be said that the regulator (in this work) is following a pre-defined plan, the analysis of actions provided in this work seem to show that generally the regulator prefers to enforce the status quo and maintaining control as opposed to establishing democratic ideals in practice.

To be able to understand social change, even such change as brought about by technology, it is not enough to study technology. Therefore this investigation has looked at the regulation of technology. Regulation has been chosen as a focus since it has a long established tradition of being an agent of social control and change. In addition to this, regulation provides the researcher with an abundance of empirical evidence to be examined.

It is also important to recognize a criticism directed towards the reliance of *design-based* control. Brownsword (2005) writes about the "regulatory pitch", which could be understood as the legitimacy offered by the regulator for the regulatory acts. *Hierarchical* regulation requires a larger degree of transparency and accountability between the regulator and the regulated while *design-based* regulation requires less transparency and accountability (Brownsword 2005).

> The bottom line, however, should not be blurred: a fully techno-regulated community is no longer an operative moral community. (Brownsword 2005, p 19).

The question Brownsword raises is an important one. When we lose the possibility to do the wrong thing and are only capable of doing the right thing we also lose our ability to make meaningful moral choices and therefore no longer act in a moral way – even if we do no wrong. This important issue deserves a more serious consideration than is possible in this work.

The main forms of regulation carried out in cases 1 (*Participation*) and 2 (*Communication*) were mainly traditional forms of command and control[44] the results of such traditional forms of regulation have been blanket prohibitions which are over-inclusive and therefore also prohibit legitimate, non-harmful activities. This therefore causes limitations in the participatory democracy as legitimate forms of participation and communication are frustrated by regulations. The main forms of regulation carried out in cases 3 (*Integrity*), 4 (*Property*) and 5 (*Access*) are exhibited in the preference to protect traditional values. This lack of regulatory adaptability leads to a growth of actor dissatisfaction with the regulatory structures. Such dissatisfaction can even take the form of direct action to circumvent or

[44] Section entitled *Regulation* page 26 *et seq*.

evade regulations. The final case (*Autonomy*) shows the regulatory activities of command and control backed up *by design-based* and *community-based* controls. This potent mixture of regulation is efficient and yet there is evidence of user dissatisfaction with the regulatory regime. Again the dissatisfaction shows itself in the collaboration of actors in attempts to circumvent regulation.

The cases in this study show the interaction between technology and regulation. What emerges from these studies is the concept of competition of regulative forces. This competition shows the disruptive force of technology upon established social norms and agreements. Technology is not only a passive artefact but plays an important role in enabling and regulating the users of technology and in this way traditional forms of regulation are facing competition.

The problem at hand is therefore our ability to deal with social dilemmas brought about by technology. This work has attempted to demystify the structures of both society and technology. This process of demystification takes place by observing that social control is a Foucauldian (1980) power struggle and that technology is not something we can chose to accept or not. We exist in a technological state.

Regulation also carries with it costs, both open and hidden, and consequences both intended and unintended. The fact that something can be regulated is not enough. For a regulation to be successful i.e. its implementation should manage to fulfil the desired goal at a minimum of cost and unintended consequences it must take into consideration the behaviour and desires of those affected by the legislation. Therefore to be able to legislate efficiently requires a cognitive ability to be able to understand the effects of a decision on the lives of those it affects.

Regulating disruptive technology deals with the attempt to share a common space, and use it for different purposes – this demands regulation. That which is regulated is the different needs of the technology users. Actors proceed to use the technology in a manner that provides added value, in some way, to their lives. This may not always be in accordance with the ideals or goals of the regulatory structure. This conflict involves the interplay of many levels of rules, values, technology and social norms.

The attempts at regulation do not always lead to the desired effects and in many cases the regulation itself becomes part of a new, unintended problem. Occasionally the problem caused by the solution can be more harmful than the initial problem.

This work exemplifies ways in which regulatory structures are attempting to deal with the problems they face by new technology. While declaring the technology to be a democratic asset in that it facilitates social interaction, few regulatory structures are comfortable with implementing a democratic participatory approach to communication with the actors. This approach is however not particularly cost efficient since actors tend to work together to find forms of circumvention in relation to structural regulation that prevents their interests. The result is that the regulator must improve its regulatory forms so as to solicit the agreement of those regulated. Such an approach will reduce the costs of enforcing regulation. This approach, however, entails a negotiation between the regulatory structure and the actors and may also have the effect that those representing regulation must also compromise their power.

The recognition of the need to share power is not an easy one to accept. However, by proceeding to attempt to enclose the citizens of a state by invoking geographical borders is becoming less cost effective and nor is this approach in line with the needs and wants of the users involved in the system. It is therefore time to move ahead and to attempt to base the legislation and control closer to the needs of the users who will be affected by the regulation. This entails the revitalisation of the concept of the social contract based upon the Rawlsian (1999) visions of setting basic rules upon which groups of users can agree. This has seemed to be an all too utopian a vision to turn into a practical reality in the diversity of the nation state. However, creating legislation based upon the needs of those who will be primarily affected by the legislation is not impossible.

The process of legislation and control must, in a much greater part, involve the needs of the users. The users are at the centre of most other design processes since it is the users who will eventually become those who are involved to the largest extent in the acceptance of the finished product. This is an issue which regulatory structures have long managed to avoid and in the place of the user it has implemented a system of representatives. Their role has been to act in the interests of the users. Unfortunately this system is not adequate in a diverse a world and therefore the representatives become an elite whose main goal is to preserve and consolidate power instead of presenting solutions for the users.

The technological infrastructure today has enabled the creation of a-national places, or places where nationality is questionable, and the carrying out of discussions outside the control of the traditional boundaries of the nation state. With this system the number of social discourses available to the individual has increased exponentially. These developments create a situation where the individual is able to better choose the discourse of her choice and is no longer dependant upon traditional information sources.

To achieve a greater level of adequate control to deal with the effects of disruptive technologies the regulation and enforcement must be based, to a much greater degree, on the needs and desires of the users. Therefore if we agree that the technology is unable to be limited by the national borders then any discussion on the control or legislation of that technology cannot be carried out on a suitable level if it remains within the national borders. To enhance the control of a technology, which has the ability to avoid legislative control from the nation state, this control must be based upon something other than the concept of the nation state as the lowest common denominator of a base of power.

To be able to achieve this, the state must come to the realisation that it is no longer the adequate forum to discuss and regulate these technological questions. Neither is it enough to enter into discussions between states. The base of power must be better connected to those who are affected by the decisions and regulations of the power structure. Only in this way can we speak of a true democratic implementation of power.

However there is an important issue that must be dealt with here and that is the insight that those taking part in the discussion must become aware of the way in which they are part of their own myths. To truly achieve the level of democratic control and organisation of disruptive technology the discussion must progress with the knowledge that nothing can be beyond discussion.

Involving users in systems development has a long tradition (Asaro 2000, Ehn 1989) the method has a recognised effect of decreasing conflicts between those implementing the system and the end-user (Franz & Robey 1984, Lyytinen 1987, Newman & Noble 1990). Involving the user has a societal equivalent in the proposals of equitable regulation proposed by Habermas (1984). Habermas suggests that to be acceptable regulation requires the participation, in the decision making process, of those social members affected by a decision.

Habermas' ideas are no strangers to IS theory (Lyytinen & Hirschheim 1988, Alvesson & Willmott 1992, Ngwenyama & Lee 1997). His work has been used to create theoretical models as well as more practical applications of his theories. The more theoretical work has been the interpretation of Habermas' theories into conceptual framework for the understanding and creation of information systems (Hirschheim & Klein 1989, Lyytinen & Klein 1985, Lyytinen & Hirschheim 1988) while the more practical application of Habermas theories in the study of communications richness (Ngwenyama & Lee 1997) or the use of communicative theory to construct a context aware electronic forum on the web (Heng & de Moor 2003).

In his *Theory of Communicative Action*, Habermas' (1984) presents a discourse ethics that assumes that the world is pluralist and consists of competing ideals and values where only a few are articulated publicly. Most have been silenced by institutional and language barriers. These unarticulated ideas cannot be protected and are therefore repressed. This represents an injustice. To attempt to correct this rules should never be contained in closed systems but should be in plain view under the review of society and not hidden behind representative bodies.

The discussion of regulation must take place among the communities most affected by the discussions and the resulting regulatory changes. The combination of ICT and society is making reality more complex and we are becoming aware that there can be no universal, political experts (Giddens 1990, Beck 1992) to whom society can defer the hard choices to. This role must, as some (Beck 1992, Fiorino 1990, O'Neil Lane 2005) have already argued, therefore be fulfilled by the users most affected by the technology and the changes in society it creates and not delegated to experts. It is important to understand that while the regulation of disruptive technology is a question concerning technology it is ultimately a question of democracy. This should be taken as a legitimising factor which grants the users rights over the decision making process in relation to their technology.

The establishment of an IT-based participatory democracy demands fundamental features such as infrastructure and accessibility questions. These are often discussed and included in traditional plans and strategies for developing electronic government (eEurope 2000, eEurope 2002). In addition to this there is the need for a sustained investment in time and education in helping the user to adapt and use IT-based systems (Grönlund *et al* 2003, Ranerup 2001). The argument put forward in this thesis is that beyond these there are more aspects necessary to create a thriving IT-based participatory democracy. These are:

1. The ability of the regulator to seriously adopt the functional equivalency approach to ensure that users of online interaction and communication are not discriminated against.
2. The active participation of the users within the participatory democracy without deferring tough choices to experts.

3. The will of the regulator to accept user participation in the regulatory process.
4. The tolerance of non-conventional uses of technology.

Whether we like it or not, our technology is changing fundamental parts of our society. These changes create conflicts between the traditionally accepted social institutions and the way in which technology allows individuals to behave. Simple use of force to attempt to ensure the survival of traditionally accepted solutions is a short sighted, costly affair that cannot succeed. The technology of today requires that societies attempt to elicit the help and participation of the technology users to a much greater degree in the decision making process. The creation of new, or adaptation of outdated, socially acceptable institutions cannot be done by a political elite. This is true both on an organisational level and on a national level.

When attempting to understand regulation it is important to attempt to understand the collective actions of individuals. Regulation itself is often the result of formalized processes and therefore to a higher degree reflects the structures within a social organisation. The actions and reactions of online actors are mainly conducted via the mediation of communications technology. This mediated communication has the effect that it is seldom possible to be "present" when communication is taking place to attempt to ascertain the physical context within which the communication is taking place. However this mediation has the positive effect that it remains available within a context. Both this availability and the context can favourably be studied to understand the motivations and goals of the actor.

In this work the study is on the limitations faced by those who would use the Internet as an infrastructure for their forays into the IT-based participatory democracy. What are studied are the different attempts to regulate technology, which disrupts traditional forms of communication and interaction. This regulation may be carried out with noble and good intentions but has the negative effects of limiting the practical possibility of conducting communication and interaction in an ongoing IT-based participatory democracy. Through this limiting effect the online participatory democracy is discriminated against and its potential beneficial effects are lost. While many of the studies, which have been carried out in the field of IT democracy, have been concerned with the democratic effects of the implementation of technological systems. This work hopes to provide a starting point for continued work on the study of the unintended negative effects for democracy created by the regulation of technology.

This thesis has shown that the regulation of technology is the regulation of democracy. Such a conclusion has its implications. The foremost of implications is how this should affect the way in which we regulate technology. As this thesis has also shown we should not limit our understanding of the concept of regulation but we must broaden our minds and see regulation for the wide web of causes and effects that surround us, it is the structures that we create and maintain. It is the systems within which we interact with others.

One important finding within this thesis is that the regulation of technology is the regulation of democracy. This finding is particularly relevant to the way in which we address the issue of regulation of technology within society. To a large degree the question of technology regulation is left to the domain of the experts. This is perhaps natural, as their competence is understood to be a fundamental requirement for entering into the discussion of technology. The negative effect of this is that the discussion is left to the realm of experts and the actors who will be affected by the choice and decisions of the experts are largely ignored. By focusing on the regulation of democracy this work hopes to show that the regulation of technology is not a discourse for and between experts but it is one where all citizens can and should be involved.

Therefore this work has used traditional regulatory theory and its current applications to better understand the way in which regulation functions as a form of social interaction between the regulator and the regulated actor. This regulatory theory is placed within a wider concept of structuration theory, which attempts to bridge the concept of individuals as either acted upon (as elements within a structural context) or as autonomous agents. Applying this approach entails focusing on social practices ordered across space and time and adopting a balanced position, attempting to treat influences of structure (which inherently includes culture) and agency equally.

Regulatory theory applied together with structuration theory entailed the study of the regulatory structures, the regulated actors and the interaction between them. To this end this thesis has chosen to view regulation in the widest sense of the term and to study online activities that affect actors, regulatory structures and the participatory democracy. Many studies on the IT democracy have shown the possibilities the technology has to offer. Additionally many studies problematise this area and show that technology on its own will not create a strong IT democracy. Supplying broadband to everyone does not create an IT society. The focus of most studies has been on the technological relationship between the user and the state. The results of these studies have often been to question the optimistic, and occasionally unrealistic, political goals that have been inadequately funded, thought through or established with the end users (Grönlund *et al* 2003). This study attempts to look not at specific applied sites or IT systems intended for citizen-state communication but focuses on the technology in general usage and the regulation of the online public sphere.

This research forms a part of the ongoing research into the role played by technology in the democratic public sphere while focusing on the regulation of such technology, in particular, to the side effects of that regulation. When dealing with technology there is a tendency to call in experts. The experts are trusted to resolve technical problems. This trust goes so far that often the experts need no longer explain what is happening and what the effects of their actions are. They are experts and therefore they are trusted.

There is a different approach when an issue arises with democracy. Then everyone is expected to participate. The complexity of the social system is seldom an acceptable excuse for anyone not to participate in the democracy and nor should the lack of formal training be understood as a drawback when the democracy is discussed.

Therefore when the two areas merge an interesting issue arises. Is it a question for the populous or is it a question for the experts? If society regulates technical problems or a democratic nature to the experts then the society will no longer be a democracy. Only if the society demands that the populous participates in the regulation of technology can the society remain a democracy. This is the implication of the realisation that the regulation of technology is the regulation of democracy.

The main result of this study has been to show the implications of technology regulation upon the participatory democracy. Each of the six case studies serve to exemplify how the regulation of technology carries far reaching negative effects to the development and use of online communication for the participatory democracy. There are two results that are seen in all the case studies. The first is the lack of functional equivalency, which creates an unnecessary burden upon the technology. Stated basically this means that we demand that our online communications not only function on par with offline communications but we place much higher demands. The second is a general discrimination against the use of online communication. In part this is due to the functional equivalency argument but it is also a result in itself. All things being equal the choice of communication remains offline communication. Offline communication is given preferential treatment in relation to online communication. In addition to these general results the case studies show the implications of regulating technology within specific areas. The effects range from disincentives to direct challenges to the use of information technology in areas concerning *Participation*, *Communication*, *Integrity*, *Property*, *Access* and *Autonomy* within a participatory democracy.

11

Conclusion

Begin at the beginning and go on until you come to the end; then stop.
Lewis Carroll

Technology is making the practical implementation of theoretical democratic ideas practicable. This is stretching our current understanding of democracy in practice. As demonstrated in this thesis, the regulator is working to cope with these changes. The general conclusion of this thesis is that the level of *Participation*, *Communication*, *Integrity*, *Property*, *Access* and *Autonomy* are negatively affected by the implementation of regulation of technology. This negative effect is judged by the disincentive for the use of technology in the participatory democracy.

As this work has shown, attempts to regulate disruptive technology are tantamount to attempting to standardise the forms in which the disruptive technology can be used. This can be seen as a form of limitation of the non-conformist, and maybe innovative, uses that technology are put to by groups using the technology.

Our technological systems create and form social orders that both enable and control the way in which social behaviour may take place. When such technological systems enable users to interact in new ways they also have an effect of disrupting established social interactional norms. In the case of participatory democracy this work has observed that technological systems are in position to allow a greater amount of participation to a larger group of users than ever before.

By allowing a greater amount of users to participate via technological systems the technology provides the infrastructure upon which democratic ideals may be put into a practice. This work argues that the understanding of democratic values of *Participation*, *Communication*, *Integrity*, *Property*, *Access* and *Autonomy* are being challenged by the fact that technological systems are allowing their implementation in new ways.

Because of this increased citizen activity in the democracy, regulators are faced with the task of re-appraising the democratic core values that are the basis for much of our social understanding of society. The situation is a complex one. If the democratic values are to be upheld then the regulator must accept both the positive and negative effects. If the negative effects of disruptive technology lead to the conclusion that the democratic values cannot be fully accepted this must then be interpreted as a rejection of participatory democracy ideal on ideological, not on technical grounds. Much of the regulation of disruptive technology thus far has been a compromise where the rhetoric of democracy is maintained while its substance is denied.

The desire of states to implement ICT has been to a large extent driven by the desire to reduce communications costs between the state and citizen. This therefore means that the goal does not necessarily include a variety of forms of interaction and communication but rather the goal is one of standardisation. Standardisation is not a fertile field where individualism or innovation easily grows.

In closing, the question must be asked – what does it all mean? The arrival of new technology whether the printing press or the Internet disrupts the traditional manner in which society arranges and negotiates established social institutions. The early period of a new technology causes little problems since the technology is relatively new, has a low impact, and the user group is more easily regulated due to its homogenous nature. The desire for regulation does not occur prior to the advent of the socially disruptive effects of the technology. Additionally, as seen in these cases studies, technology does not appear to disruptive before larger groups of users begin to adopt the technology. Once the realisation that this new disruptive technology requires regulation appears there seems to be a corresponding desire to overregulate. To a large extent this is due to the fact that the need and basis of this regulation is insufficiently explored and usually based upon specialised lobby groups or wider moral panics within society.

To counteract the negative effects of regulation of disruptive technology described in this thesis it is necessary that the regulator and, to a larger extent, society act in such a way as to stop the discrimination against online participation in the participatory democracy. The regulator must understand that participation in the online democracy is no longer, if it ever has been, a matter of citizens communicating online with authorities. The participatory democracy is a form of social interaction similar, but also vastly different to, the newspaper, social club, television, school, workplace etc.

To be able to stop this discrimination the regulator must come to accept a certain level of disorder. Most of us are condition to accept order as a positive value and disorder as a negative value. This is an oversimplification. Offline interaction contains large elements of disorganisation and so must online interaction. Without the space for disorder the online interaction will not be able to develop successfully and grow into its potential benefit to the participatory democracy. This includes the unorthodox or unconventional use of technology. Using technology in an unorthodox manner should not be seen as a negative use of technology. By allowing the unorthodox use of technology the regulator not only allows the users to explore and develop themselves but the regulator also provides a fruitful testing ground for new developments within the socio-technical field.

Therefore the practical conclusions of this thesis are as follows: (1) the regulator must learn to accept alternative uses of technology. This entails the adoption of an unbiased or functional equivalency attitude towards technology. (2) Citizens should be encouraged to participate in difficult technical decisions rather than referring tough questions to experts. (3) The regulator must accept users participating directly in the regulatory process. (4) Both regulators and users must develop a tolerance towards unconventional uses of technology.

These four recommendations (non-discrimination, citizen participation, regulator-citizen cooperation in regulation, tolerance towards unconventional technology uses) are to be understood in such a way as to inform the regulatory structure and enable the development of regulation, which treats online environments in a manner that is functionally equivalent to their offline relations.

The future role of information technology within the participatory democracy is not under question in this thesis. It is clear that this technology is being used for social interaction on a wide scale and that it will not cease to do so even if the regulation of its use is seriously curtailed. The question is what role this disruptive technology will continue to play in the participatory democracy? Whether the regulatory structures will embrace the technology as an important source of interaction and development or whether the technology will be discarded? Embracing the disruptive technology requires that the state becomes more tolerant to the technology and permit wider uses beyond those specified in the present day policy documents. Discarding the technology entails a limited, regulated use but will fail to recognise the full potential of disruptive technologies as an agent of change within the participatory democracy.

12

Bibliography

Akdeniz, Y. (2005) *An Advocacy Handbook for the Non Governmental Organisations*, December 2003, (Updated and revised in October 2005), Cyber-Rights & Cyber-Liberties. URL: http://www.cyber-rights.org/cybercrime/coe_handbook_crcl.pdf.

Alvesson, M. & Willmott, H. (1992) *Critical Management Studies*, London: Sage.

Anti-Terrorism, Crime and Security Act of 2001, United Kingdom legislation. Url: http://www.opsi.gov.uk/ACTS/acts2001/20010024.htm.

Anttiroiko, A-V. (2001) "Towards the European Information Society", *Communications of the ACM*, Vol. 44, No. 1, pp. 31-35.

Anonymous (2004) "BT acts against child porn sites", *BBC News* 8 June. URL: http://news.bbc.co.uk/1/hi/technology/3786527.stm.

Aoki, K. (1998) "Considering Multiple and Overlapping Sovereignties: Liberalism, Libertarianism, National Sovereignty, "Global" Intellectual Property, and the Internet", 5 *Indiana Journal of Global Legal Studies* 443.

Argyris, C. & Schon, D. (1974) *Theory in practice: Increasing professional effectiveness.* San Francisco: Jossey Bass.

Arne, P. H. & Bosse, M. M. (2003) "Overview of Clickwrap Agreements," *Practising Law Institute*, January–March.

Asaro, P. (2000) "Transforming Society by Transforming Technology: The science and politics of participatory design", *Accounting Management and Information Technology*, 10, pp. 257-290.

Åström, J. (2004) *Mot en digital demokrati – Teknik, politik och institutionell förändring*, Doctoral Dissertation, Dept. of Social Sciences, Örebro Universtity.

Atkinson, P. & Coffey, A. (2004) "Analysing documentary realities", in Silverman, D. (ed) *Qualitative Research: Theory, Method and Practice*, London: Sage Publications.

Austin, J. (1998 [1832]) *The Province of Jurisprudence Determined*, Indianapolis: Hackett Publishing Inc.

Awad, N. F. & Fitzgerald, K. (2005) "The Deceptive Behaviours that Offend us the most About Spyware", *Communications of the ACM*, Vol. 48, No. 8, August, pp. 55-60.

Barber, B. (1984) *Strong Democracy: Participatory Politics for a New Age*. Los Angeles: University of California Press.

Barbook, R. (1998) "The Hi-Tech Gift Economy", *First Monday*, Vol. 3 Number 12, December. URL: http://www.firstmonday.dk/issues/issue3_12/barbrook/.

Baldwin, R. (1995) *Rules and Government*, Oxford: Oxford University Press.

Baldwin, R., Scott, C. & Hood C. (1998) *A Reader on Regulation*, Oxford: Oxford University Press.

Balkin, J. M. (1998) *Cultural software: A theory of ideology*. New Haven, Connecticut: Yale University Press.

Balkin, J. M. (2004) "Virtual Liberty: Freedom to Design and Freedom to Play in Virtual Worlds", *Virginia Law Review*, Vol. 90, No 8, December.

Barlow, J. P. (1996) *A Declaration of the Independence of Cyberspace*, Self-published manifesto, Electronic Frontier Foundation.

Barnett, S. (1997) "New Media, Old Problems: New Technology and the Political Process", *European Journal of Communication*, Vol. 12(2), pp. 193-218.

Bauhn, P. (1989) *Ethical aspects of political terrorism*, 1 *Studies in Philosophy*, Lund: Lund University Press.

Beck, U. (1992) *Risk Society – Towards a New Modernity*, London: Sage Publications.

Beckman, S. (1995) "En världsbildande teknik", in Karlsson, M. & Sturesson, L. (eds). *Världens största maskin. Människan och det globala telekommunikationssystemet*, Stockholm: Carlsson.

Bedau, H. A. (1961) "On Civil Disobedience", *Journal of Philosophy*, Vol. 58, pp. 653-665.

Bedau, H. A. (1970) "Civil Disobedience and personal responsibility for injustice", *The Monist*, 54, reprinted in Bedau, H. A. (ed) *Civil Disobedience in Focus*, London: Routledge.

Bedua, H. A. (1991) "Introduction", in Bedau, H. A. (ed) *Civil Disobedience in Focus*, London: Routledge.

Beniger, J. (1986) *The Control Revolution: Technological and Economic Origins of the Information Society*, Cambridge, Mass.: Harvard University Press.

Benkler, Y. (2006) *The Wealth of Networks - How Social Production Transforms Markets and Freedom*, New Haven: Yale University Press.

Bentham, J. (1995 [1787]) "Panopticon or Inspection-House" in Bozovik, M. (ed) *The Panopticon Writings*, Bozovik, M. (ed), London: Verso Books.

Berger, P. L. & Luckman, T. (1967) *The social construction of reality: A treatise in the sociology of knowledge*, London: Penguin.

Berlin, I. (2002 [1969]) "Four Essays on Liberty" in Hardy, H. (ed) *Liberty*, Oxford: Oxford University Press.

Beyleveld, D. & Brownsword, R. (2001) *Human Dignity in Bioethics and Biolaw*, Oxford: Oxford University Press.

Biegel, S. (2001) *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace*, Cambridge, Mass.: MIT Press.

Bimber, B. (1998) "The Internet and Political Transformation: Populism, Community, and Accelerated Pluralism", *Polity*, 31, No 1, Fall, pp. 133-160.

Bimber, B. (2001) "Informational and Political Engagement in America: The Search for Effects of Informational Technology at the Individual Level", *Political Research Quarterly*, Vol. 54, No. 1, March, pp. 53-67.

Birnhack, M. D. & Elkin-Koren, N. (2003) "The Invisible Handshake: The Reemergence of the State in the Digital Environment", 8 Va. *J.L. & Tech.* 6.

Bjerknes, G. & Bratteteig, T. (1995) "User Participation and Democracy: A Discussion of Scandinavian Research on System Development", *Scandinavian Journal of Information Systems*, 7(1), pp. 73-98.

Bjerknes, G., Ehn, P., & Kyng, M. (eds) (1987*) Computers and Democracy – a Scandinavian Challenge*, Avebury: Aldershot.

Black, J. (1997) *Rules and Regulators,* Oxford: Oxford University Press.

Black, J. (2002) "Critical Reflections on Regulation", *Australian Journal of Legal Philosophy*, 27, pp. 1-37.

Blanke, J. M. (2006) "Robust Notice and Informed Consent, The Keys to Successful Spyware Legislation", *Columbia Science and Technology Law Review,* Vol. 7, pp. 1-33.

Bloor, D. (1997) *Wittgenstein: Rules and Institutions*. London: Routledge.

Boas, T. & Kalathil, S. (2003) "Open networks, closed regimes: The impact of the Internet on authoritarian rule", *First Monday*, Vol. 8, number 1 (January). URL: http://www.firstmonday.dk/ISSUES/issue8_1/kalathil/.

Bobzien, S. (2001) *Determinism and freedom in stoic philosophy*, Oxford: Oxford University Press.

Bond, G. W. (2005) "Software as Art – Encouraging a greater appreciation of the interplay between software and fine art", *Communications of the ACM*, Vol. 48, No. 8, August, pp. 118-124.

Bontchev, V. (1996) "Are 'Good' Computer Viruses Still a Bad Idea?" in *Proceedings of EICAR 1994*, St Albans, U.K.

Bontchev, V. (2003) "Should We Teach Virus Writing?" *Proceedings of AVAR 2003*, Sydney, Australia.

Bowrey, K. (2005) *Law & Internet Cultures*, Cambridge: Cambridge University Press.

Boyle, J. (1996) *Shamans, Software & Spleen: Law and the Construction of the Information Society*, Cambridge, Mass.: Harvard University Press.

Boyle J. (ed) (2003) *Law and Contemporary Problems special issue on the Public Domain*, Vol. 66, Winter/Spring.

Braithwaite, J. & Drahos, P. (2000) *Global Business Regulation*, Cambridge: Cambridge University Press.

Branscombe, A. (1995) "Rogue Computer Programs and Computer Rogues: Tailoring the Punishment to Fit the Crime", in Johnson & Nissenbaum (eds) *Computer Ethics & Social Values*, Englewood Cliffs, N.J.: Prentice Hall.

Brill, M. (1989) "Transformation, nostalgia, and illusion in public life and public place", in Altman, I. & Zube, E. H. (eds), *Public places and Spaces,* New York: Plenum.

Brown, P. (2002) "Validity of clickwrap licenses," *Practicing Law Institute*, PLI Order No G0-0124.

Brownsword, R. (2005) "Code, Control and Choice: Why East is East and West is West", *Legal Studies*, Vol. 25, No 1, March, pp. 1-21.

Bygrave, L. (2002) *Data Protection Law: Approaching its Rationale, Logic and Limits*, The Hague: Kluwer Law International.

Cardoso, G. & Periera Neto, P. (2004) "Mass Media Driven Mobilization and Online Protest", in van de Donk, W. *et al* (eds) *Cyberprotest – New Media, Citizens and Social Movements*, London: Routledge.

Carr, S., Francis, M., Rivlin, L.G. & Stone, A.M. (1992) *Public Space,* Cambridge: Cambridge University Press.

Carter, G. (2002) "It's my time and I'll sell if I want to", *The Adrenaline Vault*, March 28.

Castells, M. (1996) *The Information Age: Economy, society, and culture, Volume 1: The Rise of the Network Society*, Oxford: Blackwell.

Castells, M. (1997) *The Information Age: Economy, society, and culture, Volume 2: The Power of Identity,* Oxford: Blackwell.

Castells, M (2001) *The Internet Galaxy: Reflections on the Internet, Business, and Society*, Oxford: Oxford University Press.

Castronova, E. (2001) "Virtual worlds: A first-hand account of market and society on the cyberian frontier", *CESifo Working Paper No. 618*, December 2001.

Castronova, E. (2003) "The price of 'man' and 'woman': a hedonic analysis of avatar attributes in a virtual world", *CESifo Working Paper No. 957*, May.

Cave, D. (2001) "The Parasite Economy", August 02, *Salon.com.* URL: http://archive.salon.com/tech/feature/2001/08/02/parasite_capital/.

CDT & EFF (2003) *Open Letter to The Honorable George E. Pataki*, Center for Democracy and Technology and Electronic Freedom Frontier, March.

Chadwick, A. & May, C. (2003) "Interaction between States and Citizens in the Age of Internet: "e-Government", in the United States, Britain, and the European Union", *Governance: An International Journal of Policy, Administration, and Institutions*, Vol. 16, No. 2, April.

Changsha (2005) Changsha Intermediate People's Court of Hunan Province, Criminal Division One First Trial Case No. 29.

Christensen, C. & Bower, J. (1996) "Customer Power Strategic Investment and the Failure of Leading Edge Firms", *Strategic Management Journal*, 17, pp. 197-218.

Christensen, C. (1997) *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*, Cambridge, Mass.: Harvard Business School Press.

Christman, J. (1991) "Liberalism and individual positive freedom", *Ethics*, Vol. 101 (January), pp. 343–359.

Churchill, W. S. (1952) *The Second World War, Volume V: Closing the Ring*, London: Cassell & Co ltd.

Ciborra, C. (1992) "From Thinking to Tinkering: The Grassroots of Strategic Information Systems", *The Information Society* 8, pp. 297-309.

Ciborra, C. (2005) "Interpreting e-government and Development", *Information Technology and People*, Vol. 18, No. 3, pp. 260-279.

Clarke, I. & Sandberg, O. (2005) "Routing in the Dark - Scalable Searches in Dark Peer to Peer Networks", *Defcon 13*, Las Vegas, July 2005.

Coase, R. (1960) "The Problem of Social Cost", *Journal of Law and Economics*, 3, pp. 1-44.

Cohen, F. B. (1994) *A Short Course on Computer Viruses*, 2nd edition, New York: Wiley Publishing.

Coke Ellington, T. (2004) *Official Secrecy: Self, State and Society*, Doctoral Dissertation, Political Science, University of Maryland.

Colombell, M (2002) "The Legislative Response to the Evolution of Computer Viruses", *Richmond Journal of Law and Technology*, Spring.

Convention on Cyber Crime, (adopted 8 November 2001) Budapest, 23.XI.2001. URL: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.

Cook, T. E. & Morgan, P. M. (1971) *Participatory Democracy*, San Francisco: Canfield Press.

Cowan Schwartz, R. (1983) *More Work for Mother: The Ironies of Household Technology from the Open Hearth to the Microwave*, New York: Basic Books.

Critical Art Ensemble (1996) *Electronic Civil Disobedience and Other Unpopular Ideas*, New York: Autonomedia.

Crotty, S. F. (2002) "The how and why of shrinkwrap licence validation under the Uniform Computer Information Transactions Act", *Rutgers Law Journal*, Vol. 33, Spring, pp. 745–770.

Dahl, R. A. (1998) *On Democracy,* New Haven: Yale University Press.

Dahl, R. A. (1989) *Democracy and its Critics*, New Haven: Yale University Press.

Dahl, R. A., Shapiro, I. & Cheibub, J. (eds) (2003) *The Democracy Sourcebook*, Cambridge, Mass.: The MIT Press.

Dahlbom, B. & Janlert, S. (1996) *Computer Future*, Dept of Informatics, University of Göteborg.

Daneke, G. A., Garcia, M. W. & Priscoli, J. D. (1983) *Public Involvement and Social Impact Assessment*, Boulder, Colorado: Westview Press.

Danish Board of Technology (2002) *Open-source software in e-government, Analysis and recommendations drawn up by a working group under the Danish Board of Technology*, October 2002. URL: http://www.tekno.dk/pdf/projekter/p03_opensource_paper_english.pdf

Datastraffrättsutredning SOU 1992:110.

David, P. A. (2000) "Path dependence, its critics and the quest for 'historical economics'", in Garrouste, P. & Ioannides, S. (eds), *Evolution and Path Dependence in Economic Ideas: Past and Present*, Cheltenham: Edward Elgar Publishing.

Deibert, R. (2002) "Dark Guests and Great Firewalls: The Internet and Chinese Security Policy", *Journal of Social Issues*, Vol. 58, Number 1, January, pp. 143-159.

Deibert, R. & Villeneuve, N. (2005) "Firewalls and Power: An Overview of Global State Censorship of the Internet", in Klang & Murray (eds) *Human Rights in the Digital Age* London: Glasshouse Press.

Demokratiutredningen (2000) En uthållig demokrati! Politik för folkstyrelse på 2000-talet, Demokratiutredningens betänkande, SOU 2000:1.

Denning, D. (2000) "Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism", *Committee on Armed Services, US House of Representatives*, May. URL: www.cs.georgetown.edu/~denning/infosec/cyberterror.html.

Dent, C. & Kenyon, A. (2004) "Defamation Law's Chilling Effect: A Comparative Content Analysis of Australian and US Newspapers", *Media & Arts Law Review*, Vol. 9, No. 2, pp. 89-112.

DeSanctis, G. & Poole, M. S. (1994) "Capturing the Complexity in Advanced Technology Use: Adaptive structuration theory", *Organization Science*, 5(2), pp. 121-147.

de Sola Pool, I. (1984) *Technologies of Freedom*, Cambridge, Mass.: Harvard University Press.

Dienel, P. C. (1989) "Contributing to social decision methodology: citizen reports on technological projects", in Vlek, C. & Cvetkovich, G. (eds) *Social Decision Methodology for Technological Projects,* Dordrecht, The Netherlands: Kluwer Academic.

Di Lello, E. V. (1993) "Functional Equivalency and Its Application to Freedom of Speech on Computer Bulletin Boards", *Columbia Journal of Law and Social Problems*, Vol. 26, pp. 199-247.

DiMaggio, P., Hargiattai, E., Neuman, W. R. & Robinson, J. P. (2001) "Social Implications of the Internet", *Annual Review of Sociology*, 27, pp. 307–336.

Dogan, S. & Lemley, M. (2004) "Trademarks and Consumer Search Costs on the Internet", 41 *Houston Law Review*, pp. 777-838.

Dutton, W. H. (1999) "The Virtual Organisation: Tele-Access in Business and Industry", in DeSanctis, G. & Fulk, J. (eds.), *Shaping Organisation Form: Communication, Connection and Community*, pp. 473-495. London: Sage.

Dworkin, G. (1988) *The Theory and Practice of Autonomy,* Cambridge: Cambridge University Press.

Dworkin, R. (1978) *Taking Rights Seriously*, Cambridge, Mass.: Harvard University Press.

Dyson, E., Gilder, G. & Toffler, A. (1994) "Cyberspace and the American Dream: A Magna Carta for the Knowledge Age", *Future Insight*, Release 1.2 n August.

Easterbrook, F. H. (1996) "Cyberspace and the Law of the Horse", *University of Chicago Legal Forum,* 207.

eEurope (2000) *eEurope 2002: An Information Society for All*, An Action Plan prepared by the Council and the European Commission for the Feira European Council, 19-20 June.

eEurope (2002) *eEurope 2005: An Information Society for All*, An Action Plan to be presented in view of the Sevilla European Council, 21-22 June.

Ehn, P. (1989) *Work-Oriented Design of Computer Artefacts*, New Jersey: Lawrence Erlbaum Associates.

EFF & OPG (2003) *Internet Blocking in Public Schools: A Study on Internet Access in Educational Institutions*, Report from the Electronic Frontier Foundation (EFF) and the Online Policy Group (OPG), Version 1.1 of 26 June.

EFF (2005) *How to Blog Safely (About Work or Anything Else)*, Electronic Frontier Foundation Report, April 6. URL: http://www.eff.org/Privacy/Anonymity/blog-anonymously.php.

Eisenstein, E. (1979) *The printing press as an agent of change – communications and cultural transformations in early modern Europe*, Cambridge: Cambridge University Press.

Electrohippies (2000) *DJNZ & the action tool development group. Client-side Distributed Denial-of-Service: Valid campaign tactic or terrorist act?* The Electrohippie Collective Occasional paper no.1, February. URL: http://www.fraw.org.uk/ehippies/papers/op1.html.

Electrohippies (2003) *Electrohippie Collective's online protest against the Iraq War*, The Electrohippie Collective. URL: http://www.internetrights.org.uk/casestudies.shtml.

Ellickson, R. C. (1991) *Order Without Law: How Neighbors Settle Disputes*, Cambridge, Mass.: Harvard University Press.

Eneman, M. (2005) "Blockering av barnpornografisajter ingen lösning", *SVT Debatt,* 19 April 2005. URL: http://svt.se/svt/jsp/Crosslink.jsp?d=35188&a=388657.

Esler, B. (2005) "Filtering, Blocking and Rating: Chaperones or Censorship?", in Klang & Murray (eds) *Human Rights in the Digital Age,* London: Glasshouse Press.

Etzioni, A. (1999) *The Limits of Privacy,* New York: Basic Books.

Fagelman, T. (2004) "Commercialising the database: Commercialising the CAI Database Policy recommendations", *Internet Watch Foundation*, November. URL: http://www.iwf.org.uk/corporate/page.121.251.htm.

Feenberg, A. (2002) *Transforming Technology: A Critical Theory Revisited*, Oxford: Oxford University Press.

Field Guidance (2001) on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA PATRIOT Act of 2001. URL: http://www.cybercrime.gov/PatriotAct.htm.

Fiorino, D. (1990) "Citizen participation and environmental risk: A survey of institutional mechanisms" *Science, Technology, and Human Values* 15(2), pp. 226-244.

Fortier, F. (2001) *Virtuality Check: Power Relations and Alternative Strategies in the Information Society,* London: Verso.

Foster, R. (1986) *Innovation, the attackers advantage*, New York: Summit Books.

Foucault, M. (1979) *Discipline & Punish: The birth of the prison*, New York: Vintage Books.

Foucault, M. (1980) *Power, knowledge: selected interviews and other writings 1972-1977*, Gordon, C (ed & trans), New York: Pantheon.

Foucault, M. (1991) "Governability", in Burchell, G., Gordon, C. & Miller, P. (eds) *The Foucault Effect: Studies in Governmentality*, London: Harvester Wheatsheaf.

Franz, C. R. & Robey, D. (1984) "An investigation into user-led systems design: rational and political perspectives", *Communications of the ACM*, 27(12), pp. 1202-1209.

Freeman, L. A. & Urbaczewski, A. (2005) "Why Do People Hate Spyware?", *Communications of the ACM*, Vol. 48, No. 8, August.

Freerk (2005) *HOWTO bypass Internet Censorship*. URL: http://www.zensur.freerk.com/.

Fried, C. (1970) *An Anatomy of Values: Problems of Personal and Social Choice*, Cambridge, Mass.: Harvard University Press.

Friedman, M. (1993 [1970]) "The Social Responsibility of Business is to Increase Its Profits" New York Times Magazine, (1 September 1970). Reprinted in Beauchamp, T. & Bowie, N. (eds) *Ethical Theory and Business*, Englewood Cliffs, N.J.: Prentice-Hall.

Froomkin, A. M. (1997) "The Internet as a Source of Regulatory Arbitrage", in Kahin B. & Nesson, C. (eds) *Borders in Cyberspace: Information Policy and the Global Information Infrastructure*, Cambridge, Mass.: MIT Press.

Fuller, L. (1964) *The Morality of Law,* New Haven: Yale University Press.

Furmston, M. P. (1996) *Cheshire, Fifoot & Furmston's Law of Contract*, London: Butterworths.

Gambetta, D. (1988) "Mafia: the Price of Distrust", in Gambetta (ed) *Trust: Making and Breaking Cooperative Relations*, Oxford: Blackwell.

Gauthier, D. (1986) *Morals by Agreement*, Oxford: Clarendon Press.

Gearty, C. (2003) "Terrorism and morality", *European Human Rights Law Review*, Vol. 8, pp. 377-383.

Gehl, J. (1994) *Places for People*, Melbourne: Melbourne City Council.

Ghosh, R.A., Krieger, B., Glott, R. & Robles, G. (2002) *Free/Libre and Open Source Software: Survey and Study. Part 2B: Open Source Software in the Public Sector: Policy within the European Union*, June. URL: http://www.infonomics.nl/FLOSS/report/FLOSSFinal_2b.pdf.

Gibson, S. (2002) "The strange tale of the denial of service attacks against grc.com", *Gibson Research Corporation*. URL: http://iso.grc.com/dos/grcdos.htm.

Giddens, A. (1984) *The Constitution of Society*, Berkeley: University of California Press.

Giddens, A. (1990) *The Consequences of Modernity*, Cambridge: Polity Press.

Gomulkiewicz, R. W. & Williamson, M. (1996) "A brief defence of mass market software licence agreements", *Rutgers Computer & Technology Law Journal*, Vol. 22, pp. 335–367.

Gonner, E.C.K. (1912) *Common Land and Inclosure*, London: Macmillan and Co.

Gordley, P. (1991) *The Philosophical Origins of the Modern Contract Doctrine*, Oxford: Clarendon Press.

Grönlund, Å. (1994) *Public Computer Systems, the Client-Organizational Encounter, and the Societal Dialogue*, Doctoral Dissertation, Department of Informatics, Umeå University.

Grönlund, Å., Ranerup, A. & Gustavsson, P. (2003) *IT och demokrati, Delrapport till ITPS utvärdering av den svenska IT-politiken*, A2003:015.

Habermas, J. (1974) "The public sphere: An encyclopedia article", *New German Critique*, 3, 49-55. Reprinted in 2000, *Democracy: A reader*, Blaug, R. & Schwarzmantel, J. (eds.), New York: Columbia University Press.

Habermas, J. (1984) *The Theory of Communicative Action, Volume One: Reason and the Rationalization of Society*, Boston: Beacon Press.

Habermas, J. (1989) *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*, Thomas, B. (trans), Cambridge, MA: MIT Press.

Hadfield, C. (1959) *British Canals – an illustrated history*, London: Phoenix House.

Hamilton, S. (2003) "The War on Terrorism – Towards a 'less free, less choice' Internet for Library Users?", *World Library and Information Congress: 69th IFLA General Conference and Council*, August, Berlin.

Hamilton, S. (2004) *To what extent can libraries ensure free, equal and unhampered access to Internet-accessible information resources from a global perspective?,* Doctoral Dissertation, Department of Library and Information Management, Royal School of Library and Information Science, Copenhagen, Denmark.

Hammersley, M. (1990) *Reading Ethnographic Research: A Critical Guide*, London: Longmans.

Hammersley, M. & Atkinson, P. (1995) *Ethnography: Principles in Practice,* (2nd ed) London: Routledge.

Hanseth, O. (1996) *Information technology as Infrastructure*, Doctoral Dissertation Gothenburg studies in Informatics (Report 10), December.

Hanseth, O. (2000) "The Economics of Standards", in Ciborra, C. (ed.) *From Control to Drift: The Dynamics of Corporate Information Infrastructures*, Oxford: Oxford University Press.

Hanseth, O., Monteiro, E. & Hatling, M. (1996) "Developing Information Instructure: The Tension Between Standardisation and Flexibility", *Science, Technology and Human Values*, Vol. 21, No. 4, Fall, pp. 407-426.

Hardin, G. (1968) "Tragedy of the Commons", *Science*, Vol. 162, pp. 1243–1248.

Harris, J. W. (1996) *Property and justice*, Oxford: Oxford University Press.

Harrison, R. (1995) *Democracy*, London: Routledge.

Hart, H. L. A. (1994) *The Concept of Law*, 2nd edition, Oxford: Clarendon Press.

Hawking, S. (1994) "Life in the Universe", *Public Lectures*, reprinted in *Scientific American*, October.

Heins, M. (2003) "The Progress of Science and Useful Arts: Why copyright today threatens intellectual freedom", *Free Expression Policy Project* (policy paper). URL: http://www.fepproject.org/policyreports/copyright2dexsum.html.

Heng M. S. H. & de Moor, A. (2003) "From Habermas's communicative theory to practice on the internet", *Information Systems Journal* (2003) 13, pp. 331–352.

Hick, S. & Teplitsky, A. (2000) "Internet Solidarity: Grassroots Movement Struggles for Human Rights", in Hick, S., Halpin, E. & Hoskins, E. (eds), *Human Rights and the Internet*, London: Macmillan Press.

Hirschheim, R. & Klein, H. K. (1989) "Four paradigms of information systems development", *Communications of the ACM*, 32, pp. 1199–1216.

Hodder, I. (1994) "The Interpretation of Documents and Material Culture", in Denzin, N. K. and Lincoln, Y. S. (eds) *Handbook of Qualitative Research.* California: Thousand Oaks.

Homeland Security Act of 2002, Pub. L. No. 107-296, §§ 223, 225, 235, 116 Stat. 2135 (2002).

Hughes, J. (1988) "The Philosophy of Intellectual Property", 77 *Georgetown Law Journal*, Vol. 77, pp. 287-366.

Hughes, T. P. (1987) "The Evolution of Large Technological Systems", in W. Bijker, T, Hughes, T. P. & Pinch, T. (eds.), *The Social Construction of Technological Systems*, Cambridge, MA.: MIT Press.

Hughes, T. P. (2004) *Human-Built World – How to think about technology and culture*, Chicago: University of Chicago Press.

Hume, D. (1978 [1739]) *A Treatise of Human Nature*, Selby-Bigge, L. A. & Nidditch, P. H. (eds) Oxford: Oxford University Press.

Ilshammar, L. (2002) *Offentlighetens nya rum, Teknik och politik i Sverige 1969-1999,* Doctoral Dissertation, Örebro universitet.

Information Commissioners (2003) *Guidance to the Privacy and Electronic Communications* (EC Directive) Regulations 2003 - Part 1. URL: http://www.informationcommissioner.gov.uk.

Jefferson, T. (1903 [1813]) "Letter from Thomas Jefferson to Isaac McPherson" (13 August 1813), in Lipscomb, A. & Bergh, A. (eds), *Writings of Thomas Jefferson*, Washington, D.C.: Thomas Jefferson Memorial Association of the United States, Vol. 6, pp. 330, 333–334.

Joerges B. (1999) "Do Politics have Artefacts?", *Social Studies of Science*, Vol. 29, No. 3, pp. 411-431.

Johnson, W. J. (ed.) (1994) *The Bhagavad Gita*, Oxford: Oxford University Press.

Johnson, D. R. & Post, D. G. (1996) "Law and Borders: The Rise of Law in Cyberspace", 48 *Stan. L. Rev.* 1367.

Johnson, D. R. & Post, D. G. (1998) "The New 'Civic Virtue' of the Internet: A Complex Systems Model for the Governance of Cyberspace", in Firestone, C. (ed) *The Emerging Internet,* Annual Review of the Institute for Information Studies.

Johnsson, D. & Bimber, B. (2004) "The Internet and Political Transformation Revisited" in Feenberg, A. & Barney D. (eds) *Community in the Digital Age*, Lanham: Rowman & Littlefield.

Kahn, R. & Kellner, D. (2004) "Virtually Democratic: Online Communities and Internet Activism", in Feenberg, A. & Barney D. (eds) *Community in the Digital Age*, Lanham: Rowman & Littlefield.

Kallinikos, J. (2002) "Re-opening the Black Box of Technology: Artifacts and Human Agency", *23rd ICIS*, Barcelona, 14-18 December.

Kallinikos, J. (2005) "The Order of Technology: Complexity and control in a connected world", *Information and Organization*, Vol. 15, pp. 185–202.

Kant, I. (2003 [1781]) *Critique of Pure Reason*, Hampshire: Palgrave Macmillan.

Katz, J. (1997) "Birth of a Digital Nation", *Wired Magazine*, Issue 5.04, April.

Keighley, G. (2002) "The sorcerer of Sony", *Business 2.0 Media Inc.*, August. URL: http://www.business2.com/articles/mag/0,1640,42210,FF.html.

Kelly, R. V. (2004) *Massively Multiplayer Online Role-Playing Games: The People, the Addiction and the Playing Experience,* Jefferson North Carolina: McFarland & Company.

Kelman, A. (1997) "The Regulation of Virus Research and the prosecution for unlawful research?", Commentary, 1997 (3) *The Journal of Information, Law and Technology*. URL: http://elj.warwick.ac.uk/jilt/compcrim/97_3kelm/.

Kern, S. (1983) *The Culture of Time and Space 1880-1918*, Cambridge, MA: Harvard University Press.

Kerr, O. (2003) "Cybercrime's scope: interpreting 'access' and 'authorization' in computer misuse statutes", *New York University Law Review* November v78.

King, M. (1991 [1963]) "Letter from Birmingham City Jail", in Bedau, H (ed), *Civil Disobedience in Focus*, New York: Routledge.

Klang, M. (2001) "Who do you Trust? Beyond encryption, secure e-business", *Decision Support Systems,* Vol. 31, pp. 293-301.

Klang, M. & Roos, F. (2001) "Copyright in the age of disruptive technologies", in *Proceedings of IFIP TC8 Working Conference on E-Commerce/E-Business (EC/EB)*, Salzburg.

Klang, M. (2003a) "A Critical Look at the Regulation of Computer Viruses", *International Journal of Law and Information Technology*, Vol. 11, No 2, pp. 162-183.

Klang, M. (2003b) "Spyware: Paying for Software with our Privacy", *International review of law computers and technology*, Vol. 17, Number 3, November, pp. 313-322.

Klang, M. (2004a) "Civil Disobedience Online", *Journal of Information, Communication & Ethics in Society*, Vol. 2: Issue 2: Paper 2, pp. 75–83.

Klang, M. (2004b) "Spyware – the ethics of covert software", *Ethics and Information Technology*, Issue 3, September, pp. 193-202.

Klang, M. (2004c) "Avatar: From Deity to Corporate Property", *Information, Communication & Society*, Vol. 7, Number 3, pp. 389- 402.

Klang, M. (2005a) "Virtual Sit-Ins, Civil Disobedience and Cyberterrorism", in Klang, M. & Murray, A. (eds) *Human Rights in the Digital Age*, London: Cavendish Publishing.

Klang, M. (2005b) "Free Software & Open Source: The Freedom Debate and its Consequences", *First Monday*, Vol. 10, number 3 (March). URL: http://www.firstmonday.org/issues/issue10_3/klang/.

Klang, M. (2006) "Online Censorship & Democracy", *IFIP-TC9 HCC7 Social Informatics: An Information Society for All?*, Nova Gorica (Slovenia), Gorizia (Italy), September 21-23, Forthcoming.

Kling, R. (1992) "When Gunfire Shatters Bone: Reducing Sociotechnical Systems to Social Relations", *Science, Technology and Human Values* (17:3), pp. 381-385.

Kling, R., Rosenbaum, H. & Sawyer, S. (2005) *Understanding and Communicating Social Informatics*, N.J.: Information Today Inc.

Kollock, P. & Smith, M. A. (eds) (1998) *Communities in Cyberspace*, London: Routledge.

Kontio, J. (2004) *Diffusion of Database Innovations: A multiple case study in six Finnish organizations*, Doctoral Dissertation, Publications of the Turku School of Economic and Business Administration, Series A-16: 2004.

Kosak, D. (2002) "What's this world coming to? The future of massively multiplayer Games", *Gamespy.com*, 17 April.

Kramer, M. H. (2003) *The Quality of Freedom*, Oxford: Oxford University Press.

Krantz, M. (2002) "Video game college is 'boot camp' for designers", *USA Today*, 3 December.

Kristjánsson, K. (1996) *Social Freedom: The responsibility view*, Cambridge: Cambridge University Press.

Kroes, P. (1998) "Philosophy of Technology", in Graig, E. (ed), R*outledge Encyclopedia of Philosophy* 9, London: Routledge, pp. 284-288.

Krotoski, A. (2005) "$26,500 virtual property owner speaks", *Guardian Online*, June 16.

Kuhn, T. (1962) *The Structure of Scientific Revolutions*, Chicago: Chicago University Press.

Lakoff, G. (2004) *Don't Think of an Elephant: Progressive Values and the Framing Wars a Progressive Guide to Action*, White River Junction, VT: Chelsea Green Publishing.

Lakoff, G. & Johnsson, M. (1980) *Metaphors We Live By*, Chicago: Chicago University Press.

Lastowka, F. G. & Hunter, D. (2004) "The Laws of the Virtual Worlds", 92 *California Law Review*, Vol. 92, pp. 1-73.

Latour, B. (1991) "Technology is Society Made Durable", in Law, J. (ed) *A Sociology of Monsters: essays on power, technology and domination.* Sociology Review Monograph 38, London: Routledge.

Latour, B. (1992). "Where are the Missing Masses? Sociology of a Few Mundane Artefacts", in Bijker, W. & Law, J. (eds) *Shaping Technology, Building Society: Studies in Sociotechnical Change.* Cambridge, Mass: MIT Press.

Latour, B. (1999) *Pandora's Hope*, Cambridge, Mass: Harvard University Press.

Lessig, L. (1999) *Code and other laws of cyberspace*, New York: Basic Books.

Lessig, L. (1999a) *Code and the Commons*, Keynote Address Conference on Media Convergence, Fordham University Law School.

Lessig, L. (2001) *The Future of Ideas, The Fate of the Commons in a Connected World*, New York: Random House.

Lessig, L. (2004) *Free culture*: *How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity*, New York: Penguin Press.

Lincoln, Y. S. & Guba, E. G. (1985) *Naturalistic Enquiry*, Beverly Hills, CA: Sage.

Litman, J. (1990) "The Public Domain", *Emory Law Journal*, Fall.

Ljungberg, J. (2000) "Open Source Movements as a Model for Organising", *European Journal of Information Systems*, 2000/9, pp. 208-216.

Locke, J. (1960 [1690]) *Two Treatises on Civil Government*, Laslett, P. (ed) Cambridge: Cambridge University Press.

Luhmann, N. (1988) "Familiarity, Confidence, Trust: Problems and Alternatives", in Gambetta (ed) *Trust: Making and Breaking Cooperative Relations*, Oxford: Blackwell.

Lyytinen, K. (1987) "Different Perspectives on Information Systems: Problems and Solutions", *ACM Computing Surveys*, 19(1), pp. 5-46.

Lyytinen, K. & Klein, H. (1985) "The critical theory of Jurgen Habermas as a basis for a theory of information systems", in Mumford, E., Hirschheim, R., Fitzgerald, G. & Wood-Harper, A. T. (eds) *Research Methods in Information Systems,* Amsterdam: Elsevier Science Publishers.

Lyytinen, K. & Hirschheim, R. (1988) "Information systems as rational discourse: an application of Habermas' theory of communicative action", *Scandinavian Journal of Management*, 4, pp. 19–30.

Lyytinen, K. & Rose G. (2003a) "Disruptive Information System Innovation: The Case of Internet Computing", *Information Systems Journal*, 13, pp. 301-330.

Lyytinen, K. & Rose G. (2003b) "The Disruptive Nature of IT Innovations: The Case of Internet Computing in Systems Development Organizations", *MIS Quarterly*, Vol. 27, No. 4, pp. 557-595.

MacCallum Jr, G. C. (1967) "Negative and positive freedom", *Philosophical Review*, Vol. 76, pp. 312–334.

MacDonald, K. (2001) "Using Documents", in Gilbert, N. (ed) *Researching Social Life*, 2nd edition. London: Sage.

Magnusson Sjöberg, C. (1992) *Rättsautomation: Särskilt om statsförvaltningens datorisering*, Doctoral Dissertation. Stockholm: Norstedts Juridik.

Maher, I. (2002) "Competition law in the international domain: Networks as a new form of governance", *Journal of Law and Society*, Vol. 29, No. 1, pp. 112-136.

Manion, M. & Goodrum, A. (1999) "Terrorism and Civil Disobedience: Towards an International Ethic of Hacktivism", in *Proceedings of ETHICOMP.*

Månsson, T. (2004) *Olydnad – Civil olydnad som demokratiskt problem*, Doctoral Dissertation, Stockholm University, Stockholm: Thales Förlag.

Markham, A. N. (2004) "Internet Communication as a Tool for Qualitative Research", in Silverman, D. (ed) *Qualitative Research: Theory, Method and Practice*, London: Sage Publications.

Marx, K. (1978 [1844]) "On The Jewish Question", in Trucker, R. (ed), *The Marx-Engels Reader*, New York: W. W. Norton.

McLaughlin, A. (2006) "Google in China", *Google Corporate Blog - Googler insights into product and technology news and our culture*, 27 January. URL: http://googleblog.blogspot.com/2006/01/google-in-china.html.

McArthur, R. L. (2001) "Reasonable Expectations of Privacy", *Ethics and Information Technology*, 3, pp. 123–128.

McCormick, J. (1997) "Habermas's Discourse Theory of Law: Bridging Anglo-American and Continental Legal Traditions", *The Modern Law Review*, Vol. 60, pp. 734-743.

McLuhan, M. (1964) *Understanding Media: The Extensions of Man*, New York: Signet Books.

McQuail, D. (1984) *Communication*, 2nd edition, London: Longman Publishers.

Meikle, G. (2002) *Future Active: Media Activism and the Internet*, Sydney, Pluto Press.

Miles, S, (2002) "Ad-Aware Maker LavaSoft Frustrates Internet Advertisers", *The Wall Street Journal Online*. URL: http://online.wsj.com/article/0,,SB1035830...231.djm,00.html.

Mill, J. S. (1965 [1848]) "Principles of Political Economy", in Robson, J. M. (ed) *Collected Works*, Toronto: University of Toronto Press.

Mill, J. S. (1980 [1859]) *On Liberty*, New York: Penguin Books.

Milton, J. (1979 [1644]) *Areopagitica and On Education*, Sabine, G. (ed), Illinois: Harlan Davidson Inc.

Ministry of Modernisation (2005) *eNorway 2009 – the digital leap*. URL: http://odin.dep.no/filarkiv/254956/eNorway_2009.pdf.

Mitcham, C. (1994) *Thinking Through Technology: The Path Between Engineering and Technology*, Chicago: University of Chicago Press.

Mitchell, W. J. (1996) *City of bits: Space, place, and the Infobahn*, Cambridge, Mass.: MIT Press.

Moglen, E. (1999) "Anarchism triumphant: Free software and the death of copyright", *First Monday*, Vol. 4, number 8 (August). URL: http://www.firstmonday.org/issues/issue4_8/moglen/.

Monteiro, E. & Hanseth, O. (1995) "Social Shaping of Information Infrastructure: On Being Specific About the Technology", in Orlikowski, W., Walsham, G., Jones, M. R. and DeGross, J. I. (eds) *Information Technology and Changes in Organisational Work*, Chapman & Hall, 1995.

Murray, A. & Scott, C. (2001) "The Partial Role of Competition in Controlling the New Media", Presented at the *Competition Law and the New Economy*, University of Leicester (July).

Murray, A. (2002) "Free Expression and Censorship Through Design Protocols: A Misapplication of the ICANN UDRP", 17th *Proceedings of the Bileta Annual Conference.*

Murray, A. (2006) *The Regulation of Cyberspace: Control in the Online Environment*, London: Glasshouse Press.

Negroponte, N. (1996) *Being digital*, New York: Vintage Books.

Newman, M. & Noble, F. (1990) "User involvement in the interaction process", *Information Systems Research*, 1(1), pp. 89-113.

Ngwenyama, O.K. & Lee, A.S. (1997) "Communication richness in electronic mail: critical social theory and the contextuality of meaning", *MIS Quarterly*, 21, pp. 145–167.

NIPC (2001) *Cyber Protests: The Threat to the U.S. Information Infrastructure*, National Infrastructure Protection Center, 2001. URL: http://www.nipc.gov/publications/nipcpub/cyberprotests.pdf.

Nissenbaum, H. (1995) "Should I Copy My Neighbor's Software?", in Johnson, D. & Nissenbaum, H. (eds) *Computers, Ethics, and Social Responsibility*, New Jersey: Prentice-Hall.

Norman, D. (1990) *The Design of Everyday Things*, New York: Doubleday.

Norris, C. & Armstrong, G. (1999) *The Maximum Surveillance Society: The Rise of CCTV,* Oxford: Berg.

Norris, P. (2001) *Digital Divide? Civic Engagement, Information Poverty and the Internet Worldwide*, Cambridge: Cambridge University Press.

Norris, P. (2004) "Who Surfs Café Europa?", paper presented at the *Annual Meeting of the American Political Science Association* Atlanta.

Norris, P. (2004) "E-campaigning and e-democracy", in *Proceedings of Political Communications in the 21st Century*, New Zealand.

Norris, P. & Curtice, J. (2004) "If you build a political website, will they come?", Paper presented at the *Annual Meeting of the American Political Science Association*, Chicago, 2-5 September.

Noveck, B. S. (2005) "A democracy of groups", *First Monday*, Vol. 10, number 11 November. URL: http://www.firstmonday.org/issues/issue10_11/noveck/.

Nozick, R. (1974) *Anarchy, State and Utopia*, Oxford: Basil Blackwell.

O'Neil Lane, E. (2005) *Decision-Making in the Human Subjects Review System*, Doctoral Dissertation, Georgia Institute of Technology.

Oppenheimer, M. (1971) "The Limitations of Socialism: Some Sociological Observations on Participatory Democracy", in Benello, C.G. & Roussopoulos, D. (eds) *The Case for Participatory Democracy*, New York: Grossman Publishers.

Orlikowski, W. J. (1992) "The duality of technology: Rethinking the Concept of Technology in Organizations", *Organization Science*, Vol. 3, No. 3, August, pp. 398-427.

Orlikowski, W. J. (2000) "Using technology and constituting structures: a practice lens for studying technology in organizations", *Organization Science*, 11(4), pp. 404-428.

Orlikowski, W.J. & Iacono, C.S. (2001) "Desperately Seeking the 'IT' in IT Research - A Call to Theorizing the IT Artefact", *Information Systems Research*, 12 (2), pp. 121-134.

Orlikowski W. J. & Robey, D. (1991) "Information technology and the structuring of organizations", *Information Systems Research*", 2(2), pp. 143-169.

Orwell, G. (1990) *1984*, London: Penguin.

Ostrom, E. (1999) *Governing the Commons: The Evolution of Institutions for Collective Action*, Cambridge: Cambridge University Press.

Pain, J. (2005) *Handbook for Bloggers and Cyber-Dissidents,* Reporters Without Borders, September. URL: http://www.rsf.org/IMG/pdf/handbook_bloggers_cyberdissidents-GB.pdf.

Parker, R. (1974) "A Definition of Privacy", *Rutgers Law Review*, Vol. 27, pp. 275-296.

Pargman, D. (2000) *Code begets community: On social and technical aspects of managing a virtual community*, Doctoral Dissertation, Department of Communication Studies, The Tema Institute, Linköping University, Sweden.

Pateman, C. (1970) *Participation and Democratic Theory,* Cambridge: Cambridge University Press.

Perritt, H. H. (1998) "The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance", 5 *Indiana Journal of Global Legal Studies,* 423.

Petäjä, U. (2006) *Varför Yttrandefrihet? Om rättfärdigandet av yttrandefrihet med utgångspunkt från fem centrala argument i den demokratiska traditionen*, Doctoral Dissertation, Växjö University.

Pickerill, J. (2003) *Cyberprotest – Environmental Activism Online*, Manchester: Manchester University Press.

Popper K. R. (1959) *The Logic of Scientific Discovery*, London: Hutchinson.

Posner, E. A. (1996) "The Regulation of Groups: the Influence of Legal and Nonlegal Sanctions on Collective Action", *The University of Chicago Law Review* 63, no. 1 (Winter), pp. 133-97.

Posner, R. A. (1984) "An Economic Theory of Privacy", in Schoeman (ed) *Philosophical Dimensions of Privacy: An Anthology,* Cambridge: Cambridge University Press.

Post, D. G. (1998) "The 'Unsettled Paradox': The Internet, the State and the Consent of the Governed", 5 *Indiana Journal of Global Legal Studies* 521.

Prior, L. (2004) "Analysing Documentary Realities", in Silverman, D. (ed) *Qualitative Research: Theory, Method and Practice*, London: Sage Publications.

Proposition (1999) *Ett informationssamhälle för alla,* Prop. 1999/2000:86.

Proposition (2000) *Förberedelse till brott m.m.,* Prop. 2000/01:85 page 50.

Proudhon, P-J (1994 [1840]) *What is property?,* Cambridge: Cambridge University Press.

Power, J. (2002) *Like Water on Stone: The Story of Amnesty International,* London: Penguin Books Ltd.

Quint, P. E. (2000) "The Border Guard Trials and the East German Past: Seven Arguments", 48(4) *American Journal of Comparative Law.*

Rachaels, J. (1975) "Why Privacy is Important?", *Philosophy and Public Affairs*, Vol. 4, pp. 323-333.

Ranerup, A. (1999) "Contradictions when Internet is Used in Local Government", in Heeks, R. (ed) *Reinventing Government in the Information Age*, London: Routledge.

Ranerup, A. (2000) "On-Line discussion Forums in a Local Government Context" in Gurstein, M. (ed) *Community Informatics: Enabling Communities with Information and Communications Technologies*, Hershey: Idea Publishing Group.

Ranerup, A. (2001) "On-line Forums as a Tool for People-Centred Governance. Experiences from Local Government in Sweden", in Keeble, L. & Loader B. (eds) *Community Informatics. Shaping Computer-Mediated Social Relations*, London Routledge.

Rawls, J. (1963) "Legal obligations and the duty of fair play", in Hook, S. (ed), *Law and Philosophy,* New York: NYU Press.

Rawls, J. (1999) *A Theory of Justice*, Oxford: Oxford University Press

Raymond, E. S. (1999) *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*, Sebastopol, Calif.: O'Reilly & Associates.

Raz, J. (1999) "Obligation to obey: revision and tradition", in Edmundson, W (ed), *The Duty to Obey the Law*, Boulder, CO: Rowman & Littlefield.

Reena, J. (2001) "Want to See Some Really Sick Art?" *Wired News*, June 27. URL: http://www.wired.com/news/culture/0,1284,44728,00.html

Reidenberg, J. (1996) "Governing Networks and Rule-Making in Cyberspace", *Emory Law Journal*, Vol. 45, pp. 911-929.

Reidenberg, J. (1998) "Lex Informatica: The Formation of Information Policy Rules Through Technology", 76 *Texas Law Review.*

Reidenberg, J. (2001) "The Yahoo Case and the International Democratization of the Internet", *Fordham Law & Economics* Research Paper No. 11, Fordham University School of Law April.

Regan, P. (1995) *Legislating Privacy: Technology, Social Values, and Public Policy*, Chapel Hill: The University of North Carolina Press.

Rheingold, H. (1993) *The Virtual Community: Homesteading on the Electronic Frontier*, New York: Perseus Publishing.

Rhodes, R. A. W. (1997) *Understanding Governance: Policy Networks, Governance, Reflexivity and Accountability*, Buckingham Philadelphia: Open University Press.

Rejås, M. (2006) "Expensive Free Software?", in Klang, M., Petersson, L. & Öberg, J. (eds) *Beyond Free Software*, Leicester: Troubador Publishing (forthcoming).

Rolland, K-H. (2002) *Re-Inventing Information Infrastructures in Situated Practices of Use*, Doctoral Dissertation, Department of Informatics, University of Oslo.

Rosen, L. (2004) *Open source licensing: Software freedom and intellectual property law,* Upper Saddle River, N.J.: Prentice Hall.

Rosenbaum, N. (1978) "Citizen participation and democratic theory", in Langton, S. (ed) *Citizen participation in America*, Lexington: Lexington Books.

Ross, S. D. (1984) *Art and Its Significance: An Anthology of Aesthetic Theory*, Albany: State University of New York Press.

Rousseau, J. J. (1997 [1762]) "The Social Contract, or Principles of Political Right", in Gourevitch, V. (ed) *The Social Contract and Other Later Political Writings*, Cambridge: Cambridge University Press.

Rowland, D. & McDonald, E. (2000) *Information Technology Law*, 2nd edition, London: Cavendish Publishing.

RSF (2005) "Information supplied by Yahoo! helped journalist Shi Tao get 10 years in prison", *Reporters Without Borders*, 6 September.

RSF (2006) "Another cyberdissident imprisoned because of data provided by Yahoo", *Reporters Without Borders*, 9 February.

Ruffin, O. (2000) *Hacktivismo, Response to electrohippies*, Cult of the Dead Cow (17 July). URL: http://www.cultdeadcow.com/details.php3?listing_id=410.

Saltzer, J. H., Reed, D. P. & Clark, D. D. (1984) "End-to-end arguments in system design", *ACM Transactions on Computer Systems* 2, 4 (November), pp. 277-288.

Sandoval, G. (2000) "Sony to ban sale of online characters from its popular gaming Sites", *Cnet news.* April 10.

Sandoval, G. (2001) "eBay, Yahoo crack down on fantasy sales", *Cnet news*, 26 January.

Sartori, G. (1987) *The Theory of Democracy Revisited*, New Jersey: Chatham House Publishers.

Saul, J. M. (2003) *Feminism – Issues and Arguments*, Oxford: Oxford University Press.

Scanlon, T. (1977) "A Theory of Freedom of Expression" in Dworkin, R. (ed) *The Philosophy of Law*, Oxford: Oxford University Press.

Schauer, F. (1982) *Free Speech: A Philosophical Enquiry*, Cambridge: Cambridge University Press.

Schuler, D. (2000) "What it the Public Sphere?", *Computer Professionals for Social Responsibility* Newsletter, Vol. 18, Number 3, Summer.

Sherman, B. & Bently, L. (1999) *The Making of Modern Intellectual Property Law,* Cambridge: Cambridge University Press.

Shiva, V. (2002) *Water wars: Privatization, pollution and profit*, Cambridge Mass.: South End Press.

Silverman D. (1993) *Interpreting qualitative data: methods for analysing talk, text and interaction*, London: Sage.

Silverman D. (2005) *Doing Qualitative Research*, 2nd edition, London: Sage Publications.

Singer, P. (1973) *Democracy and Disobedience*, Oxford: Oxford University Press.

Singer, P. (1993) *Practical Ethics*, 2nd edition, Cambridge: Cambridge University Press.

Smith, D. J. (2000) "Changing Situations, Changing People", in von Hirsch, A., Garland, D. & Wakefield A. (eds) *Ethical and Social Perspectives on Situational Crime Prevention*, Oxford: Hart Publishing.

Sophocles (1912 [ca 442 BCE]) *Antigone*, Storr, F. (trans) Cambridge, MA: Harvard University Press.

Spafford, E. H. (1994) Computer Viruses as Artificial Life, *Journal of Artificial Life* 1(3), pp. 249-265.

Srijith, K. N. (2002) "Analysis of Defacement of Indian Web Sites", *First Monday*, Vol. 7, number 12 (December). URL: http://firstmonday.org/issues/issue7_12/srijith/index.html.

Stallman, R. (2002) *Free software, free society: Selected essays of Richard M. Stallman*, Boston: Free Software Foundation.

Statskontoret (2004) *Upphandlingspolicy för programvara avseende öppna standarder och öppen programvara,* GD Beslut 2004-03-18.

Strahilevitz, L. J. (2000) "How Changes in Property Regimes Influence Social Norms: Commodifying California's Carpool Lanes", 75 *Indiana Law Journal,* pp. 1231-1296.

Strahilevitz, L. J. (2002) "Charismatic Code, Social Norms and the Emergence of Cooperation on the File-Swapping Networks", *John M. Olin Law & Economics Working Paper* No. 162 (2D Series).

Sterling, B. (1994) *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*, London: Penguin.

Stenmark, D. (2002) *Designing the New Intranet*, Doctoral Dissertation, Department of Informatics, University of Göteborg, Sweden.

Strömholm, S. (1967) *Right of Privacy and Rights of the Personality*, Stockholm: Norstedts.

Suber, P. (1999) "Civil Disobedience", in Gray, C. B. (ed), *Philosophy of Law: An Encyclopedia*, New York: Garland Publishing Company.

Sundström, M. (2001) *Connecting Social Science and Information Technology – Democratic Privacy in the Information Age*, Doctoral Dissertation, Dept. of Political Science, University of Lund.

Sveningsson, M. (2001) *Creating a sense of community: experiences from a Swedish Web chat*, Doctoral Dissertation, Department of Communication Studies, The Tema Institute, Linköping University, Sweden.

Svensson, L. (2002) *Communities of Distance Learning Education*, Doctoral Dissertation, Department of Informatics, University of Göteborg, Sweden.

Taylor, J. S. (1999b) "The Theory of Autonomy", *Humane Studies Review* Vol. 12, No. 3.

Taylor, N. (2002a)"State Surveillance and the Right to Privacy", *Surveillance & Society* 1(1), pp 66-85. URL: http://www.surveillance-and-society.org

Taylor, P. (1999) *Hackers: Crime in the Digital Sublime*, London: Routledge.

Taylor, T. L. (2002b) "Whose Game is this Anyway? Negotiating Corporate Ownership in a Virtual World", in Mäyrä, F. (ed) *Computer Games and Digital Cultures* Conference Proceedings, Tampere University Press, Tampere, pp. 227–242.

Tedeschi, B. (2003) "Pop-up ads provoke a turf battle over Web Rights", *International Herald Tribune*, Tuesday 8 July, p 15.

Teece, D. (1986) “Profiting from Technological Innovation: Implications for integration, collaboration, licensing and public policy”, *Research Policy*, 15, pp. 285-305.

Tenner, E. (1997) *Why Things Bite Back: Technology and the Revenge of Unintended Consequences*, New York: Vintage Press.

Teubner, G. (1993) *Law as an Autopoietic System*, Oxford: Blackwells.

Thompson, J. J. (1975) “The Right to Privacy”, 4 *Philosophy & Public Affairs* 295.

Thompson, K. (1998) *Moral panics*, London: Routledge.

Thompson, R. (2005) “Why Spyware Poses Multiple Threats to Security”, *Communications of the ACM*, Vol. 48, No. 8, pp. 41-43.

Thoreau, H. D. (1993 [1849]) *Civil Disobedience*, New York: Dover Publications.

Tribe, L. H. (1991) “The Constitution in Cyberspace”, *The Humanist*, September-October.

USA PATRIOT Act of 2001, Pub. L. No. 107-56, §§ 105, 201-202, 204, 212, 814, 115 Stat. 272 (2001).

Utterback, J. (1996) *Mastering the Dynamics of Innovation*, Boston MA: Harvard Business School Press.

Van Valey, T. L. & Petersen, P. C. (1987) “Public service centers: the Michigan experience”, in DeSario, J. & Langton, S. (eds) *Citizen Participation in Public Decision Making*, Westport: Greenwood Press.

Varlejs, J. (1998) “Who Censors the Internet and Why?”, in *Proceedings of Freedom of Expression, Censorship and Libraries*, Riga, Latvia, October 14-17.

Vegh, S. (2002) “Hacktivists or Cyberterrorists? The Changing Media Discourse on Hacking”, *First Monday*, Vol. 7, number 10 (October). URL: http://firstmonday.org/issues/issue7_10/vegh/index.html

Vick, D. (2005) “Regulating Hatred”, in Klang & Murray (eds) *Human Rights in the Digital Age* London: Glasshouse Press.

Villeneuve, N. (2005) “Technical Ways to Get Around Censorship”, in Pain, J. (ed) *Handbook for Bloggers and Cyber-Dissidents,* Reporters Without Borders. URL: http://www.rsf.org/IMG/pdf/handbook_bloggers_cyberdissidents-GB.pdf.

Vinthagen, S. (2005) *Ickevåldsaktion, En social praktik av motstånd och konstruktion*, Doctoral Dissertation, Peace and Development Research, Göteborgs University.

Volokh, E. (2003) "The Mechanisms of the slippery slope", *Harvard Law Review* v 116.

von Hippel, E. (2005) *Democratizing Innovation*, Boston MA.: MIT Press.

Walch, J. (1999) *In the Net: An Internet Guide for Activists*, London: Zed Books.

Waldman, L. (1969) "Civil Rights, Yes: Civil Disobedience, No", in Bedau, H. (ed) *Civil Disobedience*, New York: Pegasus.

Waldron, J. (1999) "Property Law", in Patterson, D. (ed) *A Companion to Philosophy of Law and Legal Theory*, Blackwell Companions to Philosophy, Lonodn: Blackwell.

Waltzer, M. (1999) "Deliberation, and What Else?", in Macedo, S. (ed) *Deliberative Politics. Essays in Democracy and Disagreement*, Oxford: Oxford University Press.

Warren, S. & Brandeis, L. D. (1890) "The Right to Privacy", *Harvard Law Review*, Vol. 4, pp. 193-220.

Wasik, M. (2000) "Hacking, Viruses and Fraud", in Akdeniz, Y., Walker, C. & Wall, D. (eds) *The Internet, Law and Society*, London: Longman.

Watson, R. T. & Mundy, B. (2001) "A Strategic Perspective of Electronic Democracy", *Communications of the ACM*, Vol. 44 No. 1, January, pp. 27-30.

Westin, A. (1967) *Privacy and Freedom*, London: Bodley Head.

White, L. (1962) *Medieval Technology & Social Change*, Oxford: Oxford University Press.

White, L. (1972) "Technology and Social Change", in Nisbet, R. (ed.) *Social Change*, Oxford: Basil Blackwell.

Williams, R. (1980a) "Means of Communication as Means of Production", *Problems in Materialism and Culture: Selected Essays*, London: Verso.

Williams, R. (1980b) "Base and Superstructure in Marxist Cultural Theory", *Problems in Materialism and Culture: Selected Essays*, London: Verso.

Williams, S. (2002) *Free as in Freedom: Richard Stallman's Crusade for Free Software*, Sebastopol, Calif.: O'Reilly & Associates.

Winner, L. (1978) *Autonomous Technology: Technics-out-of-Control as a Theme in Political Thought*, Cambridge, MA: MIT Press.

Winner, L. (1985) "Do Artefacts have Politics?", in Mackenzie, D. & Wajcman, J., (eds), *The Social Shaping of Technology*, Buckingham: Open University Press.

Winner, L. (1986) *The Whale and the Reactor: A Search for Limits in an Age of High Technology*, Chicago: University of Chicago Press.

Winner, L. (1997) Cyberlibertarian Myths and the Prospects for Community, Draft Online at URL: http://www.rpi.edu/~winner/cyberlib2.html.

Winner, L. (2005) "Technological Euphoria and Contemporary Citizenship", *Techné* 9:1 Fall, pp. 124-133.

Wong, R. (2005) "Privacy: Charting its Developments & Prospects", in Klang and Murray (eds) Human Rights in the Digital Age, London: Cavendish Publishing.

Yates, J. (1989) *Control Through Communication: The Rise of System in American Management,* Baltimore: Johns Hopkins University Press.

Zittrain, J. & Edelman, B. (2002), *Documentation of Internet filtering in Saudi Arabia*. URL: http://cyber.law.harvard.edu/filtering/saudiarabia/

Zittrain, J. & Edelman, B. (2003) "Internet Filtering in China", *IEEE Internet Computing*, Vol. 7, Issue 2, March/April.

Zhang, X. (2005) "What do Consumers Really Know About Spyware?", *Communications of the ACM*, Vol. 48, No. 8, pp. 44-48.

Zone Alarm (2000) *Essential Security for DSL and Cable Modem Users Now Available with New Internet Security Utility - ZoneAlarm 2.0*, Press Release, 26 January.

Zuckerman, E. (2005) "How to Blog Anonymously", in Pain, J. (ed) *Handbook for Bloggers and Cyber-Dissidents,* Reporters Without Borders. URL: http://www.rsf.org/IMG/pdf/handbook_bloggers_cyberdissidents-GB.pdf.

There is no pain, you are receding.
A distant ships smoke on the horizon.
You are only coming through in waves.
Your lips move but I cant hear what youre sayin.
When I was a child I had a fever.
My hands felt just like two balloons.
Now I got that feeling once again.
I cant explain, you would not understand.
This is not how I am.
I have become comfortably numb.

David Gilmour & Roger Waters