Law in a Noise Society

Doctoral Dissertation

Nicklas Lundblad

IT-UNIVERSITY OF GÖTEBORG
Departement of Applied Information Technology
412 96 Göteborg, Sweden
1. INTRODUCTION............................................................................................................. 5
   RESEARCH QUESTION ................................................................................................. 6
   RESEARCH CONTRIBUTIONS......................................................................................... 6
   RELATED RESEARCH................................................................................................... 8
   DELIMITATIONS........................................................................................................... 9

2. THEORY AND METHODOLOGY..................................................................................... 11
   INTRODUCTION ........................................................................................................... 11
   THEORY I: INFORMATICS AS A SOCIAL SCIENCE ...................................................... 12
   THEORY II: TECHNOLOGY AND SOCIAL CHANGE .................................................... 15
   THEORY III: ARCHITECTURE REGULATION ................................................................ 19
   RESEARCH STRATEGY AND METHODS .................................................................. 22
   METHOD I: POLICY DISCOURSE ANALYSIS ................................................................ 23
   METHOD II: DE-SCRIPTING ......................................................................................... 26
   METHOD III: CRITICAL ANALYSIS ........................................................................... 29
   SUPPORTING PARTICIPATORY ELEMENTS ................................................................ 29
   DATA SETS – CHOICES AND MATERIALS .................................................................. 30

3. CONSTRUCTING AN INFORMATION SOCIETY MODEL .............................................. 34
   INTRODUCTION ........................................................................................................... 34
   FROM BELLS TO I2010 – A GENEALOGY .................................................................. 35
   CONSTRUCTING THE INFORMATION SOCIETY MODEL ........................................... 46

4. TRACING THE INFORMATION SOCIETY MODEL ...................................................... 48
   TRACES AND VALIDATION ......................................................................................... 48
   THE DATA PROTECTION DIRECTIVE ......................................................................... 48
   PRIVACY ENHANCING TECHNOLOGIES .................................................................. 57
   THE INFORMATION SOCIETY DIRECTIVE ................................................................ 66
   ELECTRONIC COPYRIGHT MANAGEMENT SYSTEMS .............................................. 73
   CONCLUSIONS ............................................................................................................ 78

5. COPYRIGHT – CRISIS AND FAILURES .................................................................... 80
   COPYRIGHT BASICS .................................................................................................... 80
   WEAKNESSES AND FAILURES .................................................................................... 83
   COPYRIGHT IN CRISIS ................................................................................................ 84
   COPYRIGHT POLICY FAILURES ................................................................................... 89
   CREATIVITY - THE INCENTIVE ARGUMENT REVISITED ........................................... 92
   FILE-SHARING AND ENFORCEMENT ........................................................................ 100

PRIVACY – CRISIS AND FAILURES ............................................................................... 112
I. Introduction

We live in interesting times. Policy makers have failed to meet the challenge posed by emerging information and communication technologies and addressing this failure requires radically rethinking the societal models that guide policy development. Continued failure will harm future growth, development and in the end the realization of the promise inherent in technical innovation. Copyright, privacy and freedom of speech are some of the areas where an old model, based on the mirage of control, has led to what mostly resembles trench warfare between increasingly polarized actors.

The model policy makers are using, its failures and possible alternatives, will be the focus of my work here. A model or a set of heuristic principles for estimating how technical change will affect society has always been necessary as help for policy makers to align and design policy responses in a way that would match the new challenges brought on by new technologies.

The policy maker’s model is important to understand and develop critically. To make sure that this model is made explicit and to criticize it is a prioritized task for any social science in which technology figures as a change element, since the model affects the future course of society.

If the policy maker’s model is false or defective or simply out of tune with society this will lead to adverse effects for society. It could lead to a situation where policy responses become increasingly less well adapted to social change, and a disconnect between citizens and policy makers could be the result – leading to loss of social cohesion, increased alienation and perhaps even a reduced respect for legislation and the democratic process.

I firmly believe that ICT-policy matters, and that what policy makers do is worthy of attention. The models they use and their failures show us something about not only technology, but about societal growth and development. A society’s way of adapting to technical change mirrors its general understanding of the world, and as such is a powerful diagnostic for any social science project.
Research question

The research in this study flows from the question of why policy makers fail to do better in adapting to the emerging information and communication technologies. This question, however, is ill-defined and hard to answer in itself. What does it mean to do better? How are we failing? What do policy makers really do when they design policy responses? All these sub-questions need to be developed and answered before it is possible to analyze the failure of ICT-policy in a structured way. The best way to do so seems to be to describe the research task I have set myself and to develop a research question against the background of this description.

Firstly, I have assumed that policy makers use models in making decisions about what policy responses to deploy. If these policy responses are failures, I assert, it is at least partly the models that have failed. The starting point of my investigation thus has to be an examination of what the model guiding policy makers up until now looks like. What model is guiding policy making today?

Secondly, I need to show that this model is indeed failing because of its inherent qualities. That means that I have to show how the model leads to concrete policy responses and how these policy responses have failed.

Thirdly, in order to answer what it would mean to do better, I need to develop an alternative societal model and show why I think that it could outperform the old societal model, and motivate why.

I have chosen to work with a set of research questions. They are:

1) What societal model guides policy makers in formulating policy responses to emerging information and communication technologies?
2) How and why does that model fail in addressing the challenges policy makers face?
3) Are there alternative models that could improve our policy making process?

The answers to these three questions suggest at least one possible answer to the question of why policy makers are not doing better in responding to the new technologies changing society at large.

Research contributions

The main contributions of the work here is the following:

1) An analysis of ICT-policy making focusing on societal models and their impact on policy responses.
2) An examination of selected legislation and architectures for uncovering underlying societal models.
3) An analysis of some breaking points where the societal models used in ICT-policy break down and where these models reach the limit of their usefulness.

4) A possible alternative model for policy making that is more aligned with the boundary cases as well as a suggestion of possible emerging discourses for policy makers.

The work presented here builds on several peer-reviewed papers to conferences and journals as well as contributions to the policy literature ranging over a period of almost ten years. Among the most important contributions that can be traced in the different chapters are:

**Books and book chapters**


**Peer-reviewed papers to conferences**


**Peer-reviewed papers published in journals:**


**Research reports:**

**Related research**

The study of the information and communication technology policy process is not new. There have been studies of the role of policy making with different emphasis (Bullock and Mountford 2001), and studies focusing on information technology as well. One of the earliest studies in this area is Laura Cram’s (1996) work examining how ICT-policy is made in the European Union. Cram’s study is a work in political science and it focuses on policy processes as these are regularly described in political science, and it is a good example of a study of policy making in the political sciences. The method chosen here will be slightly different and more cross-disciplinary. Other examples include Ian Hoseins *Regulating the Technological Actor: How Governments Tried to Transform the Technology and the Market for Cryptography and Cryptographic Services and the Implications for the Regulation of Information and Communication Technologies* (I. Hosein n.d.).

Another example is Sandra Braman’s (2006) work *Change of State: Information, Policy and Power*. Braman presents a cross-disciplinary analysis of the emergence of what she calls the informational state and she analyses power distributions as well as consequences of the rise of the informational state with a multitude of different tools. Her examination of identity, structure, borders and change delve deeply into the nature of the informational state and proves a useful theoretical companion (Braman 2006).

Braman’s studies exemplifies a multi-theoretical approach to the information society and the concept of information and builds her analysis on a framework of several different kinds of power: she analyses power as instrumental, structural, symbolic and informational (Braman 2006, 25) and uses the fourth form – her contribution – to explain how information exercises power. Informational power is simply the power to change the informational content of the other forms of power we see. Instrumental power – manipulation via physical force – is changed by surveillance; structural power – inherent in social contexts – is changed by the way information flows and symbolic power is changed by the manipulation of the information of which the symbols are a part.

Braman’s study of the rise of the informational state and how it is replacing the bureaucratic welfare state also offers a history of information policy responses, from pre-modern information policy to our contemporary environment. She claims that the information society has gone through several different stages and that policy has varied with the different stages. The first stage she identifies was the period between 1830-1900, with electrification and the beginnings of globalization as salient features of the period. In the second stage, between 1900-1960, mass communication becomes a reality and in the third stage, 1960-1990, we begin to realize that we see an informatization of society – described as an increasing reliance on the economic values of information. This is also the stage where policy
makers start to see themselves as actually formulating an information policy and the questions about the information society become important in their earliest forms in discussing the post-industrial society, to take one example. In the fourth stage, 1990-2000, Braman sees the harmonization of software and hardware as well as protocols and the actualization of the architectures as inherent in the idea of the information society. From the year 2001 and forward she claims that we live in the fifth stage, that of the informational state.

I concur in the analysis that the information society can be described as having gone through stages. I base my analysis of the assumption that we have two later distinct waves of policy responses to the information society: the first is one that starts around 1990 and ends at around 1999, these legal responses are the ones I think are based on the model of the information society. The legal reforms introduced after this are mainly reforms that either govern specific issues like telecommunications law or aim to strengthen consumer protection in different ways.

Currently, the model of the society we are supposedly responding to and shaping (the use of the word response is not to convey a passive response, but more of a response in dialogue with changes - policy making is not merely reactive) is less clear than it was then. The model of the information society used by policy makers in what Braman calls the fourth stage is a model heavily influenced by the activities pursued at the time: the development of software, hardware and protocols to construct large systems and the overall systems perspective dominates the policy making process.

**Delimitations**

In order to make a project like this manageable it is important to delimit the scope of the study.

Firstly, the study concentrates on two kinds of policy making. Where, for example, Braman studies basically all social phenomena, I have concentrated my studies on two different kinds of policy making: policy making through laws and policy making through architecture.

Secondly, most of the study is limited to two fields of policy making: privacy and copyright. The reasons for this and the criteria used are developed more in detail below, in the chapter dealing with theory and method.

Thirdly, this is not a study about how technology changes society as such, but a study of the models policy makers use to understand societal change brought about by technology. This delimitation is tricky, but necessary. I will not be asking questions – directly – about how society changes when disruptive technologies enter the stage. I will ask questions about what societal models policy makers use to understand that change and where they lead us.
Fourthly, the study is delimited in time, if somewhat vaguely. The technologies and legislation studied dates to roughly the years 1994-2001. In some cases (as in the choice of high-level policy texts) this span is expanded, but this only occurs because of the extra value in following the European policy development and its remarkable stability in confirming to one societal model.

Fifthly, law and legislation in this study is used mainly as examples of policy responses. I have not attempted to write a legal work, but limit the use of legal interpretation and analysis to cases where such analysis supports the overall goal of the study; to show how policy responses flow from the use of societal models. I use the word law in the broadest possible sense: as the sum of regulatory tools and instruments.

Sixthly, the legislative examples are predominantly European. The technologies analyzed are more international, but there is a European focus that must be acknowledged. I do not believe that there are large differences between the EU and the rest of the Western world here, but must leave that question open.
2. Theory and methodology

Introduction

The study of policy making and societal models or sets of heuristics is a field that needs to be theoretically situated within the tradition of informatics research. The object of this chapter is to establish both a theoretical frame and a methodological set of tools to attack the research questions.

I will build a theoretical foundation in three separate layers:

---

An overview of the theoretical framework
The first layer will be an examination of informatics as a social science, specifying how informatics relates to the social sciences and especially to the study of policy making and law. The second layer is an examination of social change and technology. The layer aims at situating this study in a framework for studying social change and technological change as analytically separate categories. The third is a more specific discussion of the theoretical framework for analyzing regulatory change, technology and what Lessig (1999) calls architecture regulation. The purpose of introducing this theory is to enable a discussion of technology as a policy response.

Together these three layers of theory establish a framework vital for the research strategy applied in this work. The theoretical foundations and the research strategy are necessary to answer the research questions in a way that adds to the body of research on ICT-policy both methodologically and substantially.

**Theory I: Informatics as a social science**

I understand informatics as a social science. This is not a trivial statement, even if it may seem so on the surface. I follow closely the description of what has been called *new informatics* outlined in professor Bo Dahlbom’s article “The New Informatics”. In this article Dahlbom outlines the curriculum of the new informatics thus (Dahlbom 1999):

Informatics differs from computer science generally by defining its subject matter, information technology, as a social phenomenon. Another way to organize our curriculum could begin by distinguishing important aspects of technology as a social phenomenon. One suggestion, then, and I owe this to a discussion with Lars Mathiassen, would define a general introduction to information technology as comprised of four subjects: development, use, management, and technology. Such an introduction might be offered as something of a core curriculum for information society, but it can also constitute a general framework for distinguishing different specialities within the general informatics area.

What is lacking in this definition, however, is a discussion of scale. How large are the social phenomena studied in informatics? Stating that technology is a social phenomenon does not resolve that question, but leaves it open to further discussion. Studies in informatics have – historically – taken as objects of studies (to take but a few examples): competence systems (Lindgren 2002), intranets (Stenmark 2002), IT use in healthcare (Lundberg 2000), everyday computational things (Redström 2001) and mobility (Weilenmann 2003). Methodologies range from ethnographical to psychological and sociological over action research and technical development.

---

1 That they are analytically separate does not indicate an ontological commitment on the issue of how they interrelate generally, but only serves as a useful simplification in order to find categories for classification of both processes.
2 Or complex?
But what of even larger-scale social phenomena? What of the interplay between technology and society at a macro-level? Is it at all possible to speak of informatics at the level of societal change? The arguments *against* might be that on such a general level very little can be said and that the processes of societal change are so complex as to almost be inaccessible to research. The arguments *in favor* could be that the discussion about technology and social change is both inevitable and important to society, and furthermore that it is fictitious to argue that some social phenomena are so much more complex than others as to be inaccessible to research. The social sciences have perhaps always concerned themselves with macro-level changes in society in different ways, as well as studies of smaller-scale social phenomena. Modern day social science examines phenomena that range from the specific practice of a community to the overall process of social change.

There is no lack of historical precedent in social science when it comes to looking at societal change and technology. Studies on technological societies and their development abound, from Mumford (1962) over Winner (1977) and Ellul (1964) to recent writers like Jensen (2001) or Benkler (2006). These large-scale studies may even complement smaller-scale studies, inform and be informed by them in an interplay that could very well prove useful for the overall development of the subject.

In interpreting informatics as a social science I thus perceive it to be open to both kinds of studies: both the small-scale studies of specific delineated social phenomena and the macro-level studies of societal change. I interpret “use” and “management” in Dahlbom’s definition not only as individual uses and individual management, but as the collective, societal use and management of technology in society. This necessitates a view of informatics as a layered social science ranging from small scale studies to society-wide studies of the activities suggested by Dahlbom. Social development, management, use and technology as well as organizational, group or individual layers are accommodated by this interpretation.

---

3 Indeed, it is interesting to ask what it means for a phenomenon to be inaccessible to research: does such a classification imply that there is nothing that can be said about it that will contribute to our share understanding? Or that it is merely harder to say something salient about it?

4 The distinction between individuals, groups, organizations and societies is usually not conceived of as sharp and well-defined. Different criteria can be used and some methods range over groups and organizations. The example is merely intended to show the methodological variety and wealth available to the researcher in different layers.
Interpreting informatics as a social science also has consequences for deciding on demarcation criteria for determining scientific relevance and quality. What does it mean to be a social science? What are the results of social sciences? One way to answer this question would be to follow the suggestion of William Wimsatt (2007) in thinking of social science as “piecemeal approximation” where “the complexity of the systems we are studying exceeds our powers of analysis” (Wimsatt 2007, 75) and expect the results to be sets of heuristics or “rules of thumb”. The demarcation criteria for sets of heuristics are slightly different than those for other kinds of scientific results. Again we can build on Wimsatt (p 76): heuristics produce errors that are not random, but systematically biased. This means that any set of rules will not do. The set chosen needs to produce errors in a non-random way and do so consistently. Furthermore heuristics offers no guarantee that they will produce the right answer to a problem, and they should also be very cost effective in comparison with other methods. Finally, heuristics transform a problem to a “nonequivalent but intuitively related problem” (p 76).

I am partial to an interpretation of informatics understood as a social science open to the study of large-scale social change with the aim of producing heuristics or models for understanding this change and managing it in a public policy process. This does not explicitly imply a complex ontology and no specific ontological claims are made. The object of study and the demarcation criteria here are focused at the economy of the heuristics or models applied and their boundaries in the
sense that Wimsatt and others use this term (and not at the accuracy or correspondence with a posited reality\(^5\)).

**Theory II: Technology and social change**

In order to produce heuristics it is not enough to agree that informatics is a social science. There is also a need for a description of social or societal change that can be used as a framework within the larger framework of social sciences to understand and discuss how society changes in general and how technology changes/is changed by society in particular. How does society change? How does technology change with/in/against society? One answer to this question is to state that society is changed through the decisions of the legislator and that society is crafted, in essence, by those in power. Another answer is the one provided by thinkers like Friedrich von Hayek, Austrian lawyer and economist, who argued that society is the consequence of a number of spontaneous ordering processes. Hayek will be used here because his work is generally perceived as important to the growth of public policy analysis and his work on law, social orders and social progress is often used in policy analysis (Parsons 1995, 50-51).

In *Law, Legislation and Liberty* (1973) Hayek lays down some basic principles of societal development that he thinks are at work in forming our society. He suggests that there are at least two different forms of order – directed and spontaneous, or grown or made:

The made order which we have already referred to as an exogenous order or an arrangement may again be described as a construction, an artificial order, as an *organization*. The grown order, on the other hand, which we have referred to as self-generating or endogenous order, is in English most conveniently described as a *spontaneous order*. Classical Greek was fortunate in possessing distinct single words for the two kinds of order, namely *taxis* for a made order such as, for example, an order of battle, and *kosmos* for a grown order, meaning originally ‘a right order in a state or a community’. (Footnotes omitted, italics in original).

In studying technological societies it is possible to use Hayek’s distinction between the different kinds of order and ask what ordering principle – *taxis* or *kosmos* – which most closely describes how the use of technology affects society. I will submit that technology rarely, if ever, is a part of exogenous control or *taxis*. This may seem surprising since quite a few of the fictional technological dystopias (such as Orwells 1984 or the society in the movie The Matrix(1999)) have been described as societies where technology functions as a means of exogenous control: man is, in these dystopias, controlled by technology or through technology.\(^6\)

---

\(^5\) This scientifically minimalistic approach is adopted as a natural consequence of the complexity of large social phenomena and their interaction with each-other.

\(^6\) This control can be mediated or direct, as control through surveillance or control through direct bio-technical fusion.
However, none of these dystopias have come to pass as of yet. One possible explanation for this is that technology use – at least in democracies – is distributed over a multitude of actors. Many citizens use some kind of technology. In doing so we could argue that they shape society and give rise to a spontaneous order that closely resembles kosmos as described by Hayek.

An example helps: the vision of the information society, in many ways, is a vision of a society where technology and the ordering power of technology are exogenous to society. It is a vision of taxis, of society as an organization or a made order. **The harshest conflicts are conflicts where the kosmos of technology meets with the taxis of legislation.** The clash between intellectual property rights – a set of legal rules explicitly put in place to achieve a declared societal goal – and file-sharing technologies is a case in point. This clash is a clash not only between what has been perceived to be change-averse record companies and their consumers, but between two kinds of order: a strong technological kosmos where copying is a practice well-spread and a weak legislative taxis aiming to preserve a declared societal goal that no longer carries the same legitimacy that it once did.

The large-scale macro-process of technological change is not, I submit, external or exogenous to society, but is more aptly viewed as a part of societal change. But how technology develops, and what level of control citizens exert over the use and development of technology, may affect the overall resulting society. In Langdon Winner’s classic *Autonomous Technology: Technics-out-of-Control as a Theme in Political Thought* (1977) technological change in political thought is examined to discern what major themes can be found in what essentially is the policy discourse. Winner describes the discourse as having moved from themes of mastery to themes concentrating on the loss of control or the new autonomous technology (p 15):

> In the present discussion the term autonomous technology is understood to be a general label for all conceptions and observations to the effect that technology is somehow out of control by human agency. My use of this notion stems directly from Jaques Ellul’s autonomous technique. According to Ellul, “Technique has become autonomous; it has fashioned an omnivorous world which obeys its own laws and which has renounced all tradition.”

Winner goes on to say that the term describes a state of society where “far from being controlled by the desired and rational ends of human beings, technology in a real sense now governs its own course, speed and destination.” (p 16) It is important to note that Ellul uses the word technology here, not least because it projects the image of a singular force, a single actor, on the policy stage.

In Winner’s extensive analysis of different theories about societal change many different writers (like Daniel Bell’s work (1973)) is deemed “determinist”. Winner defines technological determinism as a society where changes in technology with necessity imply changes in society as well. Following Winner I will distinguish between societal change, the dimension of taxis and kosmos and a dimension of
autonomy. Assuming no causal absolute relationship between the level of control over technology and society’s development overall enables a discussion about the impact of policy measures on the development of society and offers a useful way of categorizing societies.  

The technological determinist would perhaps argue that policy is the result of technological change, and that the politics produced by technology as well as the policy making processes in the technological society are effects rather than the causes of technological change. Accepting, on the other hand (and on faith), that policy does have some impact on the resulting society necessitates examining the dimensions of societal change and technological mastery separately. Winner here makes another point in identifying what he calls the process of reverse adaptation (p 229):

[...]the adjustment of human ends to match the character of the available means. We have already seen arguments to the effect that persons adapt themselves to the order, discipline, and pace of the organizations in which they work. But even more significant is the state of affairs in which people come to accept the norms and standards of technical processes as central to their lives as a whole.

Winner’s “reverse adaptation” could be seen as a striking description of much of the policy making in the ICT-policy discourse. The perceived need to prepare Europeans “for the advent of the information society” as the Bangemann report (1994) puts it, is a case in point. This view, that the information society is coming, and that it has policy consequences that need to be implemented whether citizens want to or not is deterministic as a matter of course, but it also reflects a view of technological change where technology is autonomous, but where actors can actually shape the society that will result – but not by shaping technology, but by molding themselves after the technological developments.

Winner’s vision of a technological society then becomes one where ultimately the reader is instructed to “expect a dispersion of power into the functionality of large-scale systems of the technological order.” (p 261, italics in original). And this is perhaps where Winner’s argument has its greatest weakness. The focus on large-scale systems leads Winner to a position against which it is possible to argue that the actual development of the information society has deviated from Winner’s predictions. It is possible to argue that in our society the large-scale systems have failed, they have broken down into smaller, patchwork or bricolage-like systems that work together, or at least try to interact with each-other. It may be true that the first architectural policy responses to the information society were indeed conceived of as large-scale systems – both in protecting privacy and copyright – but when these systems failed, the policy responses were tailored towards smaller bricolage-solutions.

---

7 It might be argued that this is a fictional distinction, and rightly so. That does not make it less methodologically useful.
Winner’s autonomy is the large-scale autonomy of systems large enough to only need “on occasion appeal to the central decision-making organs of the state for support or assistance” (p 261), not the autonomy of swarm technologies or small interacting ad-hoc mobile networks. This latter kind of small-scale autonomy could arguably be said to come much closer to the kind of technological autonomy evidenced in present-day society. Winner assumes a “center” (p 185) that would act as a controlling core in a technological society. But perhaps the course society has taken is rather one where society is characterized by multiple distributed centers and different small-scale systems that interact in producing information flows. I will keep Winner’s notion of autonomy in the theoretical framework, of a technics-out-of-control, but divorce it from Winner’s assumption of scale and argue that what we have in fact seen is a kind of technics-out-of-control, but on a much smaller scale than Winner would expect. How, then, has this come about? What is it that has happened?

One possible answer would be that as technology develops it becomes cheaper and cheaper, and more accessible to citizens of at least affluent western societies. Technology – a typical luxury good – is consumed by a few, and then the profits from this luxury consumption are re-invested in making technology cheaper and cheaper (von Mises 1984(1929), 32). The user circle widens and grows quickly to a point where even complex technologies can be owned by an individual. This “trickle-down”-effect is visible in technological markets: Computers, VCRs, digital cameras, mp3-players, DVDs and flat-screen TVs have all become cheaper and cheaper. These technologies are not technologies that can only be used to consume. They serve also as means of information production, and as such they become a powerful changing force in society. With the wide dispersal of these information technologies comes the growth of a new model of social production, described by writers like Yochai Benkler (2006, p 60):

 [...]the networked environment makes possible a new modality of organizing production: radically decentralized, collaborative, and nonproprietary; based on sharing resources and outputs among widely distributed, loosely connected individuals who cooperate with each other without relying on either market signals or managerial commands. This is what I call “commons-based peer production”.

The trickle-down effect makes commons-based peer production possible, and suddenly the technology – even if still autonomous in a macro-perspective (there is no single point societal mastery over the technologies of information production in our society, but there is individual mastery – I master my digital camera and my mp3-player, but no one masters all digital cameras and mp3-players) contributes not to a technological society in the sense that Winner or Ellul uses the term, but to something different, less organized. A spontaneous order based on widely dispersed means of information production, individually mastered, but autonomous on a macro-level.
Using the axes of control and autonomy and *kosmos* and *taxis* we can define another model of societal change. The different resulting societies are societies with spontaneous orders or organizations and where technology is either autonomous or controlled:

The different societies would typically require different models for policy making. A policy maker faced with a society where technology is under control and society at large is characterized by a top-down order has different challenges than the policy maker stuck with autonomous technology and spontaneous order.

It should be noted that here I have separated – artificially – the level of control over technology from the mode of social change. This does not reflect a belief that technological change is separate from societal change, but it does reflect the belief that it is useful to ask what mode of change policy makers envision both for technology and society. It is far from always the case that the two phenomena are viewed as entwined and co-dependent. In many cases the mode of change for technology is viewed as different from that of society at large (as will be evidenced by the analysis later).

**Theory III: Architecture regulation**

With a general framework for the informatics study of large-scale social change and a set of categories for possible societal configurations of social change and technological change, the next task becomes to situate technology in the theoretical framework. What is *technology* in informatics studies of the policy process? I submit that technology is a policy response, much as a law. Laws are, in
essence, decided. It is the nature of a law that it is definitely at some time adopted by a legislature. This does not mean that it will be followed, that it is efficient or that it has the intended effects, but law is decided. This is an essential part of how laws figure in policy making. When different actors negotiate laws they negotiate what will be decided, and when the decision is taken a new phase enters. The exact meaning of the laws may then be slightly re-negotiated in case law or in new interpretations, of course, but the legal policy making process is fairly simple to describe. Legal reforms are suggested, debated, analyzed, lobbied for and against and then voted upon and decided. This is at least the linear, simple and (admittedly) naïve view of legislation. And it actually suffices for my study, since what I need is a simple description of law-making that allows us to look at a few examples of legal reform.

It is more important for the purpose of this study to examine the theoretical foundations of why we can consider architectural change as a kind of policy response. Establishing that technology can act as a policy response also allows me to connect this study with the field of legal informatics in a more solid way, and so provides a way to situate this work in a rich tradition – but without the ambition to turn this into a work in legal informatics proper. (The study of social change and policy processes is still a field of its own in informatics, in my view.) Informatics overall have since long worked with the idea that artifacts are not neutral objects, but rather actors in society. “Artifacts have politics” (Winner 1986) and from this follows, through an argument we will examine, that “code is law” (Lessig 1999). There are other perspectives as well, where technology is isolated as a change agent or a factor in change, but these are of less interest to us here. Some writers in computer law sometimes limit the problem of technology and law to one of understanding how information and communication technologies change use (unidirectionally), but this narrow view is less useful for the analysis of policy making (Benno 2002, Westman 1998).

All technologies regulate their use and in them designers, users and others inscribe their expectations and negotiations with other actors. When the realization that artifacts are in a sense political is applied to the social phenomenon of law it opens up a fruitful field of enquiry.

The most influential work in the field examining this relationship between law and technology the last few years is unquestionably Lawrence Lessig’s Code and Other Laws of Cyberpace (1999, recently offered in a second edition Code 2.0 and based on numerous other publications (Lessig, What Things Regulate Speech ver 3.01 1998, Lessig, The Zones of Cyberspace 1996, Lessig, Constitution and Code 1996/97)). Lessig’s main argument is contrary to what early cyber-libertarians claimed: that cyberspace is naturally free or even its own jurisdiction (Barlow

---

8 Here I use law in a narrow sense, not the wide, all-encompassing sense in which the concept is used in the title of this work.
Cyberspace, Lessig warns, not only can be regulated but is regulated by its own inherent nature – by the code of which it is made up.

Cyberspace is in essence a regulated space, but regulation is less visible than it is in society at large, since it hides in architecture. The extreme example of this is in computer games/worlds like World of Warcraft where murder and theft in some instances have been programmed away, and Lessig’s argument is that if cyberspace is regulated by its architecture, then policymakers need to examine, discuss and perhaps even protect that architecture from becoming the tools of commercial actors or other would-be regulators.

If policymakers sustain the naïve cyber-libertarian idea that cyberspace is inherently impossible to regulate, that it is free by nature, they are doomed to wake up harshly when the growing economic importance of the new information and communication networks force massive redesign of the architecture. The new question participants in the policy process have to ask is how they want architecture to legislate and regulate, and if they should resist attempts at regulation that deprives the Internet of its innovative and liberating qualities (particularly, at least the early Lessig argues, policymakers need to preserve the end-to-end architecture of the Internet (Lessig and Lemley 2000), for more on end-to-end architectures see (Saltzer, Reed and Clark 1981)).

When Code... was published it was widely reviewed and it brought the question of how technology regulates to the attention of a new generation of Internet-users in a way that was accessible, exciting and thought-provoking. It also provoked criticism and counter-arguments that helped grow the theory of architecture even more.

The main problem with Lessig’s argument was that he seemed resigned to the idea that the growing commercial importance of cyberspace (his term) would lead to architecture re-design. In doing so, some claimed, he overestimated the ability of any one set of actors to control the negotiation of architectures and he underestimated the competition between different architectures.

One of the critics, David Post, an early cyber-libertarian, took Lessig to task for his mono-architecturalism and wrote (Post 2000, 19-20):

[...] if there are many different architectures, then there is choice about whether to obey these controls. If there are multiple architectures from which to choose, it is no longer correct to say that “nothing requires” booksellers to provide users the ability to browse for free. The market for bookstores, the existence of competing bookstores, and consumers’ desire to browse do so. It is hardly nothing; these are the very same things that “require[]” the real space booksellers that Lessig mentions to allow you to browse for free. And if there are diverse architectures of privacy, identity, of content protection, laid before the public, why is it so obvious that we will end up choosing the one(s) that deny us the things that Lessig (and I) think are so important?
Post’s criticism is, I believe, fundamentally correct. Lessig’s analysis of architecture regulation assumes too little competition in how architectures are negotiated. This is partly evident in Lessig’s choice of metaphors as well. He speaks of architecture as a constitution for cyberspace, and while not necessarily wrong about this, not all architectures are constitutional. Much like the legal system recognizes a hierarchy of different documents – from constitutions over laws to regulations and eventually recommendations – architecture regulation comes in a multitude of forms. Lessig here closely mirrors Winner’s and Ellul’s ideas about a single technological acting force – one architecture, not several.

The reader may agree with Lessig that end-to-end is essential to the nature of the Internet without granting him that digital rights management will be globally deployed because of the increasing commercial importance of the web.

Timothy Wu makes this point even more clearly in noting that there are certainly cases when code isn’t law (Wu 2003). Where the re-design of the architectures fail miserably and where “explosions of non-compliance” reduce the regulatory effects of code to nil. Architecture without compliance is nothing. A similar point is made by Tarleton Gillespie in his analysis of the problem of “aligning” different regulatory systems to ensure that code stays law, in his case that digital rights management technologies succeed (Gillespie 2007).

This is also, to be fair, implied by the fact that Lessig himself works with a model with four different regulators: law, norms, markets and architecture. The interplay and interactions between these different regulators shape the resulting society and Lessig never implies that architecture is the sole deciding legal factor to be reckoned with.

The conclusion that can be drawn from this is that the theory of architecture regulation in the policy process needs to be amended with a theory of compliance (Wu) or alignment (Gillespie) in order for it to be truly useful.

The theory of architecture regulation has been further analyzed, developed and expanded upon in the literature (Biegel 2001, Hosein, Tsiavos och Whitley 2002, Rotenberg 2001, Netanel 2000) and it forms an important part of the theoretical foundations of any study in legal informatics. Architecture regulation is a possible policy response and an essential part of the policy maker’s toolbox, and it is also difficult to implement in a way that ensures compliance.

Research strategy and methods
The research strategy used in this work is a three-tier-strategy employing three different methods and sets of data:
The research strategy.

The three steps I have envisioned as crucial to the study are:

1) Finding a model or set of heuristics used in ICT-policy making. This is essential to establish a starting point and to construct the model that is then subjected to critical analysis in step three. The method used here – policy discourse analysis – is well-suited to uncovering and mining the discourse for model elements to analyze closer.

2) Tracing the model. After having established that the model is present in high-level policy texts, it becomes necessary to trace it vertically into actual, concrete policy responses to validate that it actually has an influence on the everyday policy making process. It would otherwise be quite possible for a society to have a higher-level policy discourse divorced from actual legislation and policy making.

3) Finding alternatives to the model. This is where the boundaries and failures of the model are examined in closer detail. The objective in this step is to find the systemically biased errors inherent in the model used by policy makers.

The following section will present the methods in detail and motivate the choice of data as well as review earlier studies.

Method I: Policy discourse analysis

There are multiple different theories of the policy process and many new methods of study are constantly being developed (Sabitier 2007). Among the more
important are institutional analysis (Ostrom 2007), network analysis (Adam and Kriesi 2007), pluralist-elitist approaches (Parsons 1995) and the advocacy coalition framework (Sabatier and Weible 2007). Early theories about policy analysis and the policy process are sometimes called stagist, since they enumerated a number of stages or cycles in policy making thought to cover the entire complex nature of policy making (Parsons 1995, 39).

Institutional analysis focuses on the concept of institutions in society to study how the formation, design and interaction with institutions figure in the policy process. Ostrom (2007) notes that the concept of an institution has many different definitions, but uses it to refer to “the shared concepts used by humans in repetitive situations organized by rules, norms and strategies” (p 23). Institutional analysis is sometimes divided into sociological, economic and political institutional analysis depending on the methods used to study the institutions in question.

Network analysis starts from the assumption that the policy process can be described as a policy network of different actors. The concept of networks is varied – some use it to refer to a “distinct new governing structure” but it is also used “generically to different types of empirically possible patterns of interaction between public and private actors” (Adam and Kriesi 2007, 130, Parsons 1995, 184, Considine 2005, 123-140).

Pluralist-elitist approaches focus on the issue of power and its distribution in society (Parsons 1995, 39, 134-144). Here the outcome of the policy process is thought to depend on competition between different actors and ideas, rather than underlying structures or institutions. There is an underlying optimism in this approach that assumes that anyone can intervene in the policy process.

The advocacy-coalition framework is more of a method of analysis than a full-blown theory, and it is constantly being revised to cover different political systems and new forms of policy making. The latest revisions take into account, for example, “the corporatist regimes” in Europe and the “authoritarian executive regimes in many developing countries” (Sabatier and Weible 2007, 190).

The theory I have chosen to apply in a first attempt to examine the information society – policy discourse analysis – relies heavily on what is sometimes called “the argumentative turn” in policy analysis (Parsons 1995, 151-153) – a turn towards linguistic philosophy and discourse analysis. This theoretical development owes much to analytical philosophy and the linguistic turn in philosophers like Ludwig Wittgenstein as well as the analysis of discourse found in writers like Habermas and Foucault.

Policy discourse analysis is an established method of studying how public policy is made and how it develops over time. I will use the method to establish what the information society looks like and how it has developed over time. I will then distill, from the discourse analysis, a simple four-variable model to use in analyzing
a few select policy responses to the information society model. When speaking of discourses here I will use the term in the pluralist way indicated by Considine (2005). Considine speaks of “shared ‘road maps’” (p 72) and the examination of the information society I will undertake is a way of trying to show this shared road map for policy makers.

Considine (2005 p 74) exemplifies with a number of questions that can be useful in policy discourse analysis:

- What is the problem being named?
- What is omitted from the formulation?
- For whom is the problem a problem?
- Which interests benefit the prevailing definition of problems?
- Which actors are presumed to be part of this problem?
- How do the names and categories being used direct attention to solutions?
- How are exclusions being explained?

Policy discourse analysis can be thought of as a method of analysis that can be applied at two different levels. Firstly, it can be applied at the level of concepts, where we can examine different concepts and their language-games in order to see how they are used, and thus what the concepts may be taken to mean. Secondly, discourse analysis can be used to examine a cluster of concepts and how they move in the public debate in order to map an entire discourse and its genealogy. This latter approach is what will be employed in uncovering the model of the information society in modern European ICT-policymaking.

Discourse analysis is a quickly developing field and there are many different methods used as well as many different possible data sets. Norman Fairclough (2003) suggests an overall method for textual analysis of discourse that covers several different subjects. Here the focus will be on the step that Fairclough labels “assumptions”, where the overall objective is to see what “existential, propositional or value assumptions are made” and if there is “a case for seeing any assumptions as ideological” – where “ideological” will be interpreted as belonging to a certain model of social and technological change.

Discourse analysis is not limited to the examination of systems of knowledge or meaning (even if this is how the method is mostly used here). The method is also used to examine how discourses construct social relations and identities (Jørgensen-Winther and Phillips 2000). The main focus here will be on the reconstruction of what Jørgensen-Winther (2000) calls the ideational content of a discourse and what Fairclough (2003) would refer to as the “assumptions”.

It is, however, important to connect the discourse analysis used to establish a model of the information society with the critical analysis in the third step of my research strategy. As Fairclough (1992) has established the relationship between
social change and discourse is an important and valuable field for the social scientist to examine. Fairclough observes that changes in the orders of discourse (where orders of discourse are identified as sets of discourses) indicate overall social change: “I shall identify certain broad tendencies in discursive change affecting the societal order of discourse, and relate these tendencies to more general directions of social and cultural change” (Fairclough 1992, 200). This method – to challenge the orders of discourse with critical analysis of broad tendencies – will be used in order to test the limits and boundaries of the model uncovered in the first step of analysis. What emerging discourses can be observed and described?

Furthermore, it should be noted that there is a larger question here that also needs to be resolved. In using discourse analysis the researcher has to be aware of the fact that there is, as Fairclough (1992, 64) notes “a dialectical relationship between discourse and social structure, there being more generally such a relationship between social practice and social structure: the latter is both a condition for, and an effect of, the former.”

Discourse reveals, and simultaneously constructs, social structures. In this study the main purpose is to look at one part of this dialectical relationship, but that does not imply denying that there is in fact a second part, where social structures – existing public policy to take the obvious example -determines discourse as well.

**Method II: De-scripting**

Madeleine Akrich established de-scripting as a way of trying to understand artifacts and their politics. In her now classical 1992 work *The De-Scription of Technical Objects* she suggests that all technical objects come with a view of the context in which they will be used and the society they presuppose. By carefully reconstructing the scripts of usage inherent in the technologies we gain knowledge about these implied societies and usages. This is akin to the future archeology suggested by Dahlbom (2003) where the researcher re-constructs the future use of technologies from the implied scripts of these technologies.

The technique is powerful and lends itself well to the purpose of this work. The reason for this is simple and has to do with the nature of policy making. Policy making, in a sense, is a negotiation over scripts and their content. All policy needs to assume scripts and models of society in designing responses. Policy making produces scripts that are then reacted to. In a sense the policy making processes in our society could be described as a competition between different scripts, inscribed by the different actors in the policy making process.

There are, however, some caveats that have to be taken into account. Firstly, it is obvious that there is no “right” answer to what scripts an object presupposes. There may be a family of scripts or a set of scripts compatible with any technical object. This, however, is not an especially serious short-coming, since there will be
certain family likenesses in the different scripts extracted from a technical object suggesting that scripts cannot be arbitrarily assigned to social phenomena.

Another possible objection to this method is that it is imprecise. But this is not really a problem, but rather a strength. Any attempt to show that a certain technology or legal response pre-supposes a certain society with specific qualities will necessarily be imprecise. There is little use in trying to establish the one true society implied by the technologies and laws analyzed here. What needs to be done is to establish a set of societies implied and to show that this set has certain basic qualities that are common to all elements in that set. That determines the degree of generality needed in selecting variables and values in the model as well.

In her 1992 article Akrich shows how de-scripting works. She starts out by noting that it is common in the sociology of technology to accept that all innovators inscribe certain basic qualities and visions of society and use in their innovations. She draws on the work of Bruno Latour (1992) and others, showing that objects necessarily imply or convey ideas about the societies in which they work. She also notes that the designer and his or her intention alone is not enough to be able to understand what is actually the script inscribed in the object (Akrich 1992, 208):

One way of approaching the problem is to follow the negotiations between the innovator and potential users and to study the way in which the results of such negotiations are translated into technological form. Indeed, this method has been widely used in sociological and historical studies of technology. Thus, if we are interested in technical objects and not in chimera, we cannot be satisfied methodologically with the designer’s or user’s point of view alone. Instead we have to go back and forth continually between the designer and the user, between the designer’s projected user and the real user, between the world inscribed in the object and the world described by its displacement.

This is an important point, and we will try to identify points where the negotiations between users and designers, or citizens and policy makers, break down. One key methodological tool in our study is to study failed attempts at legal and technological responses to societal challenges.

The responses chosen for this study are responses that have, in some sense, failed. The stated purpose, the basic idea behind them is not achieved, and I argue that this is because the society envisioned by the designers is a different one from the one in which the users exist. In other words: the object of study here are policies that have failed, laws that are not respected or architecture regulation that is circumvented.

De-scripting technologies in this case means to search in the debris of failed negotiations to ascertain what different world-views collided. Not all failures are total. It could easily be argued that some of the technologies and legal rules I will examine are not out-right failures, and this is easily confirmed by looking at some examples of positive effects. There are digital rights management technologies that seem to work, for example. But by and large I would argue that these policy
responses and technological “answers to the machine” have been less successful than envisioned, and that this is an important indicator of an erroneous calibration of the anticipated, negotiated model of the coming society.

From this follows another interesting methodological point which is this: look at the technologies and laws where negotiations between users and designers or citizens and legislators have failed, since these are the most interesting ones to study. The failures – full or partial - are the examples where the researcher will find useful and interesting differences in the policy makers’ perceived state of society. This is why I have chosen to look at privacy enhancing technologies and copyright management technologies. They are examples of such negotiations that have broken down and where users, designers and society are currently not even at the table negotiating.

I will attempt here to de-script laws much as Akrich suggest that researchers can de-script technologies. This may seem daring or even strange, but is really trivial. Law can be thought of as a kind of technology. This is not how they are perceived in traditional legal analysis, of course: legal analysis is usually conceived of as interpretation of a succession of sources of law in seeking the answer to a specific legal question.

The idea that law can be thought of as technology has been examined in detail in reverse by thinkers and writers like Lawrence Lessig. In Lessig’s Code and Other Laws of Cyberspace (1999) there is, as we have seen, a perfect example of this argument. Code, Lessig states, is law. Architectures of technology regulate. The way societies design their information systems can discriminate against, protect or redistribute individuals’ rights.

But from Lessig’s observation the researcher can construct and experiment with the opposite conclusion: law could be viewed as a kind of technology. Borrowing the metaphors and tools of law to study technology, could enable the researcher to also do the reverse. The informatics researcher can borrow the tools of sociologists and historians of technology to study law. Law is an immensely complex and interesting artifact in human society. It is a kind of social technology, and can be studied as such. Law thus lends itself openly to de-scription of Akrich’s kind. Any law describes contexts as well as actors and users and the society they live in. Laws describe these things even explicitly in their definitions or in some cases even in their names. The so-called “information society directive” (which we will return to in detail) is a prime example. This directive was intended to adapt copyright law to the anticipated information society (even the name of the directive supports this interpretation) and to ensure that the interests of all actors and stake holders were adequately represented in the new legal framework thought to be an absolute prerequisite for the further growth of the information society.

The scripts inherent in legal rules are of two kinds: both the explicit scripts where the law tells us what we can and cannot do as well as the implicit scripts that pre-
suppose a certain order of things as given. Both tell volumes about the society envisioned by the designers or legislators. De-scripting laws promises to be a useful method to examine what a law or a legal framework assumes a society will look like. And in the course of working with this research I have come to think that it is as important to de-script laws as it is to de-script technologies, to show how they interact in complex social phenomena and the overall macro-processes of social change.

Method III: Critical analysis
As has already been indicated, the third step will be engaging in critical analysis of “broad tendencies” (Fairclough 1992) where the constructed model or set of heuristics does not apply or where it breaks down. These challenges to the orders of discourse on privacy and copyright will be examined in detail and the resulting sets of failures of the information society model used to suggest where the model breaks down.

Critical analysis of policy discourse or the established orders of discourse is a method that works by cases. In using critical analysis I will use a set of different cases to show where the model breaks down. The cases will be analysed against the model and the boundaries and failures of the model noted on a case by case basis.

Challenges, the cases used to challenge the set of heuristics are counter-examples, invented questions intended to break the discourse model and show the weakness of the set of heuristics. They are paradoxes in the sense that Lyotard (1984(1979)) uses the word: “Science does not expand by means of the positivism of efficiency. The opposite is true: working on a proof means searching for and “inventing” counterexamples, in other words, the unintelligible; supporting a new argument means looking for a “paradox” and legitimating it with new rules in the game of reasoning.” (Lyotard 1984(1979), 54)

Supporting participatory elements
The method of this study is critical and analytical, it analyses models, sets of heuristics and policy responses using different theoretical methods. But there is also a participatory element informing and underpinning the analytical work. As a practitioner and industrial doctoral student I need to mention and examine this element for completeness as well as examine the problematic of participation. For the last decade I have been immersed in a policymaking environment, and a part of several policy processes, policy-making groups and in the midst of the actual processes I am now trying to describe. Working as an ICT- policy analyst at the Stockholm Chamber of Commerce, I have been a member (from 2001) of the

---

9 Where Akrich (1992) speaks of designers and users in negotiation, it is more accurate to speak here of legislators and citizens negotiating the laws in question.
International Chamber of Commerce’s Commission on E-business, IT and Telecoms. I have been a part of many other policy initiatives as well. In the European Commission’s Expert Group on B2B-marketplaces I worked together with a group negotiating the policy environment of future e-auctions and e-markets. In the Swedish ICT-standardization committee I analyzed questions about standards and new technologies together with other specialists. As a member of the e-Europe Advisory Group I took part in the policy process that led to the current ICT-policy programme in the European Union, the i2010-programme. In a multitude of other groups, venues, conferences, meetings and contexts I have studied and participated in the policy making process as a full time employee first of an industry association and then as the co-founder and CEO of a current affairs magazine. I have written several policy papers and policy reviews – both European and Swedish. I have also engaged in debate on several of the questions in this work, copyright and privacy for sure, but also in the discussion of access and the future of e-government. The main contribution of this immersion in the practice of policy making is the internalization of codes and discourses that are used in the policy field. This, however, also represents a risk: there may well be aspects of the discourse that are not visible to one who has participated fully in the process, and this is a caveat lector. To safeguard against this the researcher can strive to bracket his or her informal knowledge, but this is at best an incomplete method.

**Data sets – choices and materials**

The data sets I have chosen to study are different texts and related materials (web sites and other documents). Firstly, I will study different high-level policy texts. To anchor these studies I will examine one text that has been identified as the canonical starting point by several authors (see for example Webster 2002) for the information society debates, the work of Daniel Bell.

**Policy texts.** The policy texts I have chosen to work with are the action plans and overall descriptions of the information society produced in the European Union policy process. The choice of policy texts was made on the basis of importance and relevance to macro-level social change – the action plans I study have been the governing documents for European ICT-policy. To delimit the choice to European texts was a conscious choice made in order to limit the materials. Using “action plans” and high-level texts ensures that the model of the information society model is constructed from an accessible policy discourse. When it is then tested against particular pieces of legislation and architecture regulation, the result, I will claim, confirms the reproduction of macro-level discourses in the production of lower-level policy responses. The choice of a starting point (not in itself a pure policy text) in the work of Daniel Bell serves to show the stability of the policy discourse studied. The discourse analysis practice of establishing intertextuality or the genealogy of a discourse (Fairclough 2003, 39-62) offers the possibility of showing not only a set of assumptions and a simple set of heuristics, but also the possibility of showing that this set has been stable for some time. The purpose in showing this is, in turn, to show that the discourse is entrenched and that it is relevant for study.
and important to the future development of society. A discourse that is easily changed and displaced is less valuable as an object of study than one that is generatively entrenched (situated deep within the orders of discourse).

*Policy responses – legislation and technology.* When embarking on this project one crucial point became the choice of laws and technologies to de-script. In the following section I will describe the choices and explain why I chose as I did. The first point, however, is to explain why I felt that it was important to study both law and technology. The policy responses to the challenges imposed by the announced coming of the information society have been of two different kinds. The most obvious policy responses are the new laws drafted and launched by politicians in order to prepare us all for the advent of the information society. There is no shortage of such responses. Some can be said to have been horrible failures, at least if we evaluate the cost-benefit equation of their being put in place. Others have been moderate to full successes and have been timely responses to legal challenges. That it is necessary to examine the actual laws motivated by the emerging information society thus seems obvious. But why examine technologies as well? In what sense can technologies be seen as responses to legal challenges?

It is possible to argue that technologies are highly relevant to understand policy responses to the information society. The basic idea behind the use of technology as a policy response was deftly formulated by Charles Clark in his assertion that the “answer to the machine is in the machine” (Clark 1996). With the information society, then, comes the idea that *policymakers can use the very technologies that change and shape our society to legislate and manage this change.* Policymakers can, in some sense, tame the technologies and shape them into policy instruments. This has been most obvious in the areas of copyright and privacy, but the same kind of thinking – thinking that technologies indeed can take some of the role played by legislation – is found in other areas as well: in discussing freedom of speech and the protection of minors from harmful speech the role of filters is as heavily debated as that of lawmaker.

Laws and new technologies have been used in tandem to respond to challenges posed by new uses of information and communication technology. In some cases they have even been entwined: laws have been used to protect the technology used to protect legal rights. The perhaps most obvious example being how digital rights management technologies are now protected in copyright law, requirements can be found in the legislation on data protection on the design and use of technical systems that are at least as relevant as examples of attempts to regulate the design and use of technology in law. Architectures have become regulatory tools. They are today a part of the regulatory toolbox and treating them as important components in socio-legal phenomena makes sense for a large number of cases. That it is necessary to include both laws and technologies in the analysis of the policy responses to the information society follows from the realization that they are deeply interconnected.
When choosing the laws to analyze in this study I used a number of different criteria. Firstly, I was anxious to include laws that are relevant and important. I wanted legal areas and laws that have been debated and discussed widely. Partly because this signals that they are important, but also to tap into the existing body of research and show where I think that a noise society perspective is useful. I was, secondly, also eager to find laws that were more than national constructs. There is a very interesting Swedish law on bulletin boards (SFS 1998:112) that I was tempted to include since it offers a peculiar and strange example of how laws presuppose certain technologies, but I excluded it on the merits that it had little or no application outside of the borders of Sweden. Thirdly, I thought it important that the laws or legal instruments examined were complex enough to offer a full world view. Short legal amendments offering to equate electronic signatures with written signatures are interesting, but difficult to de-script. The legal instruments I sought would have to be complex enough to contain a conceptual schema or a model of the society they were thought to respond to. In view of these criteria—debate, international relevance and complexity—three areas naturally suggested themselves: data protection, copyright and freedom of speech. After much doubt and discussion I excluded freedom of speech to concentrate my effort. I also found this particular area less promising in the search for internationally applicable legislation. There is no “digital freedom of speech”-directive in the European Union, to take one example.

I also delimited the choice of laws in time, to concentrate on policy responses that were drafted in and around the middle of the 1990s. This is a further reason to exclude freedom of speech since there to my knowledge is no such legislation from that time of the dignity and complexity we require. Data protection and copyright offer ample challenges and material for analysis. The legislative instruments I have chosen to de-script are European directives and the literature on these and the problems they discuss is voluminous. The debate on data protection and copyright has been heated and the complexity of the instruments is such that it is quite fruitful, I will argue, to use de-scription to examine them. The legislative instruments I have chosen are the data protection directive (95/46/EC) and the information society directive (01/29/EC). Both these directives have had a tremendous impact on national legal systems in the European Union and they are both—as we shall see—open responses to the challenges thought to emerge from the coming information society. The two directives are also examples, I would argue, that have, at least partly, failed in accomplishing what was expected of them by policymakers. Data protection in the European Union has not been saved or guaranteed by the legislation put in place. Piracy has not been curbed by the measures put in place by the information society directive. These are not full failures in the sense that the legislation is obsolete, but the legislators are still negotiating with the citizens and businesses involved and in some ways it is not impertinent to note that negotiations seem to have been brought to a stand-still.

If legal policy responses to the information society have been many, the technological responses have been equally numerous. Drawing on the popular and
already referenced idea of the “answer to the machine being in the machine” many innovators and companies have argued that they have the technology to accomplish what legislators have failed to do. There are multitudes of new technologies to choose from if we want to apply de-scription techniques. Filter technologies like the ones provided by “cybernannies” contain assumptions and scripts that are both fascinating and relevant to an analysis of the information society, but in order to find a certain logic here I have chosen to concentrate on technologies providing responses to challenges to privacy and copyright. This is not necessarily a problematic limitation. The set of technologies setting out to protect, manage, describe, negotiate and control copyright and privacy is immense. Privacy enhancing technologies (PETs) and digital rights management technologies (DRMs) are widely available in different designs and lend themselves to ready analysis. The way these technologies were envisioned, and the way the policy makers thought they would be designed, is indicative of the scripts, the possible usage of the technology envisioned. A further fact supporting the choice of these two categories of technologies was that they are also – in some sense – failed technologies. This is shown not least by the fact that the failures of, for example, audio compact disc protection are discussed openly in law journals (Lyon 2007). DRMs have not stopped file-sharing of pirated music and films. PETs have not been adopted in significant degree and remain a promise to be fulfilled. In the previous case the negotiations between designers and users have degenerated to controversial law suits. In the latter they have lapsed into benign ignorance. Within the actual categories there are many different applications and models that lend themselves to de-scription. I will choose a few major ones, giving ample reference to others for the reader to examine.

Policy failures. The choice of “broad tendencies” or dissonances that upset the orders of discourse is necessarily ad hoc. There is no simple way or method to identify phenomena that disturb a certain set of heuristics. The challenges I have chosen or invented are challenges that I have perceived to be interesting and where I think that the challenge is important enough to make the model fails. When studying and stress-testing any system one will use the most challenging – if ad hoc – cases to do so. The object of the third step of the research strategy is to make the model fail – to examine in what way it actually fails and use this insight to formulate an alternative and complementary model.

10 I also have the advantage of having authored an early (1998) study on electronic copyright management systems as well as some work on privacy enhancing technologies (1999) and this affords me the opportunity to reflect on what has happened with these technologies over time. Again it is important to situate the technologies some way back in time to gain at least a slight perspective, even if it can be argued that a few years make little or no difference.
3. Constructing an information society model

Introduction
After having established the theoretical foundations and reviewed the methods it is time to proceed to the first step in the research strategy. This step will construct a set of heuristics or a model of the information society as this society is depicted in European policy texts. Using policy discourse analysis I will try to situate the European policy texts in a genealogy and network of texts that can be traced back to Daniel Bell’s (1973) work on the post-industrial society. The purpose of this is to show how the model of the information society is constructed and maintained in the policy process through a consistent intertextuality. This intertextuality amplifies the model and entrenches it in the discourse, makes it resilient and slow to change – qualities that are essential to appreciate the importance of a set of heuristics or societal model. The more entrenched, the more important it is.

Bell is not the only possible starting point, but he is often used as a canonical starting point for discussions about the information society. There is, however, another important starting point too. While Bell discusses the sociology of the post-industrial society and points to many themes that have become identified with the idea of an information society, he does not emphasize the economics of information. The idea that the economy is now based on information is often referred to as another important theme in the information society, and here the work of Porat (1977) and Machlup (1962) is often referenced.

Machlup examined the share the information sector and knowledge economy had of the national economies, and Porat continued to examine the information economy in his work, documenting the share it had of the overall economy. This focus on the economics of information is an important aspect of the information society model. The reason I have chosen to start from Bell rather than from Machlup or Porat is that Bell actively tries to described the entire society, while the more narrow focus of Machlup and Porat is economic. In thinking about the information society model I will try to include this aspect as well, however.
From Bell to i2010 – a genealogy

The idea of an information society is hardly new. The concept can be traced back to several different authors. Frank Webster, a sociologist and professor of cultural studies at the University of Birmingham, has examined a multitude of definitions of the information society in his work *Theories of the Information Society* (Webster 2002). In a useful analysis he argues that there are at least five different definitional categories being used in defining the information society: the technological, the economic, the occupational, the spatial and the cultural. And in each category examination of technologies, economic parameters, occupational statistics, spatial relations and cultural behavioral patterns are used to define society as an information society in different ways.11

Webster also tracks the origins of the information society. Among the most important early writers he mentions Daniel Bell (1973) and Marc Porat (1977). In order to anchor the policy discourse analysis I will start with Bell and show how the basic discourse established by Bell has filtered down through the years, keeping a strong grip on public policy for an extended time.

In *The Coming of the Post-Industrial Society: A Venture in Social Forecasting* (1973) Bell sketches a new form of society, based on different principles than the ones that underpin the industrial society. He identifies five different “dimensions” that can be used to analyze this society. These dimensions form the core of the discourse that has developed and strengthened over time into the multi-faceted and prevalent discourse of the information society encountered today.

Bell writes (p 14):

> The concept of the post-industrial society is a large generalization. Its meaning can be more easily understood if one specifies five dimensions, or components, of the term:

1. Economic sector: the change from a goods producing to a service economy;
2. Occupational distribution: the pre-eminence of the professional and technical class;
3. Axial principle: the centrality of theoretical knowledge as the source of innovation and of policy formulation for the society;
4. Future orientation: the control of technology and technological assessment;
5. Decision-making: the creation of a new “intellectual technology.”

---

11 Webster, highly critical of the different categories as well as of the concept of the information society as such, proceeds to examine these in great detail to find fault with most of them.
The idea of an axial principle is introduced a few pages earlier. Bell speaks of axial structures and axial principles as the “organizing frame around which the other institutions are draped” and “the energizing principle that is a primary logic for all the others” (p 10). He exemplifies with several social theorists, and argues that Weber worked with the idea of rationalization as an axial principle, while Marx worked with the business form as the axial structure of capitalist society (p 10).

Bell’s vision of the post-industrial society is a vision of control, and it marks the beginning of a discourse of control that then comes to permeate much of the thinking about the information society. Bell even writes about the “control of technology and technological assessment” and suggests that the post-industrial society (he examines but rejects the concept of “the information society” on vague grounds) will be a society that assesses and chooses technologies to architect structures of control in society.

The idea that society will make better decisions and that theoretical knowledge will become central also implies a greater degree of control and a quality of theoretical knowledge that will increase over time. The very idea of “intellectual technology” is intriguing. Bell writes: “What is distinctive about the new intellectual technology is its effort to define rational action and to identify the means of achieving it” (p 30) and continues “[t]he goal of the new intellectual technology is, neither more nor less, to realize a social alchemist’s dream: the dream of ordering the mass society” (p 33). Bell himself remains carefully skeptical of this goal, but the description can be seen as an accurate representation of much of the hope of the policy discourse that follows.

I will now move on and examine genealogical traces of Bell’s vision in a number of European Union policy documents. The documents I have chosen are some of the large plans and visions of the information society presented by the commission, specifically the Bangemann report (which is an important starting point for ICT-policy making in the European Union) and the succession of action plans put forward by the European Commission.

I will package the five dimensions into three. The reason for this is that my intentions differ from Bells. Bells five dimensions were used to analyze statistics and other sets of data than the ones I will examine. Where some of Bell’s dimensions are separate in order to enable another kind of research strategy, they can be melded to be used in policy discourse analysis.

The idea of a new intellectual technology can be seen as and treated as a symptom of the belief in technological control, and so I will treat them as one element in Bell’s vision. I will also bundle the centrality of theoretical knowledge and the pre-eminence of the professional and technical class, since these two dimensions intersect in that the technical and professional class are the keepers of theoretical knowledge – and how they are defined in opposition to the other classes. Again,
since there is no need to study these separately in doing policy discourse analysis, I will merge them into one category.

**The Bangemann report** is a starting point for much of the ICT-policy discourse in the European Union. The report was commissioned by a high level group with broad representation from “prominent persons” in December 1993 and delivered in June the following year.

Using the condensed version of Bell’s dimension the following analysis can be offered.  

*A service economy*. The Bangemann report concentrates on information services and the importance of the growth of a market for information services in the European Union. The main benefits for consumers are also envisioned as greater access to services and entertainment, “from home banking and teleshopping to a near-limitless choice of entertainment on demand”.

*Pre-eminence of the professional and technical class and the centrality of theoretical knowledge*. The theme of the technical class enters the Bangemann report as a fear for a “two-tier society”, where those groups who are not “comfortable” with the new technologies may reject them. The Bangemann report also stresses the need to “[p]reparing Europeans for the advent of the information society” – with lifelong training and education.

*Control through technology and technological assessment and a new intellectual technology*. In the initial description of the “revolutionary challenge to decision makers” the authors write: “Technological progress now enables us to process, store, retrieve and communicate information in whatever form it may take – oral, written or visual – unconstrained by distance, time or volume [...] this revolution adds huge new capacities to human intelligence” – indicating a strong sense of control through technology in the sense, at least, that technology will enable humans to control their environments. Furthermore, the report envisions a standardization process that will bring forth new technologies where needed: “When the market is not providing acceptable technical solutions to achieve one of the European Union’s objectives, a mechanism should be sought to select or generate suitable technologies” – a vision that connects closely to Bell’s description of the post-industrial society as a society where technological assessment and control is unproblematic.

Interoperability and structure in information sets is not seen as a great problem, and the Bangemann report – while touching on the subject in connection with

---

12 Pages will not be offered for the reports and action plans, since they are available in a number of different layout versions and printings. There is no simple and authoritative source for all the documents, and the quotations can easily be traced by searching in the documents, so the actual motivation behind offering the page numbers of different layouts is lacking.
telecommunication standards – proclaims: "World-wide interoperability should be promoted and secured". Interoperability between semantic standards or information schemas is not mentioned or considered.

Another area where the control aspect is clear is when the report discusses privacy and encryption. The authors considered encryption as an enabler of the information society, but reserved the right to legislate use and access to strong encryption for governmental control and access. The idea that it would prove almost impossible to control the use of encryption is nowhere to be found. Instead, the report states that "a solution at the European level is needed which provides a global answer to the problem of protection of encrypted signals and security".

The research programmes in the European Union is given the role of providing society with technologies and solutions, and the report suggests ten applications that need to be introduced for “blazing the trail”: teleworking, distance learning, a network for universities and research centers, telematic services for SMEs, road traffic management, air traffic control, healthcare networks, electronic tendering, trans-European public administration network and city information highways13, expressing the assumption that it is a policy decision to choose among technologies (assess them, to use Bell’s phrase).

The Bangemann report also enumerates effects for different actors, and the description of the actors here is valuable to further analyze the discourse:

"What we can expect for...

- Europe’s citizens and consumers: a more caring European society with a significantly higher quality of life and a wider choice of services and entertainment.

- The content creators: new ways to exercise their creativity as the information society calls into being new products and services.

- Europe’s regions: new opportunities to express their cultural traditions and identities and, for those standing in the geographical periphery of the Union, a minimizing of distance and remoteness.

- Governments and administrations: more efficient and responsive public services, closer to the citizen and at lower cost.

- European business and small and medium sized enterprises: more effective management, access to training and other services, data links with customers and suppliers generating greater competitiveness.

- Europe’s telecommunications operators: the capacity to supply an ever wider range of new high-value added services.

---

13 Local networks for cities.
The equipment and software suppliers; the computer and consumer electronics industries: New and strongly-growing markets for the products at home and abroad”

Note that citizens and consumers are passive users of services, and not active creators. The content creators are separate. They have “their creativity” and are separated from the citizens and consumers, a class of their own. The unsaid here, the assumed, is that creativity is still a limited domain.

In essence the Bangemann report contains assumptions that form a policy discourse that is strongly reminiscent of Bell’s description of the post-industrial society – the elements of control, structure, intellectual technology and the pre-eminence of the knowledge class can all be reconstructed from the text.

The Bangemann report was formally adopted in a slightly changed form as *Europe’s way to the information society* – a communication from the European Commission. While less bombastic the action plan follows the report closely. The action plan is interesting since it is a response from the formal structures to the exorbitant tone of the Bangemann report, it is toned down and factual rather than visionary, but still the same themes remain: control is still the basic theme, and issues of privacy and intellectual property rights are addressed in the same way as in the Bangemann report.

**The e-Europe 2002 action plan**, subtitled “an information society for all” was adopted in 2000. The first action plan set out an intense and ambitious schedule which in parts had to be revised (all the actual dates are in 1994 and 1995, but many of the regulatory reforms undertaken by the Commission took longer than that to complete). The Commission then received a high level expert group report in 1997, and that report then was developed into the e-Europe programme over a number of years (Anttiroiko 2001) and issued and adopted in 2000.

Again, an examination of the document with the intention of tracing intertextuality is illuminating:

*Service economy.* The e-Europe programme is heavily connected to the so-called Lisbon process and still focuses on services. The policy methods used include support for “new infrastructures and services across Europe” and the focus on Internet services – specifically “cheaper and faster Internet” is strong. The regulatory reforms focus on the telecommunication service sector with a view to speeding up Internet adoption.

Infrastructures are admittedly not services, and the focus on them could be seen as a deviation from Bell’s dimensions. On the other hand it is possible to argue that infrastructures play a supportive role, they are demanded for offering services of different kinds. This is supported by the lack of focus on products through-out the report.
Pre-eminence of the professional and technical class and the centrality of theoretical knowledge. Again the role of the technical class is approached through the fear of a digital divide. The question of the preeminence of the professional and technical class is addressed as a problem that needs to be met by education: “Europe’s education and training systems must adapt to the knowledge society” – an example of Winner’s theme of reverse adaptation. The centrality of theoretical knowledge is also obvious in the different initiatives to establish life-long learning that are included in the action plan.

The policy discourse also constructs a process of victimization wherein those who lack knowledge will be excluded from society. The action plan worries that “further efforts will be required to address the problems of those who risk exclusion from the information society and the workforce.” Employability is decided by theoretical knowledge and the action plan even sketches a necessary fight against “info-exclusion” for citizens with disabilities.

Control through technology and technological assessment and a new intellectual technology. In the e-Europe action plan an interesting dissonance emerges. Where the Bangemann report did foresee that security would be an important part of the future information society, the authors did not harbor much doubt that the security issues would be resolved with regulatory measures. The e-Europe action plan notes that “[t]he economic damage caused by disruptions (e.g. by virus, denial of service attacks) in Internet functioning is increasing”.

The actual evidence pointing to problems in controlling technology are however trivialized and reduced to a question of integrating security products better, and the solution is found in re-adjusting to the new environment. The policy discourse does not waver, even if the security problems have increased: a new technology, the smart card, is introduced as the solution: “smart-cards is an enabling technology which can increase the level of confidentiality and privacy in information society services”. One way of interpreting this is to say that the technological fix is used as a rhetorical device intended to show that the policymakers still control the social and technological change.

The perceived problem of slow growth in e-commerce is addressed through legislating on technologies that are thought to be enablers, such as e-money. This pattern repeats itself from earlier efforts to legislate technology into being and use: the legislation on electronic signatures was another attempt to assess and legislate on not-yet-offered technology in order to speed adoption and development.

This use of legislation to create an imperative of use and development is another inherited policy element from Bell’s post-industrial society. Bell’s new intellectual technology seems, at first glance, to be lost from view, however. Little is written about how technology will enhance decision making, but what has probably happened is that the wish for a new intellectual technology has merged with the idea of the future of government. The weberian rationalization of the state in the
bureaucracy melds with Bell’s vision of new intellectual technologies and the result is a demand for an e-government, an e-administration, which will ensure that the government becomes more efficient, more decisive and cheaper to work with. The Bellian intellectual technology becomes a technology of the state and is subsumed under the e-government programmes for new forms of electronic public procurement, e-health and e-administration.

Bell’s influence remains strong in the e-Europe programme, and his dimensions are still present. The changes in discourse, the first inklings of dissonances (information security problems) are observable, but not decisive in changing the overall policy discourse. Bell’s intellectual technology is merged with the idea of the better, stronger information society state into the vision of e-government.

The follow-up action plan to the e-Europe 2002 action plan, e-Europe 2005, is adopted in 2002 and develops much the same themes as the previous action plans.¹⁴ The connection with the Lisbon agenda remains strong.

Service economy. Services remain the main focus of the plan. Mobile, multimedia and e-commerce services are identified as main growth factors and the convergence problematic is introduced in a broader context. Services are identified as more problematic than before and funding becomes an issue: “funding more advanced multimedia services depends on the availability of broadband for these services to run on, while funding broadband infrastructures depends on the availability of new services to use it.” The existing game, where each actor waits for the other to make the first move, is addressed as the basic problem of the service economy and the policy response is to increase demand and reduce uncertainty in different ways. Public services – using the infrastructures – are hailed as possible solutions to the waiting game problems. The service economy is now not only a private market, but it becomes a part of the public sector’s responsibility. A “next generation of services” – post-convergence – is expected to increase productivity and employment.

Pre-eminence of the professional and technical class and the centrality of theoretical knowledge. The new action plan goes further than earlier plans. Where the e-Europe programme originally was worried about the employability of those that did not possess the skills necessary to work in the information society, the new plan states bluntly: “Member States [...] should launch actions to provide adults [...] with the key skills needed for the knowledge society, to improve their employability and overall quality of life (my italics)”. The key skills are identified as “basic computer skills and higher order skills such as teamwork, problem solving, project management, etc.”.

¹⁴ To avoid confusion here it is probably a good idea to note that the year in the title of the action plans is the expected date when the plan will be complete.
Control through technology and technological assessment and a new intellectual technology. Security remains a concern, and a cluster of policy initiatives are launched to come to grips with what is perceived as a growing problem. The smart card is mentioned, but not hailed as the overall solution any more. More research is promised, and the field of research is widened to include “the ‘human factor’ in security e.g. basic standards, user-friendliness of systems.” A Cyber security task force is promised, a “center of competence on security questions” and the answer to increased security problems is yet another technology, a grand vision of “a European computer attack alert system”. But something is happening in the security field: influenced by outside developments the Commission now speaks of “a culture of security” and notes that the problem of security may not be a solely technological problem. Control through technology is not supplanted by, but complemented by control through culture. E-government remains as the hope for a new intellectual technology, and now also as an enabler of the service economy.

Another area where the action plan points out a need is interoperability. There is a growing concern with the lack of interoperability, but the scale of the problem is still underestimated: “By end 2003, the private sector should, supported by the Commission and Member States, have developed interoperable e-business solutions for transactions, security, signatures, procurement and payments. This will facilitate services enabling seamless, secure and easy cross-border electronic commerce and mobile commerce.” The faith in technology assessment and control through technology is undeterred by earlier problems with interoperability.

The action plan does, however, suggest that the policy area is growing too quickly and in a diversified way. A new steering group is suggested as an institution to coordinate the policy field, the private sector is brought in to further control the development. This is perhaps another small sign in the discourse that the policy makers felt that the information society was not completely under control. The idea of introducing an institution for coordination and exchange of experiences signifies a change in the attitude towards the information society – the plethora of policies on national level signify another change: the questions are becoming increasingly important and an institutional conflict over where the regulation of information society issues should be decided is possible.

The intertextual network of policy texts is still strong, even though the security issues are showing that the level of control thought to be possible may not be realistic.

The next plan, the i2010-plan, represents a kind of breaking point and a return to the early beginnings of ICT-policy. The subtitle – “A European Information Society for growth and employment” echoes the earliest report on the information society available from the European Commission, a White Paper called Growth, Competitiveness and Employment: The challenges and courses for entering into the XXlst century (COM 1993). The mention of competitiveness is conspicuously gone, but this may be because the Lisbon agenda, at the time of formulating the action
plan, was heavily criticized and judged a failure. In a sense one can read the omission as a resigned attitude to the promises inherent in the Bangemann report, a disappointment if one will, but this may not be the entire truth. In the institutional battle between the commission and the Member States on ICT-issues, the Member States reclaimed much of the initiative in issues pertaining to e-government development and the overall ICT-policy discourse was fragmented into different areas: e-government, e-procurement and information security received growing interest and develop into policy fields of their own, if closely connected with macro-level societal ICT-policy. This was reflected on a very basic level in the length of the action plans. The i2010-plan is merely 12 pages, down from 22 for the e-Europe 2005 action plan and 29 for the e-Europe 2002 action plan.

Service economy. The convergence theme is strong, and services ‒ media services rather than multimedia services ‒ are identified as a key driver. A new policy convergence is sought in response to the digital convergence and regulatory frameworks need to be changed, the Commission states. Services are also the driver behind the “single European information space” ‒ an interesting concept that closely mirrors the single market. The provision of digital services is also one of the first objectives of the action plan. The service economy remains a strong focus in the i2010-plan. Infrastructures to provide services are expanded to include spectrum issues.

Pre-eminence of the professional and technical class and the centrality of theoretical knowledge. Inclusion is a strong theme in the i2010-plan. The geography of the professional and technical class becomes an interesting theme: regional divides and competence gaps are highlighted as priorities. A new technical class emerges in the technical public servant, providing “ICT-enabled public services” and the new technologies are even more heavily identified with the quality of life.

Control through technology and technological assessment and a new intellectual technology. Security is lifted from the overall policy document and the action plan refers to another planned policy document with a Strategy for a Secure Information Security. The security problems have by now developed as a policy field of their own, strong and connected with the growing policy discourse around security in society overall, following the September 11 terrorist attacks.

The policy discourse of the information society is still closely connected to research and the hope of assessing and developing new technologies is not gone. Interestingly, the plan identifies a number of “key bottlenecks” that tellingly indicate the problems that remain: “interoperability, security and reliability, identity management, rights management and ease of use”.

The notion of intellectual technologies, helping us decide better, is re-introduced and research efforts will focus on “technologies for knowledge, content and creativity ‒ including cognition, simulation and visualization”. This is an
unexpected turn, but follows from the revolution in the role of the user in the information society. From being a simple consumer, the user is now an empowered prosumer, both producing and consuming content and services.\textsuperscript{15} The i2010 action plan remains true to its inheritance from Daniel Bell and follows the discourse closely. In a sense it moves closer to the center of the intertextual network, towards Bell, in that it re-introduces the idea of intellectual technology.

Daniel Bell’s sketch of the post-industrial society remains a strong intertextual center in the policy discourse on the information society. The themes of control, a technical class and a service economy remain the organizing principles of the discourse, the basic structure of the policy debate.

One theme in the policy discourse stands out: the belief in technology assessment and research as rational methods of meeting the information society. The thought that smart cards would solve information security issues, the conviction that interoperability would not be a problem and the faith in regulation as a means to address the issues of content production and intellectual property rights.

The information society model I claim is used or implicit in policy making is less complicated than the complete Bellian analysis. It needs to be simpler and more like a rule of thumb to be useful for policy makers and for this study. I have chosen to reduce Bell’s analysis to the \textit{theme of control}. This control theme can be divided into three different sub-themes that then can be used to form the basis of the information society model I claim is implicit in the public policy process:

- Control over information production. Bell’s postindustrial society is one where control over information production is possible and necessary. Theoretical knowledge is in the hands of a professional or technical class, a preeminent class that dominates the processes of technology assessment and control.

- Control over information distribution. Bell’s world is a world in which information is readily available when needed and erased when harmful. The same themes run strongly through the policy discourse of the European Union on new technologies.

- Control over structures and interoperability. The idea that information interoperability – semantic, technical, legal and organizational – would pose problems does not enter into Bell’s model and remain equally absent, for a long while, from the policy discourse on the information society in the European Union.

\textsuperscript{15} The distinction between content and services remains strong in the policy discourse, which may seem surprising. One possible explanation has to do with the policy process: the traditional content producers and content holders do not see what they do as services, so they refuse to change.
Is this enough? Can these three rules of thumb be used to examine actual policy responses in legislation and architecture regulation? Remember that the policy discourse analysis started with Bell, and that Webster (2002) and others traced the information society idea to Bell and Marc Porat (1977). Porat’s contribution was one of endowing information with value and making the information society one where information became the carrier of value. This dimension remains important in the policy discourse as well as in the general view of the information society – retracing the discourse analysis the element of information as a valuable commodity is present in several of the examples I have already given. The three rules of thumb generated by transforming the policy discourse analysis should, then, be complemented with a fourth: a belief about the value function of information that is hidden behind the recurrent focus on knowledge in the policy discourse. The value function of information is perceived to be simple: information gathered is transformed to knowledge and immediately valuable.

With these variables: information production, information distribution, information structure and information value, it is possible to construct a very simple model of the information society, and the next step will be to trace the influence of this model. Before doing this it is useful to reconnect the results of the policy discourse analysis with the theoretical foundations developed earlier. What kind of society is the information society as it is developed in the network of intertextuality examined here? There is, one discovers in a close reading, a difference between Bell and the European policy texts that is quite interesting. Bell speaks very little about the market. The European policy texts all speak about market solutions and free market development (see the Bangemann report for ample examples). Two different information societies can then be distinguished: Bell’s model can be represented as taxis and control over our systems and the model inherent in the European policy documents is one where kosmos and control interact.
The policy texts assume the same control as Bell does, but they also assume a free market order, a spontaneous order. This is one of the first dissonances in the information society model: can one have control and kosmos? Are the two actually compatible? If they are not compatible the model will fail – as we will see it does.

**Constructing the Information Society Model**

Having come this far I can now summarize and formulate the model of the information society that is needed to examine the policy responses The simplified model, looks like this:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Model Assumption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Production</td>
<td>Information growth is modest to fast but it is also fairly concentrated, where industry and government are the main producers of information.</td>
</tr>
<tr>
<td>Structure</td>
<td>Information is well-structured and interoperability at different levels is achievable with some effort.</td>
</tr>
<tr>
<td>Distribution</td>
<td>It is possible to secure networks and information is disseminated through a few large nodes in the network.</td>
</tr>
<tr>
<td>Value</td>
<td>The value of information increases with the amount of information available, with the usual diminishing returns.</td>
</tr>
</tbody>
</table>
In the next chapters I will show how that this is the model that can be found in the actual policy responses developed by policy makers. This is a model where the element of control is strong. It is a set of heuristics implying that architecture regulation is possible with few problems and where use of technology can easily be regulated in law.
4. Tracing the information society model

Traces and validation
The information society model suggested in the previous chapter was constructed from a network of high-level policy texts. To ascertain whether or not this model is actually used by policymakers requires using the description methods introduced at the second step in the research strategy to reverse engineer the model from a number of actual policy responses, to trace it in actual policy responses.

In this chapter this will be done for both legislation and architecture regulation. Drawing on the theory of architecture regulation I submit that describing technology used to regulate offers a good way to ascertain and reverse engineer the model implicit in policy responses.

Why, then, trace the model through both legislation and architecture regulation? The reasons are many. Firstly, it is a question of robustness. If it is possible to establish through two different forms of policy responses that it is likely that a certain set of heuristics is used this adds to the robustness of the analysis. Secondly, using only a de-scripting of legislation would have given an erroneous account of the importance that architecture regulation plays in the modern public policy process. Both measures are equally important and deserve equal attention in the research strategy as well as in the actual policy process.

In the following pages I will show that the information society model is present both in privacy legislation and privacy enhancing technologies as well as in copyright legislation and electronic copyright management systems.

The Data Protection Directive
The data protection directive\textsuperscript{16} (95/46/EC) is a central piece of legislation. Not only does it create a common legal framework for privacy in the European Union, it also introduces the idea that the object of regulation should be the management of personal data – a \textit{processing model}. The alternative is clear: policymakers could establish a liability regime where those harmed by some processing of personal data had a right to sue for damages. This model – an \textit{abuse model} for protecting personal data – is being raised more and more often as a possibility in the discussions on reforming the directive.

The fact is, however, that Europe has the most comprehensive legislation in the world on privacy. And this legislation was debated, discussed and introduced in 1994 to 1995, when the Internet was still young and new. The risk for misconceptions and over-regulating is obvious as well as the risk of missing important threats to privacy, and the critical voices have been many – from business interests arguing that the costs imposed on companies are too hefty to motivate with the benefits for privacy, to privacy advocates arguing that the legislation provides little or no guidance in a multitude of new questions facing citizens.

The directive has now been transposed to national law in all member states and there is a growing body of research, case law and commentary on the legal content of the directive. What I will do here, however, is not engage in legal interpretation. The purpose of this section is to find a set of de-scriptions of the directive that show what kind of imagined society this piece of legislation is a response to, what set of heuristics has been used.

That the directive is a response to an idea of a developing information society may seem trivial, but it is explicitly stated in the preamble of the directive:

\begin{quote}
"Whereas, given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data;"
\end{quote}

The attempt at generality – to escape the perceived error of not being \textit{technology neutral} – is significant as well. There is a sense in the directive of having found a model that is independent of the actual changes in technology that can occur. Technology-neutrality is often seen as a merit and to state that legislation is technology-neutral has become the finest praise one can lavish on a new law. This

\textsuperscript{16} 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
is strange, taking into account that this supposedly technology-neutral law already seems out-dated in many different areas.\footnote{One could write quite a lot about the concept of technologically or technically neutral legislation. The opposite of which would be technologically \textit{determined} legislation. I think that there are good arguments for stating that there is no such thing as completely technology-neutral legislation, and that the real issue is to be conscious of what legal rules are technologically determined and make sure that the \textit{form} chosen for these rules is such that it is open to frequent amendment. The aim of a good legislator should thus be not to become so general as to escape all technologically determined rules, but to become so wise in the ways of technology as to be able to choose the form of legislation in harmony with the technological detail required to achieve the stated goal.}

For the researcher the attempt at technology neutrality becomes a gift, however, since it implies that what is left of inscription is what the legislators at the time were not even aware of as technologically determined. The inscriptions in a law thought to be technology neutral tell a lot about the society, the actors and the interactions regulated in the directive.

In our de-scripting of the directive we will use the preamble of the directive. The preamble is the part of a directive that explains the reasons for and the arguments behind the shaping and launching of the directive, and it is rich with policy making scripts. It offers a slightly more expanded version of the condensed legal language in the actual articles and makes it easier to follow the policymaking process. The preamble of a European directive is also provided as a kind of interpretative background, although the legal status of the text in the preamble is highly debatable. It is uncertain or even unlikely if the European Court is bound to respect interpretations and comments made in the preamble if they find that they are incompatible with the overall interpretation of the articles in the directive.

The only possible drawback in using the preamble as study object is that the researcher risks losing some interpretative space that is implied by the articles but eliminated in the preamble, that is where the preamble says more than the actual article where the corresponding rule is stated. It may be assumed, however, that this risk is negligible for the purposes here. I am not trying to find exact legal meanings or an exact judicial interpretation, but rather reconstructing the ideas of society inscribed in the directive as a piece of technology.

This is also why the \textit{legal} status of the preamble is unproblematic. The text in the preamble may not be legally binding for the courts, but this is a matter of little importance if the researcher is not making a legal, but rather a de-scriptive statement about the society model implied by the directive.

The interpretation is given a head start in paragraph 2 in the preamble. The society envisioned in the data protection directive is a society filled with "data processing
systems” and these systems are complex wholes that are “designed to serve man” (par 2 in the preamble).

The systems themselves are made actors in the vision of society that inhabits the directive, the systems "must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals”.

One could write volumes about this view of data processing systems and the degree of anthropomorphism that permeates it, but the perhaps most interesting thing about the formulation is just the fact that the large-scale systems are actors in the data protection directive.

The systems control information distribution and production, they are units of regulation in the sense that they can be subjected to the will of the legislator and they must do so, for they have been designed to “serve man”. The paragraph in its entirety says:

(2) Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;

This speaks eloquently about the view of information production and processing in the directive. Information is produced and processed in large-scale systems that "contribute to economic and social progress".

The Swedish Data Act of 1973 is modeled on the assumption that personal data processing is an interaction between large data processors, first and foremost the state and its authorities, and the citizen. The data protection directive, however, implies that the processing of personal data is not only an interaction between citizens and state, subject and sovereign.

The directive portrays personal data processing as a pre-requisite for the internal market. Indeed, this is the very rationale behind the directive as p 3 in the preamble which states:

Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded.

That both public and private actors are involved is clear in p 5 which notes that data will flow between “all those involved in a private or public capacity in economic or social activity in the Member States.”
Personal data in the directive is valuable and has become a part of the economy and market. The harmonization of European rules is needed to realize the potential of the internal market, and to – almost as an afterthought – protect the fundamental rights of the individual.

The directive signals a clear understanding of the fact that the processing of personal data will increase, and that it will become more common, since “the progress made in information technology is making the processing and exchange of such data considerably easier” and it draws some of its legitimacy from this fact, again in par 5 “whereas the exchange of personal data between undertakings in different Member States is set to increase [...]” (par 4).

The directive clearly states that the need for new rules is connected to the development of new technologies and “the coordinated introduction of new telecommunications networks” (par 6).

The widening circle of actors inherent in the data protection directive is also directly referenced in the preamble. In par 12 the directive states: “the protection principles must apply to all processing of personal data by any person whose activities are governed by Community law; whereas there should be excluded the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, such as correspondence and the holding of records of addresses”.

This is intriguing, and seems to argue against my contention that the information society envisioned by these laws is one where information production is concentrated. But look at the exception again: “by a natural person in the exercise of activities which are exclusively personal or domestic, such as correspondence and the holding of records of addresses” – this holds the key, I think, to sustaining the argument that the society of the data protection directive is one where individuals are less important as information producers. Natural persons are thought of as corresponding or keeping address books. Quite understandably they are not the publishers of blogs, hosts of wikis or distributors of videos on video web sites – they are users, to return to our earlier analysis, and not creators.

Yet, this is an interesting paragraph. It is possible to interpret it as anticipating that everyone will process data, and to explicitly say that everyone should be responsible under the legal rules set out in the directive when they do so.

The state still has a privileged role, and “the processing of personal data that is necessary to safeguard the economic well-being of the State does not fall within the scope of this Directive where such processing relates to State security matters” (par 13). This is also a shift in thinking, since the original idea about data protection to a great extent was thinking about the balance of power between the state and the citizen. This balance, the legislator now tells us, will not be struck in
the general overarching legal instrument regulating privacy in the European Union, but elsewhere.

Then, in par 14, a direct reference to the emerging information society as a reason for the legislative response is given: “given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data”.

It is not impossible to see the data protection directive as a response to a society where the processing of personal data has become an economic interaction between different parties, drawing on the ideas about the information society from thinkers like Porat (1977) and Machlup (1962). Processing personal data is however still not a commonplace interaction engaged in by everyone by default. Specific rules for specific sectors of society are possible and anticipated (paragraphs 22 and 23)

One actor in particular is consciously left outside of the realm of protection. Paragraph 24 states clearly that “the legislation concerning the protection of legal persons with regard to the processing of data which concerns them is not affected by this Directive” – implying that the directive does not envision changes for companies and organizations as a part of the changes and “developments under way” that need to be handled in this specific format.

Paragraph 25 is useful as a catalogue of actors as well as a catalogue of interactions. It states that obligations are imposed “on persons, public authorities, enterprises, agencies or other bodies responsible for processing and the intera, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the right conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances”

This paragraph is in fact a good place to pause and reflect more on the set of actors and interactions that are inscribed in the directive. An attempt to extract from this paragraph some clues as to what model of the society is inscribed in the directive gives several interesting details.

The individual, here, is treated as a partner in the interactions concerning his or her personal data. The individual must be informed, have the right to consult and object to processing. Perhaps not a full partner, but still a partner. Where the old conception of processing personal data was one of pure exercise of governmental power (to simplify) the view of the directive is that the individual is an active actor in taking care of his or her personal data.
Another piece of evidence that shows that the legislators behind the directive had no idea how fragmented the Internet would actually become is the notion that personal data can be reconstructed from a multitude of sources. The directive notes (par 26) that “the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible”.

The main gist of this interpretative rule is that if there is a number of distributed pieces of information they are to be treated as personal data if they can be collected by “means likely reasonably to be used” and used to produce personal data. This raises a host of issues, not the least of which is the question of whether or not IP-addresses are personal data or not, a legal issue that has raised contention (but where at least the Swedish Data Inspection Board has ruled this to be the case)(Datainspektionen 2005).

What does this say about the directive's implicit model of society? Would the legislator have included a paragraph such as this if they had envisioned a society where the granularity of personal data was such that we could have tidbits from people in services like Twitter and where entries in age-old discussion groups coupled with entries in Wikis allows almost anyone to reconstruct vast personal profiles from a few hours with some of the most popular search tools? What is not personal data under this paragraph?

In the ideal type model of the information society this is less problematic: the number of information producers and distributors are fewer and the paragraph could make sense, but when the fragmenting becomes more severe, the idea that distributed tidbits of information could be personal data if they are possible to connect with other pieces of information is breathtakingly expansive and all-encompassing.

One might argue that this was intended. Search engines and other tools were envisaged and the legislators set out to make them impossible, but this seems less likely. And that the multitude of logs and other data that can be used to collect information was taken into account when formulating this paragraph seems likewise unlikely. The sheer enforcement costs that this would imply suggests that the view of an identity's cohesion that the legislator had was a view of a far less distributed identity. Here is evidence to suggest that the level of distribution of information was thought to be low to moderate at least. Otherwise the rule is hard to understand.
Paragraph 28 of the preamble sets out the basic framework under which processing is allowed and gives a few insights into what the directive implies about information quality and structure. It states that “any processing of personal data must be lawful and fair to the individuals concerned; whereas, in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and legitimate and must be determined at the time of collection of the data; whereas the purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified”

The quality requirements and the demand for accuracy are laudable but also seem to belong to a world were data quality can in some sense be guaranteed or revised much more easily than in a society where unstructured data from a multitude of producers is collected from a sea of channels. The idea that data should be deleted when used is also something that implies a different view of society, one where data is actually erased at all.

In some sense it is accurate to say that the default settings of the information society are open for discussion. It is possible to imagine that the data processing systems, the purpose of which is to “serve man”, can be made to delete and forget after our wishes.

The data subject, the individual, is an actor taken seriously. The main interaction inscribed in the directive is that of consent (par 30). Again this implies a society where individuals’ interactions involving personal data is structured and concentrated. The directive envisions a world where: “the processing of personal data must in addition be carried out with the consent of the data subject or be necessary for the conclusion or performance of a contract binding on the data subject”.

Processing is possible under other circumstances as well, such as “a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person, provided that the interests or the rights and freedoms of the data subject are not overriding” and there are also loop holes for commercial use of personal data stating that “in order to maintain a balance between the interests involved while guaranteeing effective competition, Member States may determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies; whereas Member States may similarly specify the conditions under which personal data may be disclosed to a third party for the purposes of marketing whether carried out commercially or by a charitable organization or by any other association or foundation, of a political nature for example, subject to the provisions allowing a data subject to object to the processing of data regarding him, at no cost and without having to state his reasons”, but the main interactive form in the directive is consent. In any schema or model of the world implied by
the directive the individual’s consent becomes a crucial interaction. In some cases – where the “data [...] are capable by their nature of infringing fundamental freedoms or privacy” the requirement is even explicit consent (p 33).

The directive also presupposes that society will retain clear demarcation lines for different information production sectors. It is perhaps here that there is the best evidence for the hypothesis that the directive presupposes few information producers. The directive tries, in the interest of the freedom of speech, to exempt journalistic activities from the scope of the directive, stating that “the processing of personal data for purposes of journalism or for purposes of literary of artistic expression, in particular in the audiovisual field, should qualify for exemption from the requirements of certain provisions of this Directive in so far as this is necessary to reconcile the fundamental rights of individuals with freedom of information and notably the right to receive and impart information, as guaranteed in particular in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms”

This rule may seem quaint in its naïve conception of the world as neatly divided into categories where journalistic and literary intent is clearly discernable, but a more charitable interpretation is that it is a way for the legislator to open up for case law determining where the boundaries should be drawn. Even so the idea that it will be easy to discern journalistic intent has collapsed under the avalanche of blogs emerging in the last few years.

As an interesting side note here one can examine the Swedish case of credit information provider Ratsit.se. This company provided free personal data about all Swedes, down to the taxes they paid and their crediting rating by relying on a “publisher’s certificate” readily available from the Swedish Radio and TV agency. These certificates were introduced as a way for journalists and literary artists to declare their “journalistic intent” and to thus be exempt from the directive, but since the agency has no rights to examine the merits of the applications it issues all applicants a certificate without fail. Ratsit.se could thus, during a number of months, freely distribute information that is otherwise heavily regulated without even informing the data subjects about the fact that the information about them was accessed.

The attempt at safe-guarding certain interests fails in the complexity of deciding who is and who is not playing a certain role in society. When this leads to public authorities resigning and allowing everybody to define their own roles the legislative compliance is reduced to very low levels.

The systemic thinking in the directive runs deep. In setting out rules for transparency and information the directive assumes that it is possible to ensure the fairness of processing by putting “the data subject [...] in a position to learn of the existence of a processing operation and, where data are collected from him” and to give him or her “accurate and full information, bearing in mind the
circumstances of the collection”. This idea again seems to rely on the assumption that data collection and processing is done in a structured, centralized and orderly fashion and that the collectors themselves actually know that they are collecting the data in question.

The implicit idea that data is processed in centralized systems is also evident in the requirements the directive puts on security, demanding that “appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing [...] these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected”

The idea that it is possible to make such an assessment suggests a high level of control. It seems to suggest a society where systems are clearly delineated with sharp boundaries and sharp system ownership. A mesh of systems and applications with mash-ups and collaborative web applications seem less open to these kinds of assessments or requirements.

The large systems still exist, of course, but they are not the only threats to privacy. This, again, is a good place to remind the reader that I do not think that all policy responses to an information society are failures and should be given up, but I think that they leave important issues unregulated and that they miss crucial problems. The hypothesis is that we need to adjust, not overthrow, the policy responses we have made in adapting to technological change.

I could go on and delve deeper into the directive, and exhibit more and more of the same ideas. From the analysis presented so far I hope that it is fairly evident that the scripts implied by the directive are scripts for the information society model.

The data protection directive is a legal response to technological change that is modeled on the idea of an information society where information is far more structured, information production more concentrated and distribution of information ordered and orchestrated. It is, in short, a policy response that is consistent with a policymaker that works with the information society model constructed in the previous section.

**Privacy Enhancing Technologies**

Emerging new technologies pose a challenge to privacy. It is even possible to argue that personal data is a recent innovation and that it has been brought into existence by the changes and innovations in technology and architecture. The idea of personal data can be seen as a direct conceptual product of the emerging surveillance and monitoring technologies. These technologies produce personal data, and in them we find inscribed the concept of privacy. Peter Blume (1997), researcher in legal informatics, observes that:
The idea of privacy – that a sphere of a person’s life is private – arises when the technologies that can be used to infringe private life are developed. [...] As indicated, technological developments lead to new methods of infringement.

This is nothing new. The relationship between privacy and technology is an old one and even the perhaps most well-known definition of privacy connects the emergence of new technologies with the need for a legal concept or even a right (Warren & Brandeis 1890):

Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right “to be let alone.”10 Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that “what is whispered in the closet shall be proclaimed from the house-tops.”

The case that Warren and Brandeis commented on was the direct consequence of the use of a technology that was new in 1890: photography. New technologies have always been a part of the production of personal data, and the reader need not go any further than simple positioning technology to find another good example.

The promise of delivering services to anyone, anywhere at any time is compelling and interesting. Many companies today work with position or location based wireless services such as Global Positioning System or triangulation, and positioning technology is rapidly becoming cheaper and cheaper to use to provide timely services. Many service providers today use position or location to add value to information or services delivered via wireless or mobile devices as a trivial component of their technology. But with the rise of these new technologies we suddenly face a host of new legal challenges to which we need new responses. The positioning technologies produce positions; turn our movements and situations into goods for trading. These positions are about us, and therefore they are – in the legal sense – personal data. But how do we treat them legally? Who owns a position? The subject in that position or the provider using technology to produce the position? These questions are not trivial, since they decide not only how our future privacy is shaped, they also decide what business models are possible and in the end they affect and change and interact with the possible technological solutions for position-based marketing, to take one example.18

The production of a new class of personal data thus creates a policy challenge. In the case of positioning technologies a partial answer to this legal challenge is found in another European directive, namely Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive

18 Again we encounter a dilemma not unlike that pointed to by Jessica Litman (2001) in her examinations of copyright (see the chapter on copyright). There is a similar “sleight of hand” at work here – simply extending old concepts to new technical realities.
on privacy and electronic communications). This directive contains an explicit response to the technological challenge in Article 9, where a basic consent rule is laid down requiring that data subjects consent to positioning.

But legislative responses are not the only possible responses to technological challenges. If technologies can be used for producing personal data and to commercialize them, it is equally possible to attempt to design technologies to protect personal data, and this is exactly what has been tried the last ten to fifteen years.

I will now turn to an analysis of some early thoughts on systems, business models and protection schemes to examine what ideas about society were inscribed in these. There are more modern technologies as well – but since I am trying to ascertain the model used for the early legal response to the information society they will be mentioned only cursorily. There are many technologies designed to protect individuals’ privacy on the Internet built partly as responses to applications that are designed for monitoring, and partly as applications that work pro-actively to protect the individual’s privacy. They all come with an inscribed vision of the society in which they will be deployed. These technologies usually go under the name Privacy Enhancing Technologies and they are good examples of architecture regulation. The study of privacy enhancing technologies is worthwhile for several reasons.

Firstly, the symbiotic systems where technology and law are employed to regulate issues are becoming more and more important in the emerging information society. The whole debate about architecture regulation and the way technology shapes society is more relevant now than perhaps ever before and privacy is perceived as an ever-more important question.

Secondly, privacy enhancing technologies as policy responses to the changing society are interesting and important. The technologies, and architectures, that are developed here must fulfil certain legal design requirements and this interplay is interesting to study. Privacy enhancing technologies are artifacts that exist in part as legal entities and in part as technological entities.

The main reason for us to engage in de-scripting privacy enhancing technologies is that they exemplify a specific and important observation about what policy making is like in the information society. In the information society policy making often turns into systems design or product development. The idea that societies can safeguard privacy by developing technological fixes, by creating architecture responses when taken to its extreme gives the end result is that policy making becomes product development: new business models, technologies and protocols are designed to create a policy response to a complex challenge of emerging technologies.
“Privacy enhancing technologies” (PETs) is, however, not a well-defined and neatly delimited concept. Legal informatics writer Herbert Burkert (1997 p 126) divides the concept into four subsets of conceptual models:

- Subject-oriented models that aim at preventing individual identification.
- Object-oriented models that aim at preventing objects to reveal data about where they come from, from whom and where data is destined.
- Transaction-oriented models that aim at eliminating all tracks of transactions without actually focusing on the objects of the transaction.
- System-oriented models that aim at implementing all of the above in an integrated environment.

Burkert’s typology partly focuses on the possibility of anonymizing different elements of identity in the online environment. There is another class of PETs that concentrate less on prevention and more on negotiated disclosure. Privacy can be enhanced even by negotiating a limited set of data to be collected, to take a simple example. This is part of the thinking behind another early standardisation attempt, P3P, which we will look closer at later.

Most privacy enhancing technologies are based on the idea that privacy depends on or should depend only on the identifying step, where a data set is connected to an individual. In fact, many behavioural patterns collected and compared may reveal the identity of an individual indirectly rather than by directly identifying someone. The early responses to the information society thought that citizens or users did indeed come to the net with anonymity, and that they needed tools to retain that anonymity. To identify users was the threat posed by technology, and then everyone would know what they had done. The inscription here, in this idea of privacy enhancing technologies, then is that users live in a society with data sets that can be connected with identity in an act of identification that is immediate and absolute. This requires both that information is structured and that it is produced in large sets by a limited number of producers.

There is some evidence to suggest an evolution in the notion of privacy enhancing technologies: from encryption via anonymisation to negotiation platforms. Some even argue that PETs must be and can be built into the Internet itself (May 2001). The opposite has also been discussed – with different key escrow solutions outruling privacy when the interests of society seem more pressing (Denning 2001).

Again, both May and Denning suggest a view of society as an architecture open to design and regulation, an architecture with centralised power, gatekeepers and control. The reader finds in May and Denning the same kind of architectural hope, the hope that technology will allow itself to be designed to prevent our negotiation of legal rights to collapse. This hope rests on the model of the information society as a society where information is structured, produced in limited amounts by few producers and distributed under control.
Another possible definition/innovative response to the growing risks is the idea of constructing distinct and protected on-line pseudonyms and to use these for protecting anonymity. This also assumes the notion of an identity to be protected, a hidden identity that can be unlocked with a “true name” to use the term coined by science fiction writer Vernor Vinge in his eponymous novel from the 1980:s. Vinge, in this novel, depicts a future society where much of the power of society is being exercised in an online world, by pseudonymous actors that sometimes oppose the authorities. The key to subduing an individual is to be able to connect the pseudonym to a “true name”, a physical, real identity. It is first then that the state can start to exercise its traditional monopoly of violence. Vinge’s dystopia is illustrative for many reasons, but perhaps most because it deviates fairly much from the actual development of Internet use.

What about pseudonymity, then? How does it relate to privacy enhancing technologies? The problem of pseudonymity is indeed surfacing as a promising field for legal sociology (Lucock and Yeo 2006). There are probably more pseudonyms in existence today than ever before in the history of mankind (witness the nine million players of World of Warcraft, most of which use pseudonyms, or the pseudonymity actually built into Second Life, where the last name is pseudonymous by default – an example of architecture regulation with high local impact), but there is also an enormous amount of information published, distributed and processed where the individual has chosen to identify him or herself. From blogs over videos and photo albums openly available the exhibitionism of netizens is more palpable than the power of being able to dismantle someone’s pseudonymity. We share our true names happily for a few extra visits to our blog or web site.

I know that I should be reprimanded for making this general statement from the vantage point of a Scandinavian democracy. It is true that in dictatorships maintaining pseudonymity might entail the difference between life and death. I do not mean to belittle this horrid fact, but I still want to point out that in democracies the development of the Internet has deviated from Vinge’s dystopian visions of the future.

The very idea of privacy enhancing technologies as a policy response shows that the early visions of technology responses were based on visions of a society where the objective of protecting privacy was achieved by stopping individuals from connecting structured information about an individual, from a limited amount of information producers, with his or her identity. The key to this was thought to be in finding technologies to control distribution and dissemination of personal data. The overall model emerging here is the information society model.

The technological foundations for privacy enhancing technologies vary. One of the more well-known solutions that aim at anonymizing the parties in communication is onion routing and here the basic idea is to establish a number of layers that cooperate to generate anonymity on the level where the actual messages are
transported, on router-level (Goldschlag, Reed and Syverson 1999). *Onion routing* uses dedicated encryption servers that send messages between themselves in a way that makes it very hard (if yet not impossible) to find out where the messages come from originally. Another example of a similar solution is the *Crowds project* (Reiter and Rubin 1999). This technology is used to shift the messages through a large amount of intermediary points in the network. The point being to make it possible not to identify the individual, but only the “crowd” from which a message comes: “An innovative way to become an invisible user is simply to get lost in the crowd. After all, anonymity loves company” (Reiter and Rubin 1999). Each user becomes a part of the crowd, and this collective effort at creating an anonymising crowd is an interesting product both socially and legally.

Similar technology is used in the more and more popular Tor-project, hosted by the Electronic Frontier Foundation. The Tor-project aims at creating a usable and simple technology to implement onion routing and protect users against traffic analysis. The technology is freely available and believed to be promising (Electronic Frontier Foundation Tor Project 2007).

When we examine privacy enhancing technologies as a policy response it becomes startlingly likely that policy makers and others seemed to believe that much if not all of the problems and challenges associated with privacy in the information society could be handled with what can only be described as a kind of business development attitude, or a product development scheme.

Product development is elevated to a policy making process and all kinds of different actors mix in designing more or less plausible policy responses to technological change. When John Hagel and Marc Singer launch the idea of the *infomediary* in their book *Net Worth* (1999) the idea is a curious mix of business advice, policy advice and technological design blueprint. The idea was quickly adopted by the market and as a direct result company PrivaSeek launched a product called PersonaXpress19 that let the user store information and define under what conditions it could be used. It is instructive to examine what the news reported about the product at the time(Cox 1999):

"PrivaSeek describes itself as a "consumer-driven information intermediary, or "infomediary," that benefits a consumer by giving them control over when, how and who uses their data. PrivaSeek's software "helps consumers control global marketer's use of their personal data," while providing timesaving form filling functions and value-added brokerage services for negotiating discounts with marketers. "PrivaSeek Persona is a consumer-provided profile; PrivaSeek Valet is a personal information assistant and PrivaSeek Vault is a secure online safety deposit box for storing personal profiles and privacy settings"

The idea that personal data can be assembled into a “persona” is interesting and the degree of cohesion and control that PrivaSeek thought it could offer over the

19 See http://wwwpersona.com
Persona can be quickly de-scribed to show an information society model operating behind the product rhetoric. But the perhaps most intriguing thing about the news item quoted is that it mixes policy issues so clearly with business logic. Here the goals of protecting personal data are enmeshed in business hype.

Some companies even became engaged policy players with perhaps less of a profit motive than a policy agenda. The chief example of this was Zero Knowledge Systems, a company that developed one of the first large scale anonymizing networks and called it “Freedom”. The mesh of policy and business, of technology and politics in the company format was symptomatic of the belief that the information society presented a unique opportunity to re-architecture society to preserve, change or open up certain values.

Technically this was not a terribly complicated solution. *Anonymous Internet Proxy* (AIP) servers interacted through so-called *wormholes* with websites beyond the Freedom Network, and the actual user was hidden within the cloud of anonymity created by routing requests and other traffic randomly sent and received through the network. The weakness in this system was that it needed a fair number of users to establish a secure cloud.

What is interesting about the Freedom-network from the perspective of this study is that it gives such a perfect example of the assumption that it is possible to control distribution channels and the user’s choice of communication networks. The Freedom Network is an information society concept, in a sense, since it builds on this idea of control.

The idea of privacy enhancing technologies led to a development where policy makers and entrepreneurs joined forces with political actors, but the end result was deeply disappointing to those who believed that society could be re-architected. Zero Knowledge Systems has changed its name to RadialPoint and no longer offers privacy enhancing technologies as its main services or even as a significant component in its services. PrivaSeek no longer exists. The Anonymizer still exists, but the company is not a major participant in the policy process. The proxy-server surfing solution it offered was simple enough and did not require massive alignment, but it did not change the fact that most users do not seem to care about their privacy (Cranor, Reagle och Ackerman 2000).

The idea that policy making could be reduced to product development proved faulty and what we instead see today is that the development of privacy enhancing technologies like Tor is much more like “modding”, the practice of writing short snippets or modules to modify pre-existing software (mostly games)(Camargo 2006). Today we see privacy enhancing technologies enter the stage as modules in the popular browser Firefox, to take one example. The grand schemes for overhauling the market and directing a major change in consumer behaviour are gone. Architecture responses to privacy challenges are no longer framed in policy

63
making as product development, but in the far more fragmented and diversified process of modding.

Another of the principal approaches to privacy enhancing technologies was to implement protocols for negotiating the exchange of personal data. The World Wide Web Consortium (W3C) developed a platform specifically dedicated to exchanging information on information practices: **Platform for Privacy Preferences** (P3P). This suggested standard won support from many different actors in the field, and it is a prime example of attempted architecture regulation in the field of privacy.

The platform offers a model of how different actors can exchange information about the collection and use of personal data. The platform has often been said to be an important part of understanding privacy protection by technical means (Cranor 1999) and it presents a good example of how good privacy enhancing technologies were expected to look.

P3P is, however, not really a technical solution or a software package. It would perhaps be more correct to describe P3P as a suggested model protocol for how the information flows regarding electronic tracks should be exchanged. In reference to architecture, P3P is a blueprint where the actual implementation can vary. The goal of P3P was to establish a high-transparency solution for users and to have this solution implemented in popular technologies such as web browsers. P3P was “developed to as an industry standard providing a simple, automated way for users to gain more control over the use of personal information on Web sites they visit. At its most basic level, P3P is a standardized set of multiple-choice questions, covering all the major aspects of a Web site's privacy policies. Taken together, they present a clear snapshot of how a site handles personal information about its users. P3P-enabled Web sites make this information available in a standard, machine-readable format. P3P enabled browsers can "read" this snapshot automatically and compare it to the consumer’s own set of privacy preferences. P3P enhances user control by putting privacy policies where users can find them, in a form users can understand, and, most importantly, enables users to act on what they see” according to the P3P web site.

The idea behind this was that if users know what information is actually collected about them they at least have fair warning. It might, it was thought, often be enough to explain what information will be collected, how it will be used and who will have access to this information. This idea presupposes structured interaction between users and website owners, and even more – it seems to presuppose that the use case the designers have in mind is a commercial transaction.

Today large volumes of information are indeed collected in e-commerce, but this is hardly the only form of interaction that threatens privacy through massive data collection in the sense that P3P implies. To imagine that a web site can have **one** privacy policy is to imagine at least a certain level of centralised information.
production. Collaboratively produced web sites like wikis can of course have centralized privacy policies, but they will be much harder to enforce and control.

So how well did P3P work? Did it work at all? There were several problems with P3P, and it is instructive to examine them. It is an old wisdom that if one wants to boil a frog it is bad practice to boil the water first and then drop the frog in it. The frog will then make every effort at getting out of the water, and it will escape the intended gourmet dinner. If one instead puts the frog into a pot of cold water and boils that water slowly, the frog will not notice the increases in temperature, since they are continuous and slow, and it will be boiled without noticing. That, at least, is what the old wisdom tells us. The adage "boiling frogs" might not be an international one, but it illustrates a well known problem in decision science: people have a tendency to notice large changes that occur more than they recognise small changes that accumulate continuously. This is relevant in the analysis of cost structures on the Internet as well, and brings us some insight into the problems facing a legislative response like P3P. When people lose their privacy they do it cookie by cookie, personal data item by personal data item. That process is a clear-cut boiling frog process. Users wake up one day naked in the eye of the world and that is pretty much it. They leak personal data and there is a point after which they lose the ability to maintain a private sphere. Users may regain it if they become reclusives, but living in the world is being subject to a kind of privacy entropy, where users become ever-more transparent.

P3P is an immediate shift, from privacy dissipating to privacy being thrown out in the open, being discussed, debated, negotiated over and this is an important reason for why P3P has not had greater impact. The continuous de-regulation of privacy cannot be met with discrete and instantaneous attempts at architecture regulation. The only way this could work is if there is an external catastrophe. Dag Wiese Schartum notes (Schartum 2001):

My assumption is that data protection will be of low importance to most of the population. This is because many people will be insensitive to data protection infringements and it will only creep into their lives as a ‘background noise’ that they will respond to only when it is combined with other incidents that capture their attention.

Privacy infringements in a society where information is unstructured, information producers many and diverse, distribution uncontrolled and the information growth unchecked simply disappear into the “background noise”. The din of noise takes the drama out of slow erosion process. P3P could not overcome this as is evidenced by the overall extremely low adoption rates of P3P20 (E-soft n.d.):

20 The statistics is scarce, imprecise and it has been unsuccessful work trying to find any more recent data on P3P-adoption.
The work on P3P has been discontinued, and even if the protocol is implemented in some popular browsers and does seem to have greater penetration in some categories, especially e-commerce sites, it does not seem to gain any particular speed (Egelman, Faith Cranor and Chowdury 2006). The concept of policy making as protocol design, the idea that society could set out a protocol and then leave to the users to safe-guard their privacy was simply rejected by users living in a society where information negotiation would consume too much time, efforts and resources, and where centralized protocol adoption never was an option. And still attempts at developing policy in protocol format continue. One of the heirs of the P3P-standard is a project symptomatically called The Policy Aware Web (The Policy Aware Web Project 2007).

In summary, then: the privacy enhancing technologies that were developed in the 1990s were well within the information society model. Assumptions of control, over the production, distribution and structure of personal information dominate in the de-scriptions of the technologies. The value function of personal information was assumed to be that of any other goods, as evidenced by the idea of infomediaries. The de-scription of privacy enhancing technologies validate the model or set of heuristics constructed under the first step in the research strategy.

**The information society directive**

In directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society, the European legislator has tried to respond to the challenges inherent in the emergence of new information and communication technologies.

That this is indeed envisioned as a response to the emerging information society is evident already from the title of the directive and it is an interesting piece of legislation to examine and de-script, since it offers many insights into how the information society was envisaged by the legislator at the time it was drafted.
The information society directive is more recent than the data protection directive, but in part this is an illusion, since the directive is based on the 1996 WIPO agreements on copyright (see par 15 in the pre-amble). Both pieces of legislation studied here are thus from the middle of the 1990:s and the inscribed vision of the information society found in them is from that time.

I have already found significant evidence in the data protection directive to suggest that the society that this legislation is a response to is thought to be one with a few important information producers, controlled information distribution and structured information. The working hypothesis suggests that we should find the same in the information society directive.

The background of the directive is found in paragraph 2 of the preamble:

(2) The European Council, meeting at Corfu on 24 and 25 June 1994, stressed the need to create a general and flexible legal framework at Community level in order to foster the development of the information society in Europe. This requires, inter alia, the existence of an internal market for new products and services. Important Community legislation to ensure such a regulatory framework is already in place or its adoption is well under way. Copyright and related rights play an important role in this context as they protect and stimulate the development and marketing of new products and services and the creation and exploitation of their creative content.

The rhetoric is interesting: the suggestion here is that the framework is not only a response to the changing environment, but an actual tool in bringing this environment into being. The directive is needed to “foster the development of the information society in Europe”. This makes our de-scription of the directive even pertinent, since this means that the directive contains a normative view on how the information society should work.

The basic motivation of the directive and the legislation is economic and the hope is that harmonizing the law on these issues will “foster substantial investment in creativity and innovation, including network infrastructure, and lead in turn to growth and increased competitiveness of European industry, both in the area of content provision and information technology and more generally across a wide range of industrial and cultural sectors. This will safeguard employment and encourage new job creation.”

The perspective here is industrial. What is needed is fostering investment and making sure that the European industry provides content and technology. The first actor the de-scriptor encounters is this “industry” loosely defined as one of the prime movers in bringing about the information society. Nowhere to be found is the multitudes of collaborating Wikipedia-enthusiasts or the bloggers happily typing their nights away. They are not the envisioned industry, but rather the intended recipients of the content provided by this industry.
Another actor we see in this paragraph is the famous “content provider”. This concept returns in many policy texts and it is almost never defined. What is a content provider? Is it some intermediary between the creator and the consumer? Is it the commercial providers of copyrighted goods?

It is possible to argue that that the directive is targeted at a vision of society where information production is fairly centralized. This suspicion is strengthened by the next paragraph (par 5), which discusses the expected changes brought about by technology. The paragraph starts out by claiming that “[t]echnological development has multiplied and diversified the vectors for creation, production and exploitation.” But both creation and production are then ignored and the paragraph continues: “While no new concepts for the protection of intellectual property are needed, the current law on copyright and related rights should be adapted and supplemented to respond adequately to economic realities such as new forms of exploitation.” It is the exploitation, the interaction between the content providers and the consumers that needs to be dealt with. We clearly see that the changes in creation and production methods envisioned by for example Yochai Benkler (2006) are not the subject of this piece of legislation. That we are on the brink of a new method of social production is nowhere to be discerned in the directive.

And this becomes even more clear in the next paragraph (p 6), where the reader meets the technological development as a threat: “without harmonisation at Community level, legislative activities at national level which have already been initiated in a number of Member States in order to respond to the technological challenges might result in significant differences in protection and thereby in restrictions on the free movement of services and products incorporating, or based on, intellectual property, leading to a refragmentation of the internal market and legislative inconsistency.”

The technological challenges will force states to increase protection and the products – again the industrial perspective – based on intellectual property will be harder to market and sell with “legal consistency”. The challenges envisioned here are challenges that will necessitate new forms of protection, not challenges that will enable individuals to create and consume more information than ever.

This may seem a trite remark – of course the legislator concentrates on the economic aspects of protection and the trade related aspects of a lack of harmonization – what else could the legislator actually do? There is nothing else the legislator should do, one may even argue, since the overall societal benefit and cost should be the focus of the legislator.

But therein lies a problem. If the overall cost and benefit effects of technological challenges is the focus and responsibility of the legislators there should be, here, a different line of reasoning if the society envisioned was one where creators were everywhere to be found, blogging, collaborating on wikis and sharing information.
If this was the society envisaged the question should be how we weigh the advantages of quick and accurate information allocation in a society against the needs for protection. There are even writers who argue that there may be significant societal benefits to weaken protection if this implies that information is utilized more efficiently for the greater good of the society (Shavell 2004).

This is a line of reasoning that is nowhere to be found in the directive, and this in itself presents evidence that the society the legislators have in mind is one where information is produced not by everyone, but by “content providers” in a “European industry”.

One of the following paragraphs gives us a valuable clue to what actors are inscribed in the directive. The paragraph states that (p 9):

> [a]ny harmonisation of copyright and related rights must take as a basis a high level of protection, since such rights are crucial to intellectual creation. Their protection helps to ensure the maintenance and development of creativity in the interests of authors, performers, producers, consumers, culture, industry and the public at large. Intellectual property has therefore been recognised as an integral part of property.

This is a portal statement, giving much away about the actors implied by the legislation. They are all uniformly motivated by economic incentives and they seek economic remuneration for their creation. They need to be well-protected and their creativity is maintained by the legal protection offered.

This is a view, again, consistent with a kind of creation that needs investments to come about. The protection, the legislator implies, is needed as a kind of protection for the investor. He or she needs to know that they will be able to get the expected return on investment to dare create. The point is further developed in the following paragraph (par 10) which states that:

> “[i]f authors or performers are to continue their creative and artistic work, they have to receive an appropriate reward for the use of their work, as must producers in order to be able to finance this work. The investment required to produce products such as phonograms, films or multimedia products, and services such as “on-demand” services, is considerable. Adequate legal protection of intellectual property rights is necessary in order to guarantee the availability of such a reward and provide the opportunity for satisfactory returns on this investment.

Here information production is a sector in the industry, not a wide-spread practice among everyone. The role of the _amateur_ is non-existent and creation needs to be financed.

Paragraph 11 goes on in the same manner, stating that “[a] rigorous, effective system for the protection of copyright and related rights is one of the main ways of ensuring that European cultural creativity and production receive the necessary resources and of safeguarding the independence and dignity of artistic creators.
and performers.” Note the reference to dignity, which is revealing. Artists are somehow dignified, they are a category apart. Creation is confined to a smaller set of individuals and this set needs to be protected, encouraged and financed.

In par 12 the directive mentions the cultural importance of copyright, without developing the notion further. It is assumed as self-evident that copyright ensures cultural growth and the counter-argument of Lessig (2001) and others, that too tight an application of copyright law may instead hamper creativity and innovation, is not even addressed.²¹

But all is not well. New technologies have entered the stage and they dissolve the control that is needed to protect the artistic set. In fact, the directive states, there is a need not only for legal protection, but for technical responses to the technical developments: “[a] common search for, and consistent application at European level of, technical measures to protect works and other subject-matter and to provide the necessary information on rights are essential insofar as the ultimate aim of these measures is to give effect to the principles and guarantees laid down in law.”

The reader learns more about the interactions envisioned in paragraph 23. This paragraph notes that there is a need to harmonise the author’s right of communication to the public. The interaction here is one where there is an author and a public, and this is an established model from copyright law, but since it remains here the directive endorses it, and reaffirms its belief in the form of creation that is implied by differentiating author and public.

It is easily realized that this is a view that is hardly consistent with collaborative creation of works or with the distributed and parallel creation implied by many modern creative projects. The image of an author communicating with the public reveals itself here as a strong influence, even though it is possible to argue that it should be thought of as an anachronous relic of another time, surviving in only the expected information society. The author makes the work available and this is an exclusive right (par 25):

[i]t should be made clear that all rightholders recognised by this Directive should have an exclusive right to make available to the public copyright works or any other subject-matter by way of interactive on-demand transmissions. Such interactive on-demand transmissions are characterised by the fact that members of the public may access them from a place and at a time individually chosen by them.

Again the model implied is hardly one where co-creation and collaboration permeate the society envisaged in the directive.

²¹ That it is not addressed is chronologically obvious, but the argument was made before Lessig and existed at the time of the drafting of the directive.
Another actor, always present in the directive, is the network and internet provider. These actors are exempt from liability and the directive clearly states that “[t]he mere provision of physical facilities for enabling or making a communication does not in itself amount to communication within the meaning of this Directive.” Again this gives the reader a substantive clue to what the society the legislators were expecting looked like. The legislators were consciously trying to avoid placing the responsibility for upholding copyright on the infrastructure providers, but they saw these two actors or functions as important components in the information society.

The directive also sets out some interactions – specifically those that are technically necessary for communication to persist – as exempt from the directive (par 33): “[t]he exclusive right of reproduction should be subject to an exception to allow certain acts of temporary reproduction, which are transient or incidental reproductions, forming an integral and essential part of a technological process and carried out for the sole purpose of enabling either efficient transmission in a network between third parties by an intermediary, or a lawful use of a work or other subject-matter to be made.” But it is important that these reproductions never have any value: “[t]he acts of reproduction concerned should have no separate economic value on their own.”

In paragraph 31 the reader finally meets with the actual consumers of the created works, and they are – not surprisingly - termed users:

[a] fair balance of rights and interests between the different categories of rightholders, as well as between the different categories of rightholders and users of protected subject-matter must be safeguarded. The existing exceptions and limitations to the rights as set out by the Member States have to be reassessed in the light of the new electronic environment.

These users are introduced after the rightholders – the balance between the rightholders is the first item of consideration, the balance of rights between the users and the rightholders (how could there be any such balance of rights, when one party is actually called the “rightholders” one is tempted to ask) is mentioned as an afterthought.

Finally, in arguing that the directive is a response to an information society where information is structured, production centralized (or industrialized as in the case of this directive) and distribution controlled it is illuminating to look closer at the introduction of legal protection of technologies for rights management in the directive.

---

22 The old quip about only drug takers and computer owners are called users is not completely inapplicable here: reducing citizens to users in the copyright narrative implies that their role is consuming culture rather than co-creating it.
The directive seems almost to echo the hope that the answer to the machine is in the machine in stating that “[t]echnological development will allow rightholders to make use of technological measures designed to prevent or restrict acts not authorised by the rightholders of any copyright, rights related to copyright or the sui generis right in databases.” (par 47).

But the time between the WIPO agreements and the directive has not seen the great introduction of copyright management technologies that was expected, and the legislator cautiously assumes that this is due to the fact that it is easy to circumvent these technologies. The answer to the answer to the machine was also in the machine:

> [t]he danger, however, exists that illegal activities might be carried out in order to enable or facilitate the circumvention of the technical protection provided by these measures. In order to avoid fragmented legal approaches that could potentially hinder the functioning of the internal market, there is a need to provide for harmonised legal protection against circumvention of effective technological measures and against provision of devices and products or services to this effect.

The new technological protection schemes need legal protection. The idea here is that it is quite possible to “effectively restrict acts not authorized by the rightholders of any copyright” (p 48) implying great faith in the amount of control over distribution of information in society. It will be possible, the directive continues, to “ensure a secure environment for the provision of interactive on-demand services, in such a way that members of the public may access works or other subject-matter from a place and at a time individually chosen by them.”

The model implied here seems to be one of a fragmented internet with secure environments, the systems perspective is strong and the belief in secure technologies is evident. That the society implied here is one with systems and control is further supported by the next paragraph (p 54):

> [i]mportant progress has been made in the international standardisation of technical systems of identification of works and protected subject-matter in digital format. In an increasingly networked environment, differences between technological measures could lead to an incompatibility of systems within the Community. Compatibility and interoperability of the different systems should be encouraged. It would be highly desirable to encourage the development of global systems.

The information society will be, the directive proclaims, a society managed and governed with global systems. It is hard to find a clearer formulation of the ideal type model of the information society: one where information is structured, information production centralized and distribution controlled – *globally*.

That information will be well-structured is alluded to in the next paragraph:
Technological development will facilitate the distribution of works, notably on networks, and this will entail the need for rightholders to identify better the work or other subject-matter, the author or any other rightholder, and to provide information about the terms and conditions of use of the work or other subject-matter in order to render easier the management of rights attached to them. Rightholders should be encouraged to use markings indicating, in addition to the information referred to above, inter alia their authorisation when putting works or other subject-matter on networks.

Again the set of actors is interesting to note: the directive is inscribed with “rightholders” and they “put” works on networks. This is the image the directive projects, these are the scripts inherent in it. And this is also clear in the threat model that is anticipated in the directive. The threat to this ordered, system-centric, global and controlled environment is “third parties”: “[i]n the digital environment, in particular, the services of intermediaries may increasingly be used by third parties for infringing activities.” But the threat is not perceived as great, and the responsibility for taking care of this minor nuisance is placed squarely on the shoulders of the intermediaries: “[i]n many cases such intermediaries are best placed to bring such infringing activities to an end.” But the development since the directive was put in place has showed that this is no slim task.

In uncovering the set of heuristics in reading the directive, the evidence of description suggests that the view of information production, structure and distribution is indeed one that is consistent with the ideal type model of the information society. Furthermore the focus on the value of information seems to suggest that information is indeed thought to become more valuable the more there is – and that it should be protected.

**Electronic copyright management systems**

In looking for architecture regulation to de-script it became obvious that it would be useful to use the early copy protection mechanisms designed for the Internet. They show, even more clearly than the DRMs of today, that the architecture regulative response was modeled on the information society model. I did an early study of these systems (Lundblad, The Answer to the Machine... 1998) and will draw examples from this study and use these to show how the system design and results indeed can be traced back to the information society model.

But there is another good reason for choosing the early electronic copyright management systems as an object for studying policy making as well. Much as privacy enhancing technologies integrated policy making in what mostly resembled product development, the electronic copyright management systems attempted to reduce policy making to systems development. The underlying rhetoric in much of the materials was based on the presumption that if the systems were designed well, then the challenges posed by the emerging technologies could be handled. The balance between copyright and privacy, the question of fair use and the question of copyright’s role in society were all treated as design problems rather than anything else.
One of the largest and most imperial electronic copyright management systems projects was the IMPRIMATUR-project (The acronym stands for Intellectual Multimedia Property Rights Model And Terminology for Universal Reference). The project is a natural starting point in de-scripting the copyright management systems since it sets itself such a gigantic task: to resolve all negotiations between actors in the copyright field and devise solutions for all problems to come. The first phase of this almost slightly megalomaniacal project was focused on consensus building. The goal was building decisive and comprehensible consensus around all questions pertaining to information trade (Cordis 1996):

In the emerging Information Society there are many conflicting interests between rights-owners, information providers and end-users with respect to copyright and intellectual property rights (IPRs) protection. The IMPRIMATUR consortium is working to reconcile these differences stimulating public debate aimed at developing a consensus in this field. This work is of particular importance for the "information industries" whose business lies in the creation, trading and use of information. The project operates primarily through a publicly accessible Web site, which facilitates a two-way exchange of information between the information industry and IPR owners on IPR management issues. Eventually IMPRIMATUR will devise and recommend processes to protect and trade all types of intellectual property, whereby rights are respected while user needs are met.

The last sentence is noteworthy. It signals the intent in the clearest possible terms: to devise and recommend process to protect and trade all types of intellectual property, whereby rights are respected while the user needs are met. This would be no small feat, but IMPRIMATUR was far from alone in trying to build broad consensus at the time. In fact, almost all electronic copyright management systems at the time started out with the presumption that their work was to agree on what systems would be designed for information commerce.

The policy makers/system designers also thought that they were doing the information markets a favour. Without their efforts there would be no sharing of information on the net, no information providers would ever allow their materials to be put on line. The main idea here was that the power to provide information was securely in the hands of a few information producers who had to be convinced of the benefits in digitization. One example of this attitude is found in the Talisman-project, another one of the classical ECMS-projects(Talisman 1999):

TALISMAN aims to provide European Union service providers with a standard copyright mechanism to protect their digital products against large scale commercial piracy and illegal copying. With the increasing availability of digitally stored information and the development of new multimedia services, security questions are becoming ever more urgent. The acceptance of new services depends on whether suitable techniques for the protection of the information providers’ interests are available.

One problem that has not found a solution yet is the one of how to realize copyright protection for digitally stored data.
Note that the de-scription implies that new service providers would have to deem technologies “suitable” before they joined the fray. The last sentence again is almost ironic. The one problem remaining to be solved back in 1999 still remains unsolved and today the consensus is slowly inching towards the view that protection is not necessary (see the section on digital rights management).

An even more architectural solution was offered by another project, FIRM. FIRM is also an acronym and stands for Framework for Interoperable Rights Management. The objective is to define a service layer on top of existing Internet protocols. Here the architectural responses envisioned were at the infrastructure level, implying great faith in the ability to re-design the system.

The authors themselves describe their project thus (Röscheisen and Winograd 1997):

FIRM is based on the assumption that the rights management landscape will continue to be heterogeneous, with each of the systems making different design trade-offs to best accommodate the constraints from a specific area of application. FIRM therefore defines a two-level standard, consisting both of a generic specification that defines a domain-independent common rights language object model, and a standard format that allows anyone to contribute media-specific or domain-specific rights definitions.

The FIRM projects worked with contracting solutions and has introduced the notion of an e-person (or epers):

An epers is a software agent that is the persistent digital representation of (a role of) a person with a structured request interface. When acting online, users are identified by a (possibly opaque) handle to their e-person, allowing any communication partners to get back this structured representation and negotiate access conditions in detail—only in some cases involving the user (e.g. when certain interactions are not covered by the default preferences that a user set up for his or her e-person).

One and the same person can have more than one epers. A Unix account can be seen as a current form of a limited version of an e-person.

Winograd and Röscheisens project focused on a special form of digital contracts called “commpacts”. The idea of compacts is expressed in the report as well:

Commpact (also: smart contract): A commpact is the computational object that is the digital representation of an agreement between two or more parties, be it a legal contract or a more lightweight "communication pact" (e.g. one related to privacy). Commpacts are "smart contracts" in that they have a structured (FIRM) interface, code that implements behavior, state (e.g. the validity status, the number of times a right was exercised, etc.), and a set of textual descriptions. In other words, compacts represent a mixture of informal textual descriptions and implementation code (where the fact that both have the same semantics is the responsibility of the designer of the underlying commpact form). Commpacts are effectively a network-centric form of an authorization monitor. They authorize actions, enforce prerequisites ("student
status required"), and provide a way to live up to obligations (e.g. initiate a payment transfer when fulfilling an obligation). In other words, the piece of text by which we generally know legal contracts is just the result of one of the many methods that can be called on conmpact objects - but there are also others, including negotiation methods (e.g. ‘terminate’), structural messages (‘get me the set of promise objects’), and, last but not least, authorization interactions (‘exercise this right’).

The most interesting part of Winograds and Röscheisens project is that it tried to establish a rights management layer that will able to operate together with several different CMS’s. The idea seems to be to build the “Rights Management Layer” into the very fabric of the Internet. In this way the approach is clearly different from that of traditional ECMSs that try to build systems within the framework of existing networks.

Such a system clearly presupposes a high degree of control, and especially over distribution networks. Uniformly adding one layer to a network is no small task, and structuring all agreements in conmpacts presupposes a well-structured information environment.

Technology like this presupposes order, control and an environment in which there is considerable structure. Consumers remain consumers and enter into “conmpacts” with the information producers. This is an information society project following the information society model closely.

That the copyright management systems would succeed was at the time taken as a given. One author, in analysing the different ECMS-projects, writes (Cornish 1996):

"The age of the Electronic Copyright Management system is dawning. For owners it is a dream come true. They can obtain payment and control copying of virtually all electronic documents. For some librarians and users it is a nightmare because it enables access to information to be controlled totally by the copyright owner, thus ensuring the total monopoly of intellectual property. For the practising information worker it is reality that is going to happen. Just how and in which mode we do not yet know but it is here to stay. The important thing is to make certain that one person’s dream does not become another person’s nightmare."

This was, at the time, probably only a slight exaggeration. The general feeling at the time was that the large systems being designed would dominate the information industry and enable information commerce. The metaphors are telling. The AMIDE - Advanced Multimedia Information Dissemination Environment – project states that the intention is to build environments that work as shopping centres:

"AMIDE environments may be seen as large shopping centres with all the enabling infrastructure, where small and medium enterprises will be free to promote and operate a variety of information shops, where individual talents will be able to offer their services in open areas and where the consumers will be able to window, shop, to test, try-out, buy and take away information goods."
This idea, that one could build shopping centers in cyberspace, directly uses the metaphors of real architecture to show how a policy response could be designed. And I think it is fair to claim that this was not seen as overconfidence in the ability of architecture to regulate behaviour. This was seen as a serious response to the envisioned information society model, where producers were assumed to be few, distribution controlled and structure well-defined.

The legal discourse at the time echoed the assumption that these systems would become dominant. The discussions centered on issues such as how we can guarantee that certain rights are built in, or what happens if we circumvent the system to protect, for example, “our right to read anonymously” (J. Cohen 1996).

The systems thinking that produced IMPRIMATUR and other similar systems is based on a model of society where all the salient points in the information society model are present. Controlled distribution (note the idea of bilateral agreements, as if systems were states), structured information and centralised information production as well as consumption are all components in the de-scriptions used to reverse engineer the heuristics of the designers.

The idea that consensus building is important also implies an interesting view of the state of affairs: that it is up to the industries to decide what technological change entails. This very non-schumpeterian view was quickly challenged by the emerging technologies and the system designers were replaced by actors of different kinds involved in what has been called “tinkering” or bricolage by Claudio Ciborra (Ciborra 2002). Ciborra’s book The Labyrinths of Information: Challenging the Wisdom of Systems (2002) actually points to a lot of the problems faced by Electronic Copyright Management Systems. The systems that Ciborra studied in the book were strategic information systems, but the claims of these systems – to offer competitive advantage in a global economy, are actually humble compared to the claims of some of the ECMS-projects. Ciborra’s observation that bricolage has become an important part of technology use/design is an observation that creates a dissonance in the heuristics. The bricoleur is not at home in the information society. When the attempts at “global systems” for “content providers” breaks down, policy making as system design breaks down with it and the bricoleur enters the stage.

If ECMS focused on large system models, we have today seen a reverse to a different kind of technology. This technology sometimes goes under the name of Digital Rights Management (DRM). Digital Rights Management is not radically different from ECMS, but some changes have occurred.

The first is a shift in the objective. Where the ECMS was a solution designed to establish a controlled environment, a control architecture, for the flow and consumption of information, the DRM-architecture relies more on trying to control only the content. Where the content is is only important at the moment of consumption.
The second is that being able to recognise the content through watermarking or other means seems to have lost some of its importance. It might be surmised that today authors realise that their content is either encrypted and protected or open and impossible to control.

The third is that the payment systems are now not necessarily connected to the DRM-systems. The development of electronic cash of different kinds is not essential for DRM to work, since different existing solutions can be used for paying for content.

The fourth is that DRM-systems often are more technical and less organisational. This is an important point that is closely related to the first point made, but it deserves to be mentioned separately, since the actual effect is that systems are now integrated into a wealth of different organisational structures.

The research on digital rights management exploded during the early 21st century and there was a huge amount of work being put in from the industry to be able to establish these new technologies in the digital environment. Today, however, several record companies are ditching their efforts to launch DRMs (BBC 2007, Fiveash 2007). One reason for this is the extremely difficult work required in aligning all the actors to make these systems work. Gillespie (2007) offers an illustrative review of the Secure Digital Music Initiative that shows how hard it is to implement controlling technologies with the support of both legal reforms and architectural regulation. There is simply no way to establish the levels of control needed to successfully launch DRMs.

The idea of an Electronic Copyright Management System is an idea that is aligned with our ideal type model of the information society. The idea of a system for selling and maintaining works presupposes a highly structured information set. The notion of a large system for distribution presupposes a high level of control over distribution networks and practices.

Even if the systems were thought to enable multiple creators and the information production in theory at least was distributed and de-centralised, ECMSs were responses based on the concept of the information society. They were systems embodying the hope that everything could be designed and agreed on in consensus; that the new environment would be a shopping center and a new layer could be invented for information commerce.

In a sense it is perhaps this that is most evident: the ECMSs embody the idea that policy makers could design markets and their technology, and build a framework for commerce, rather than live through the creative destruction so convincingly illustrated by for example Joseph Schumpeter in his works. It was a dream of control.

Conclusions
The tracing of the information society model, using both legislation and architecture regulation, suggests that the model can be de-scripted out of both the policy responses to copyright and privacy. The second step in the research strategy – validating the model or set of heuristics arrived at through the policy discourse analysis – leads to the conclusion that the information society model is implicitly, at least, at work in the European policy making processes in the 1990s.
Copyright, is, even for the skilled lawyer, a tricky subject. It is probably wise, in the light of this fact, to review a few of the basics before we start discussing legal reforms or architecture regulation. Copyright is the common term denoting a section of what is usually called intellectual property rights (IPRs). IPR also covers important legal constructions such as patents, pattern rights and trademarks.

Copyright has deep roots in legal history, and dates back well into the 15th century. It is a legal innovation that is closely related to respect for the author and the author's rights.

The rationale behind copyright is multifaceted. Some argue that the main reason for inventing copyright was to encourage creativity and to incentivize artists to create. Another theory is that copyright is a moral right encoded in legislation and that the right to an intellectual work is much the same as that of the carpenter to his table. A third theory simply states that copyright is a protection for an investment that cannot be regained if the inventor does not get some time and exclusivity to get a return on his or her investment.

The economic argument – which I will refer to as the incentive argument - is perhaps the simplest: if I know as an author that anyone can steal my works without paying for them, I will be less inclined to invest something valuable of my own – time, money or other resources – in them. If, on the other hand, I know that my work is protected, then I will invest and create in the knowledge that I can benefit from these investments in my work.

This is also balanced by a theory of openness in which it is stated that to ensure that works of significant value are shared with society, a monopoly right can be constructed that allows the innovator to exploit the work under a certain time and then share it with society, thus adding to the overall good of society.
In our day and age copyright has been developed to also cover pure investment protection reasons. Anyone who invests in creating a significant database resource, for example, is under this theory entitled to protection merely because the investment would not otherwise be made, and the value of the product could not be contributed to the market, without this protection. This line of argumentation motivates the sui generis protection for databases, for example.

**International and National Law**

There is a considerable international element in IPR-law. The World Intellectual Property Organisation (WIPO) is the originator of much of the legislation that has been nationally implemented today.

WIPO is the international organisation of cooperation in the copyright sector and manages the different international treaties that govern much of the IPR-legislation in the world today. The treaties relevant to copyright are:

- Berne Convention for the Protection of Literary and Artistic Works
- Brussels Convention Relating to the Distribution of Programme-Carrying Signals Transmitted by Satellite
- Convention for the Protection of Producers of Phonograms Against Unauthorized Duplication of Their Phonograms
- Rome Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations
- Trademark Law Treaty (TLT)
- WIPO Copyright Treaty (WCT)
- WIPO Performances and Phonograms Treaty (WPPT)

The different conventions handle different aspects of copyright, and the most recent is the WCT, that was finalized in December 1996 after intense discussions in the WIPO. The WCT was intended partly to adapt copyright to the changing technological environment, and has now been transposed to both European and American Law.

In Europe the transposition is found in the *Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society*, and the United States the implementation is found in the *Digital Millennium Copyright Act*.

**The scope of Copyright**

Copyright is really several different rights integrated into one. Usually copyright scholars speak about two basic forms of rights: the economic rights and the moral rights. We will introduce them briefly below.

**Economic rights**
The economic rights are the rights that most people usually think about when they think about copyright. Somewhat simplified one might say that these rights are rights of reproductions and performance.

The rights of reproduction are formulated in the Berne convention and it is useful to look closer at the wording in order to get a sense of how these rights have been constructed:

(1) Authors of literary and artistic works protected by this Convention shall have the exclusive right of authorizing the reproduction of these works, in any manner or form.

(2) It shall be a matter for legislation in the countries of the Union to permit the reproduction of such works in certain special cases, provided that such reproduction does not conflict with a normal exploitation of the work and does not unreasonably prejudice the legitimate interests of the author.

(3) Any sound or visual recording shall be considered as a reproduction for the purposes of this Convention.

The rights of performance are also defined and presented in the convention. The definition gives a sense about the wide range of rights awarded in speaking about reproduction:

(1) Authors of dramatic, dramatico-musical and musical works shall enjoy the exclusive right of authorizing:

(i) the public performance of their works, including such public performance by any means or process;

(ii) any communication to the public of the performance of their works.

(2) Authors of dramatic or dramatico-musical works shall enjoy, during the full term of their rights in the original works, the same rights with respect to translations thereof.

Both these rights are fundamental in the understanding of copyright on a basic level. These are the rights that copyright discussions often deal with, and the underpinnings of a multi-billion dollar industry encompassing the music, film and software industry around the world.

Moral rights

The other set of rights usually associated with copyright are the so-called moral rights, encompassing firstly the right to be designated as the author of a work, and secondly the right not to have the work manipulated or changed in way that is detrimental to the reputation of the author: The moral rights are formulated thus in the Berne Convention:

(1) Independently of the author's economic rights, and even after the transfer of the said rights, the author shall have the right to claim authorship of the
work and to object to any distortion, mutilation or other modification of, or other derogatory action in relation to, the said work, which would be prejudicial to his honor or reputation.

(2) The rights granted to the author in accordance with the preceding paragraph shall, after his death, be maintained, at least until the expiry of the economic rights, and shall be exercisable by the persons or institutions authorized by the legislation of the country where protection is claimed. However, those countries whose legislation, at the moment of their ratification of or accession to this Act, does not provide for the protection after the death of the author of all the rights set out in the preceding paragraph may provide that some of these rights may, after his death, cease to be maintained.

(3) The means of redress for safeguarding the rights granted by this Article shall be governed by the legislation of the country where protection is claimed.

These rights are more seldomly actually enforced and under examination in the public debate. The bulk of copyright issues are concerned with issues of economic rights.

Copyright, then, is often understood to consist of economic and moral rights to an intellectual work. Copyright is a complex legal subject, rich with intricate problems and tricky questions, and as such it has been heavily debated.

The policy discussions about copyright have been heated and the attempt to find policy measures that respond to the challenges to the old copyright regime is still, I will maintain, unsuccessful.

**Weaknesses and failures**

The third step in the research strategy is perhaps both the most complicated and the easiest. The task set out for this third step is to examine possible counter-examples, weaknesses, friction and dissonances in the information society model. The purpose of this is to find the boundaries of the model, where it breaks down.

Testing for boundary conditions is rational in cases where the model has failed. This necessitates a discussion of whether or not the policy responses based on the information society model have indeed failed.

I have argued that the result of the preceding analysis has been to show that the policy responses to the technological challenges examined – both the legal reforms and attempts at architecture regulation – are in essence modeled on the information society.

That only means that the responses are consistent with the model of the information society re-constructed out of different policy documents, and is perhaps not really a great surprise. It would have been more surprising to find large dissonances between what legislators say that they will do and the actual policy responses, but the reverse is not strange.
**What it does imply, however, is that the phenomena studied are examples of policy responses based on the ideal type model of the information society and that there should be some failures associated with them if I am right in assuming that the information society model is failing policy makers.**

Is there, then, any evidence of these failures to support that contention? I will argue that there is, but remember that I have not argued that the responses are complete failures, but merely that they fail to some degree because they start out from an erroneous model of society or set of heuristics.

Examining both data protection and copyright for failures is instructive.

**Copyright in crisis**

That copyright has been one of the most problematic areas in the intersection of new technologies and law is not surprising to anyone who has followed the public debate the last thirty years or so. Consider the following quotation (Allan, et al. 1978(1968)):

> The new technology has produced a copying machine which is threatening the economic interests of copyright holders.

What technology would you guess they are referring to? What machine? The answer is as entertaining as it is informative:

> This new technology is the photocopier – a device which allows individuals to make single copies of printed works economically.

Technological advances have perpetually been perceived as a threat to the copyright holders, and their interests in different ways.

In much-publicized court cases such as Napster, mp3.com, Kazaa and Grokster the music industry has fought to preserve what it perceives as its rights. Simultaneously, with changes in intellectual property rights law and the development of viable alternative regulatory regimes, such as that presented by the open source movement or creative commons, current copyright and its institutions has been subjected to heavy criticism.

The intensity of the debate is mirrored in the number of works that have been published in this area. As we previously noted Lawrence Lessig is one of the most well-known writers on this subject with his books *Free Culture* and *The Future of Ideas*. Lessig has also been involved in litigation, particularly one very important court case, the so-called Eldred-case, and his engagement in this case reflects many of the key issues that have come to characterise this debate.

Copyright was one of the early policy issues that the first generation cybervisionaries came to study, as it seemed obvious that so much was going to
change. John Perry Barlow writes, in a 1994 article that now belongs in the canon of the copyright debate (Barlow, The Economy of Ideas 1994):

Throughout the time I’ve been groping around cyberspace, an immense, unsolved conundrum has remain at the root of nearly every legal, ethical, governmental, and social vexation to be found in the Virtual World. I refer to the problem of digitized property. The enigma is this: If our property can be infinitely reproduced and instantaneously distributed all over the planet without cost, without our knowledge, without its even leaving our possession, how can we protect it? How are we going to get paid for the work we do with our minds?

Barlow’s conundrum quickly became the entire industry’s conundrum. Initially the idea that someone would download music files over the Internet may have looked ridiculous to some observers, but it quickly became an undeniable factor in the copyright markets. The music industry reacted violently, and often with law suits. A large number of cases have since been tried over different aspects of online and digital music distribution. The subjects vary.

- MP3-players. In one case the Recording Industry Association of America (RIAA) claimed that it should be illegal to sell mp3-players, since the format was used for playing illegally copied music. They lost this case, on the basis that it resembled a court case much like it about video players. In that case the Court found that it should not be possible to stop a technology that had legal uses as well as illegal as soon as the legal uses actually were not only theoretical.
- Napster. RIAA sued Napster for making available a network in which a large number of illegally reproduced files were distributed. The Napster case was won, in a sense, by the music industry (Carroll 2002).
- Kazaa. The cases have involved both forcing ISPs to give out identities of file-sharers and the legality of the Kazaa system itself (Ginsburg and Ricketson 2006).
- MP3.com The website made music of 80 000 CDs available over the net for registered users admonishing them that they could only listen to and download music they owned. The court found that it did not need to enter into discussion on whether or not it was legal for users to download digital reproductions of music that the users owned; they stated instead that MP3.com had violated the right of reproduction and thus found for the music industry (United States District Court for The Southern District of New York 2000).
- Grokster. The music industry argued that those that design technology that can be used to infringe on copyright should be held responsible along with those who actually infringe. The high-profile case was decided in favour of the music industry, but only because the defendants had – according to the court – encouraged piracy in
their marketing materials (Beckerman-Rodau 2006, Landes and Lichtman 2003).

The large numbers of court cases have also been accompanied by a loud public debate, with both nuanced and academic participation, as well as more aggressive rhetoric. The digital copyright issues have become the centrepiece of much of the on-going legal debate about the Internet and IPR. The debate has been fierce and interesting.

The writings of Lawrence Lessig have become the centerpiece of much of the debate on copyright. With his many books on the subject and his thorough research, he has for many, become the icon of copyright skepticism.23

Lessig outlines a programme for reforming copyright in The Future of Ideas (2002). The main components of this programme are severely reduced terms of protection, and the development of neutral platforms. In this proposal, he specifically emphasizes what he calls the rebuilding of the creative commons. This rebuilding would be started with different incentives to donate copyrighted material to the public domain and developing the creative commons actively as well as protecting the public domain from new attempts at re-introducing regulation.

Lessig developed this idea together with a number of other copyright scholars and the Creative Commons24 is hugely successful. In summary, Lessig’s position is (simplified) that it is necessary to limit copyright to ensure creativity, and that the architecture of the Internet is an important part of the set of conditions required for creativity to exist.

Another of the important voices in the copyright debate is James Boyle. In his early work Shamans, Software and Spleens: Law and the Construction of the Information Society (1996) he notes that copyright will be one of the crucial issues in the construction of the information society. Interestingly, Boyle bases much of his research on the idea that we are indeed moving into an information society, a view he notes is entirely uncontroversial in the legal community, again showing how entrenched this idea or model has become (Boyle, A Politics of Intellectual Property: Environmentalism for the Net? 1997):

> Everyone says that we are moving to an information age. Everyone says that the ownership and control of information is one of the most important forms of power in contemporary society. These ideas are so well-accepted, such cliches,

---

23 It is important to distinguish between copyright skepticism and copyright abolitionism. The first is a question about how the rights and functions inherent in copyright should be designed for our times, the second the belief that there is no need for copyright whatsoever.

24 See Creative Commons website at [http://www.creativecommons.org](http://www.creativecommons.org) (visited 2007-12-31) for more on this intriguing attempt at license reform where legislative reform has proven hard.
Boyle was also one of the first legal writers to argue that we need to examine the rhetoric of the copyright debate to be able to understand it better. He even argued that copyright is in dire need of a reformulated discussion.

Boyle suggests re-inventing the public domain:

Similarly, I claimed the "public domain" is disappearing, both conceptually and literally, in an IP system built around the interests of the current stakeholders and the notion of the original author, around an over-deterministic practice of economic analysis and around a “free speech” community that is under-sensitized to the dangers of private censorship. In one very real sense, the environmental movement invented the environment so that farmers, consumers, hunters and birdwatchers could all discover themselves as environmentalists. Perhaps we need to invent the public domain in order to call into being the coalition that might protect it.

Boyle’s call for a movement and a new concept to center around are both evidence of a growing worry about the alignment of copyright with society at large.

Another important writer in the area of digital copyright is Jessica Litman. In her 2001 work Digital Copyright (2001) she analyses the evolution of copyright in the information society and offers a number of insightful examples of problems and what she calls the “copyright wars”.

The main contribution in Litman’s work, in my opinion, is however the discussion on choosing metaphors that features in her book. In this analysis Litman highlights that copyright has moved from being a “bargain between authors and the public” to “copyright as property” (Litman, 2001, p. 81). In this shift much changes, Litman writes, and it is important to realize that this shift is not merely a shift in metaphors, but also a change in the regulatory conceptual framework that is being developed around copyright. Copyright is only property in a metaphorical sense, and this she feels is important to emphasize. Litman notes (Litman 2001, 86):

My argument, here, is that this evolution in metaphors conceals an immense sleight of hand. We as a society never actually sat down and discussed in policy terms whether, now that we had grown from a copyright-importing nation to a copyright-exporting nation, we wanted to recreate copyright as a more expansive sort of control. Instead, by changing metaphors, we somehow got snookered into believing that copyright had always been intended to offer content owners extensive control, only, before now, we didn’t have the means to enforce it.

This is an important point. Litman shows that it is not self-evident how we extend copyright to new domains, technologies, media channels and other innovations. A part of the policy crisis can be directly attributed to the fact that we as a society
have assumed that there is no difference between the creative landscapes created by the new and old technologies. This is a “sleight of hand” that is causing the tension in a regulatory framework constructed for another time, another society and another technology.

The way copyright has been reformed has also given rise to debate. One example is the new protective measures introduced for technical attempts at regulation. Pamela Samuelson was one of the first writers to note and discuss the important issue of technical protection for copyright, and she immediately saw that it would be connected with several problems. Samuelson is also one of the “new environmentalists” (Samuelson 2001, 99):

> It will sound strange perhaps to put it this way, but our information ecology will be disrupted if intellectual property rights get too strong. So far Greenpeace hasn’t taken up the cause, but maybe it should.

Samuelson has concentrated some of her work on understanding and exploring the ramifications of technical protection measures or copyright management information (CMI). Already in 1996 she noted that these systems could offer problems (Samuelson 1996):

> My own concerns about CMI didn’t arise until after I heard a prominent publisher speak about the idea of making CMI “smart,” that is, able to report information about the user back to the publisher from whom the document came. Such systems would seem to have a strong potential to be invasive of user privacy[...]

Samuelson has since written a large number of articles exploring the consequences of technical measures. She shows that when copyright is amended to address technical change it is often in a defensive way that fails to balance existing, legitimate interests.

David Bollier discusses and extends the reasoning about a creative commons and the public domain in Silent Theft: The Private Plunder of Our Common Wealth (Routledge 2002). His line of argument highlights a tension between private and public in the copyright policy debates.

Julie Cohen is a prolific and important writer on the dilemmas of copyright. In her much-quoted “The Right to Read Anonymously: A Closer Look at “Copyright Management” in Cyberspace” she argues that technical protection for copyrighted information may well come into conflict with the first amendment, since the freedom of speech must entail also the freedom to form one’s opinions freely (J. Cohen 1996). Cohen, much as Samuelson, argues that copyright interests are unsatisfactorily balanced against other interests.

---

25 Copyright Management Information – a variant of copy protection technologies.
Even the economic arguments for copyright have been challenged. David Vaver has written a work on the expansion and growth of copyright in which he suggests an alternative economic view of copyright (Vaver 2000):

> If intellectual property was seen as a form of subsidy – a willingness by society at large to provide economic benefits to one sector in return for the prospect of larger benefits for all – then few would question the need to keep intellectual property under constant review to ensure that the scheme was working well.

In the same context David Rice has stressed that the idea of copyright is really a young one, based on economics that may no longer apply (Rice 2001, 128):

> 'Intellectual Property' is in fact a relatively new usage in US and even in other law. Much of what we speak of under the rubric has its roots in unfair competition, not property, law concepts and rules. Implicit in the increasing 'propertization' of intangible interests is the sacrifice of the far greater flexibility and adaptability of liability rules in response to changing conditions and needs in favour of securing greater immediate security through adoption of the relatively more brittle property rights and rules.

What all these examples show is that copyright is under strain. It is a prime example of a policy area where the negotiations have broken down.

The debate on copyright is becoming more and more heated. The examples I have given are just a few from a wide and growing body of literature discussing the future and effects of intellectual property in general and copyright in particular. That the debate is connected with the challenge posed by new emerging technologies is hard to doubt: the rise of the computer and the Internet is cited in all these works as the inciting factor for the need to revisit the design of copyright.

*All this goes to substantiate the claim I made in the beginning: that there is a sense of crisis in copyright meriting the choice of copyright policy as a subject to examine closer.*

**Copyright policy failures**

Copyright policy has failed on several different levels. As indicative evidence of this we can take the fact that the European Union continues to legislate on copyright in several new pieces of legislation – one might argue if the information society directive had really enabled the copyright industry and the content providers for the information society nothing further should be needed.26

There are, of course, some counter arguments to the view that copyright policy has failed. The growth of the creative industries and the content sector in the European economy has exploded. This was the explicit intent of the directive. It is of course possible to point to the fact that using this observation is committing a post hoc

---

26 This is, however, somewhat naïve. The counter-argument would be that law should adapt (albeit slower) to changing social conditions *all the time.*
ergo propter hoc-error, in assuming that the directive’s coming before the creative boom proves anything about the causality of the situation, and I agree with this analysis. There is no proof that the directive led to the creative explosion, and considering that much of the creativity is regulated by a license that explicitly exempts many of the protections afforded by the directive (Creative Commons-licenses), the causality can be called into question.

In one area, at least, the directive has proven to be a huge failure, and that is in its protection of technical measures and if the purpose of the law was to quench illegal copying, it has failed. But the failure means little, since a booming content industry is now growing despite (or, as some say because of) rampant copying.

There is another failure that needs to be taken into account, here, I think and that is the legitimacy of the copyright system. The legal reforms in the information society directive have been directly responsible for the rise of a counter-copyright movement. The legitimacy of copyright has been severely hurt by this, and this is a failure as well. One example of how the legitimacy of copyright has suffered from the disconnect between the legal reforms directive and the society users perceive themselves to live in is how the file-sharing debates have affected policy makers. In the recent 2006 Swedish elections the question of file-sharing music actually became a hot policy issue and both of the leaders of the largest parties asserted that they thought it unnecessary to hunt down teenagers sharing music on the Internet (Jerräng 2006). Four of the seven parties in the Swedish parliament were for decriminalizing file-sharing, and this was bi-partisan, with the both right and the left block, the Social Democrats, the Moderates, the Greens and the Center Party in favour and the Left Party, The People’s Party and the Christian Democrats against.

The debate that led up to this was initiated by the previous year’s implementation of the information society directive, and so is directly related to the directive.

Have technical protection measures like ECMSs or DRMs worked? That depends on what measures policymakers apply in judging if they have achieved their goal. There are several different possible goals. It is useful to examine them:

(1) The technical measures succeed if they completely stop illegal copying.

This is the strongest possible measure, and if this indeed was the goal of the technical protection mechanisms they have failed miserably. Security expert Bruce Schneier explains why (Schneier 2000):

Against the skilled user, no countermeasure works. [...]Because breaking the countermeasure can have som much value, building a system that is secure against these attackers is futile. And even worse, most systems need to be secure against the smartest attacker. If one person hacks Quake (or Intertrust or Disappearing Inc.), he can write a point-and-click software tool that anyone
This observation must be modified however: some measures work against some users and a second goal could be this:

(2) The technical measures succeed if they are sufficiently hard to circumvent for the regular user.

Some writers seem to think that such partial protection is enough. If a copyright protection scheme can only be cracked by 3 percent of the Internet user population, then that is enough to claim that the technology is successful. This was maybe true in a world in which distribution could be controlled, in the world of the Electronic Copyright Management Systems. In that world it was sufficient to rely on the fact that a lot of people did not know how one could circumvent the technical measures. If a few computer professionals could circumvent the protection then that would only be a marginal problem. This is a terrible goal in a world where the Internet plays a dominating role. In this world –as Schneier points out – things follow the crack once/copy everywhere rule. If this indeed was the then goal the technical measures have succeeded, but their success is limited. It is control under the consent of the controlled. But there is some truth here: small protection measures can achieve acceptable levels of legitimate use.

A related goal could be this:

(3) Technical measures succeed if they raise the awareness about copying being prohibited.

This is probably one of the most positive consequences of the technical measures implemented today for the copyright holder who wants to find some successes. Region codes for DVD-players for example are useless as anything else than an awareness raising activity. Most people know that there are region-coding solutions, and most people ignore them. But they know they are ignoring them. This is an effect that seems less desirable when taking into account that the users knowing that they ignore laws actually lessens the legitimacy of the coding-technology and the legislation protecting that same technology. But if this is the purpose, some of the technical measures have surely succeeded.

Overall, the goal of implementing technical measures has of course been to protect copyrighted material. If we take this to be the basic purpose to be fulfilled by the technical protection schemes, there are several reasons for calling the technology a tentative failure.

The number of files exchanged now in the file-sharing networks are more than before the laws protecting technical measures were introduced. The flow of copyrighted material, the number of users and the volume of traffic is at least
unaffected if not larger than before the laws were introduced, making this a policy failure.

Several large actors in the music industry are leaving DRMs behind as a solution of the past (Fiveash, 2007). The reason is that technical protection is extremely difficult to accomplish and achieve, especially where information structure is dissolving, information production is growing quickly and the number of producers are exploding. If control over networks and distribution also is dwindling the task becomes almost insurmountable.

In examining both the information society directive and the large electronic copyright management systems, as well as the digital rights management technologies, I have tried to show that the responses are indeed modeled on an ideal type model of the information society, and I have pointed to failures that have resulted from this as well.

These failures are important and they are accompanied by some fundamental challenges to the way policy makers have been thinking about copyright. In the following sections I will present two different examples of such challenges and discuss what they may mean.

**Creativity - the incentive argument revisited**

In information society models, copyright is consistently hailed as a great enabler and a pillar of the market, and the reason for this is that it is needed to *incentivize people to create* (remember the Bangemann-report and the information society directive with their “content providers”). Creativity is viewed as something that must be incentivized. Examining this argument offers an opportunity to examine the information production model. How and why is information produced? And is this consistent with the information society model?

The argument that we need to foster creativity by strengthening and respecting copyright is sometimes referred to as the *incentive argument for copyright*. I will argue here that today we are forced to give up the incentive argument for copyright in all but its simplest forms, and that we need to re-examine the basic motivations for copyright, since the modes of creativity have changed.

The incentive argument takes different forms, but in its more extreme formulation the argument suggests that without intellectual property rights we would not get music, literature or any other intellectual creation. If our protection of intellectual property becomes too weak, we cannot have an information society – because no one will provide the “content” of this society.

Now, copyright can also be defended on other grounds. We could argue that the property rights assigned in copyright are moral in nature and accrue as a consequence of the artists work effort. Or we could argue that copyright is, as many other forms of intellectual property, an investment protection measure from
the legislator. But what if we bracket all these arguments for copyright and assume a society with abundant free creation – what arguments for copyright would then hold, if any? The incentive argument in favour of copyright is really rather weak. It begs the question of what kind of copyright encourages what kind of creativity and it seems to be defeated by the creativity seen every day. I will examine it more closely below in a number of versions, and see how they fail.

In her 2007 article *Creativity and Culture in Copyright Theory* Julie Cohen points to an interesting observation (Cohen, 2007, pp. 1151-1152):

Creativity is universally agreed to be a good that copyright law should seek to promote, yet copyright scholarship and policymaking have proceeded largely on the basis of assumptions about what it actually is. When asked to discuss the source of their inspiration, individual artists describe a process that is intrinsically ineffable.

Rights theorists of all varieties have generally subscribed to this understanding, describing creativity in terms of an individual liberty whose form remains largely unspecified. Economic theorists of copyright work from the opposite end of the creative process, seeking to divine the optimal rules for promoting creativity by measuring its marketable byproducts. But these theorists offer no particular reason to think that marketable byproducts are either an appropriate proxy or an effective stimulus for creativity (as opposed to production), and more typically refuse to engage the question. The upshot is that the more we talk about creativity, the more it disappears from view.

The old heuristics of the information society model assumed a limited circle of creative artists and an information industry that would have to be encouraged to disseminate their information on the internet. This is clearly an erroneous model of society today. Today creativity is everywhere: blogs, music websites, wikis and a multitude of other websites share openly and freely content of different kinds. The content providers of the old information society model turns out to be us.

The simplest form of the incentive argument simply states that without copyright law, *artists will not create*. This argument looks so silly that it is almost self-defeating but it is still worth taking as a starting point, since it is not so silly as one might think.

Firstly, the argument says nothing about getting paid. What is said is that policy makers need to create incentives to make sure that people create. But it does not specify that the incentives must be the economic rights in copyright, the incentives might as well be the moral rights.

If construed as an argument for the moral rights it suddenly does not sound so silly. If policymakers remove the legal rules that ensure that creators have attribution rights as the author of a work it seems reasonable to assume that even those that are completely uninterested in money may feel disinclined to

---

27 Rights to have the work attributed to them – a part of the moral rights complex.
create. If nobody knows I created a work I might feel less strongly about creating it, at least if I create as a means of personal expression.

This is at least a reasonable assumption, albeit one that is probably not universal. People have different incentives for creating. Some simply like the process, like writing or painting, and do so not because of any legal rules or regulations. Others think more about creativity as an instrumental activity – a way to increase their fame or wealth.

This said, I think it is fair to agree to the proposition that the existence of a copyright regime – with some kind of moral and economic rights – may positively influence the rate of creativity in a society. But this is far cry from agreeing to the idea that society would not get any creativity if it eliminated copyright.

Today creativity is everywhere. Works are created at a hectic pace, everywhere and by everyone. There are few people that earn enormous amounts of money on copyrighted works, but there is a lot of creativity. Sure, some of these may create in the hope that they will one day be able to cash in on their works, but the majority must be assumed to create because they like it. It is an activity that is pleasurable and interesting. It offers a way to realize yourself and explore intellectual challenges. The moral rights may have some importance for creators, but in many cases the economic rights are totally unimportant.

It is interesting to examine the opposite of the incentive argument since it shows that copyright regimes are not automatically tools of repression: if somebody argued that any copyright law will decrease the level of creativity in a society it would be quite hard to take this seriously. Toying with the idea of a legal reform that eliminated the economic rights and left the moral rights, would this then lead to less creativity than if we had no copyright law what-so-ever?

I do not think so, but it is an open question and reducing the argument to be about whether or not any copyright law will increase creativity allows efficiently escaping the current debate about the current copyright regime. (I do believe that a version of the incentive argument focused on the moral rights may actually survive in a naturally creative society).

The next argument is the first step on a slippery slope that contains some of the murkiest thinking in the philosophy of copyright law. In this formulation the incentive argument claims that it is only if society incentivizes in assigning economic and moral rights that it entices the right creators to create the right kinds of works.

The thought behind this formulation of the incentive argument is perhaps that the most worthwhile creativity in society must be unlocked and encouraged from reluctant creators. Why these people would be reluctant to create if they create
interesting works is hard to understand. How policymakers know that a certain set of incentives will lead to creativity with certain properties is another conundrum.

As a matter of fact policymakers rarely if ever discuss the incentive argument from this angle. Agreeing that copyright law fosters creativity policy makers should be discussing intensively what kind of copyright law fosters what kind of creativity – but this discussion is hard to find. And the answers are equally hard to give.

Are there copyright laws that foster multi-faceted creativity? It is possible to imagine copyright laws that encouraged diversity in creativity. Such laws could be designed to protect only that which is sufficiently non-mainstream and to do so with prizes and awards instead of with a system that requires a licensing regime. Are there copyright laws that foster creativity in areas where we see the creation of works declining or inching towards extinction? Copyright that encourages creativity in certain languages, social groups or other selective protective regimes are possible as well.

I would not necessarily encourage any of the suggested copyright regimes, but the questions asked here show that the incentive argument is actually hollow: it is an empty argument in that it begs the question of what copyright law, what incentive, fosters what creativity. In a naturally creative environment the idea of some sets of creativity being “right” is moot – creativity is everywhere. Works are already there, out there, everywhere.

The preceding argument was the first gingerly dance down the slippery slope of the intellectual quagmire found in the quality version of the incentive argument. Here the argument states that if society does not incentivize economically it will only get low-quality creativity. There are several possible responses to this version of the argument, and it does not even hold in the information society.

Firstly, quality is subjective. One man’s quality is another man’s rubbish. Copyright is granted equally to rubbish and art for this very reason. That a work is protected by copyright says nothing about its quality.

Secondly, the relationship between investment and quality is impossible to prove. It is possible however to argue that certain works would not have been made if it were not for the existence of copyright. Works that are extremely expensive and commercially viable would not have been produced if there was no way to get a return on investment – but this is not an argument for copyright as an incentive for creativity, this is an argument for copyright as investment protection. The difference is subtle: in the first case the argument states that copyright fosters creativity, in the second case the argument merely states that copyright fosters creative production of works that are expensive and commercially viable. The end result if policymakers accept copyright-as-investment may actually be less creativity overall.
Thirdly, creativity has become much more collaborative during the last few years. This in turn has led to a situation where works are always works-in-progress. Quality is ensured through sustained creativity – but this sustained creativity with many participating creators is actually hampered by the current copyright law, since manipulating works is an act requiring consent from the original creator.

To think that the legislator has the ability to design copyright not only to incentivize creativity, but also that it automatically fosters a qualitative and optimal creativity is simply wrong.

It is far more interesting to examine the idea that incentivizing is morally right. This argument states that copyright fosters creativity and is a small token of thanks to the people who engage in creativity. Sure, they would do so anyway, but this is no reason not to thank them is it? Your friends do things for you that they would surely do, at least for a while, even if you neglected them. You reciprocate because you want to signal that you are a good guy.

It is possible to see copyright as reciprocation for creativity rather than anything else. It becomes a second order incentive, an incentive to create again if you will since creativity is appreciated. Copyright signals that creativity is an activity that is important, strengthens your social status and offers you an elevated position in society.

This version of the incentive argument fails in a society with the excessive creativity evidenced today because nobody knows that you have created something. When everybody creates, it is hardly possible to gain status by being a creator. And creation builds on “the shoulders of giants”, enabling us to ask an entirely new moral question: what should the creator give back?

When everybody creates works, and works become collaborative efforts that are distributed in large networks, the idea that society needs to incentivize somebody to create becomes slightly ridiculous for a large set of cases. There are still, of course, situations and creators that would defend it, but its validity is reduced.

The old idea, that policymakers needed to ‘foster’ or ‘enable’ or ‘encourage’ creativity, and that they would be addressing a caste of creators seems dead wrong. Creativity is everywhere. It is the default setting. The policy challenges and metaphors need to change. People create songs, web pages, blogs, videos and other materials. They contribute to Wikipedia and chat rooms all over the web. Citizens live in a sea of creative havoc and in the age of “user-generated content”.

The information society model breaks down in societies where everyone creates. The need for incentives, the possibility of controlling information production and distribution all break down and fail. The model cannot answer why society would need copyright at all or how it should be designed. It offers no answers or new metaphors since it was not crafted to handle an extremely creative society, where
- to reconnect with the theoretical foundations – the autonomy of small-scale technologies leads to a wealth of creative works.

Following Nagle (2007), Boyle (1997) and others, policy makers should perhaps actually view copyright as an environmental problem, and assert that copyrights should be assigned much as any other rights that destroy common resources. Perhaps the emission rights trading systems being developed today could provide guidance: societies could allocate a certain, limited sets of copyrights to different nations and then let the highest bidder copyright their works, but keep the strong disincentive to do so for the majority, this protecting the creative space. The reasoning behind this metaphor would be that the set of possible works is practically finite (if infinite in theory) and every copyrighted work destroys a corona of possible works around it, variations and similar works that will not be created or at least not disseminated for fear of being sued by rightholders. Copyrights would be viewed as pollution or destruction of our common creative space.

To allocate copyrights as emission rights would almost be in line with the reasoning found in Pasquale (2007) where excessive creativity is seen as a negative externality, but Pasquale’s argument for thinking about noise in environmental terms is slightly different. Pasquale writes that the information producers need to take responsibility for the fact that they are contributing to an excess of information in our society. One possible policy measure, he suggests, is to widen the copyright exemptions for those that work hard to reduce the information in society, the categorizers: search engines, wikis and other filters. These service providers should be exempt from copyright and what they do, indexing and organizing information, should be seen to fall under the heading of “fair use”. In the European Union that would amount to inserting a special exemption in copyright law for indexing, categorizing or organizing information for accessibility and usability – since the European legislator has left no opening for extending “fair use” in case law.

Another intriguing question, that cannot be answered by the information society model is what will happen when the enormous boom in information produced the last ten years or so becomes public domain. Society lives, in a sense, with a ticking creative bomb. The public domain will grow quickly in about a 100 years, when the current copyrighted information loses its legal protection. What will happen then to creativity and art in our society?

Some may argue that the term of protection will be extended, some may even fear that there will be infinite terms of protection, but what if there actually is a public domain boom in about a hundred years? How will the public domain handle the enormous amount of information then flowing into it? Again the information society model has no answer.
Artists are being forced, one could argue, on relying on other sources of scarcity to create value than the scarcity of works. In many cases works will be available quickly at low cost to most people. But there are other forms of scarcity. The actual performance of works, the creation of works, is still something that requires attention and thus obeys the rules of scarcity of attention.

Rasmus Fleischer has pointed out that when speaking of encouraging art or incentivizing artists, what is meant is almost always encouraging only one aspect of art, the aspect of creating works. Not performances as such. Traditionally performance rights have, to be sure, been protected as well, but not nearly as well as the economic copyright. Yet still performing seems somehow, somewhat simplified, to be primary. Fleischer argues that in the age of digital reproductions policy makers may need to re-focus on performance as an artist format (Fleischer 2006, Fleischer 2007).

There is ample reason to re-visit the old motivations for copyright in a society where creativity is everywhere, distribution instantaneous and structure flimsy at best. This would necessitate a thorough re-thinking of the nature of creativity, leaving the idealized image of the romantic genius author aside and accepting abundance of creativity as a given. Policy makers need, generally, to revisit the historical foundations of copyright and other intellectual property rights. There are far too few studies examining the nature of creativity and the history of intellectual property constructs, even if there are some scholars pursuing this line of research (Carroll 2004).

One of the largest challenges to the information society model is the role of users. Instead of passively consuming information users contribute, collaborate and create (Crumlish 2004). It has even become popular to speak of “We - the media”, signaling that media today is everyman’s game in a sense (Gilmor 2004). The analysis of this development has even led some theorists to the conclusion that we are now witnessing an entire new mode of production emerging in society (Benkler 2006).

The examples are many, and worth recapitulating. While the Wikipedia is the perhaps most famous, there are numerous other sites with what is called – unfortunately, I think – user-generated content. Video-sharing sites and search engines both draw on the values created by users in different ways and in an average blog it is safe to assume that comments are as valuable as, if not even more valuable, than the actual posts.

The effect this has on the ideal type model of the information society of the middle of the 1990s cannot be overestimated. Assuming that information will be produced

---

28 Unfortunately because it seems to suggest that other content comes from some higher source of content creation that is above and beyond the simple user.
by a select few, that production will be controlled and sparse, no policy problem ever arises. Information may grow old and rot, but this can be dealt with. Information overload may be a problem at times, but it can be tempered, as long as the information producers hold the prerogative of producing information in their hands.

Removing this prerogative results in massive amounts of information. Instead of the structured question and response-situation in a court of law with clear roles and limited interaction, we find ourselves at a magnificent party where everyone talks to everyone else and the chatter fills the room to such a level that it can be hard to hear what your interlocutor is actually trying to convey.

That information production is widely distributed is trivial to establish. Look at the growth of the blogosphere or of user generated content in general. It is known that the blogosphere grows quicker than any other information set measured in the history of man (Sifry's Alerts 2007) and the growth of user-generated content will probably accelerate when the young generation grows up (if it keeps its media production patterns) (Pew, 2006).

The wide distribution of information production has also lead to an immense production of information. As seen above some sources even indicate that the amount of information digitally stored actually doubles every three years (How Much Information 2003).

The quickening pace of information production contributes to the background noise and coupled with the ever-cheaper storage technologies being developed the end result is that we see an explosion in information storage of different kinds. Not only do we have more information producers, we also have more information hosts than expected in the the information society model.

Here, then, the information society model fails since it assumes a level of control over the creative process, distribution of works and the value of information that is inconsistent with many of the phenomena encountered today.
**File-sharing and enforcement**

Another example of a phenomenon that the information society model cannot contain nor handle in a good way is the continued failure to control file-sharing networks as well as the counter measures employed in trying to destroy these networks. In this section I will present a study of how copyright holders are currently fighting these networks and show why their tactics are hard to address with the information society model. This section is based on (Lundblad, Noise Tactics in the Copyright Wars 2006) but has been adapted and reworked to emphasize the lessons we can draw for the information society model.

In the ongoing fight for control over copyrighted material on the Internet, the strategies are now becoming more and more complex. Lawsuits, information campaigns and copyright protection schemes are complemented with more questionable tactics. One such tactic is the use of different technologies that pollute the file-sharing networks in different ways. Such pollution can usefully be thought of as pollution or poison introduced in the communication network, and it offers a number of interesting issues.

Here the focus will be on the legal issues associated with such pollution strategies and related approaches.

As noted earlier, over the last few years it has become more and more clear that the design of technologies, of architectures or code, is an important object of study for anyone wanting to understand the development of legal systems in the information society. As we have shown, scholars such as Lawrence Lessig have explored this in detail, explaining that “code is law” and that the design of software and hardware has become more than a purely technical pursuit – it is now a regulatory activity in every sense of the word (Lessig 1999).

Much of the focus in Lessig’s work, however, is on the constructive design of control architectures that express or try to create certain regulatory effects. Lessig says very little about the possibilities of disruptive attacks on architectures and what regulatory effects such attacks may have. Such disruptive attacks are also inconsistent with the information society model, since they seem to indicate a loss of control over distribution.

There are, however, a number of ways in which one could use the fact that architecture regulates – or that code is law – in order to create regulatory effects not by building architectures, but rather by destroying existing architectures. Setting out examining how noise of different kinds can be directed, added and utilized to disrupt architectures a wide range of possible measures become available to us.
Freedom of speech can be destroyed by flooding a website that says things that are controversial to some. Privacy can be protected by introducing massive amounts of slightly incorrect information in systems in order to blur the picture given of an individual and copyright can be protected by submitting massive amounts of rubbish to file-sharing services, muddling the network and destroying search capability within these networks. Here I will limit myself to a discussion of how copyrighted works can be protected by attacking the architectures of file-sharing, and to the legal issues related with such practices.

Noise tactics come in many different forms and formats. It is useful to try to determine some different forms of noise tactics in order to be able to discuss them in more detail. The perhaps most common attack would be the use of a decoy, i.e. a file that claims to be a copyrighted work, but is in fact something else (Christin, Weigand and Chuang 2005). This something else may vary: it may be a worthless file that contains nothing at all – random numbers for example. It may also be another work, or a copy of the work in question but with noise interjected into the song or film as to make it less pleasurable to see or listen to.

We would call these decoys passive decoys of different kinds. They do not attempt to harm the user/downloader or his or her system. They are merely useless.

The opposite is true of active decoys that contain viruses or programs that harm or destroy material on the user’s computer. Such content also comes in many different forms and shapes but active attacks can usefully be thought of as computer viruses, worms or perhaps even rootkits that enable hacking the user’s computer later.

Active attacks can, generally, also be categorised according to the effort required by the user to be afflicted. High effort-attacks are attacks which only afflicts the user if he or she actively seeks out pirated material in the networks. An extreme example may be an image-file of a popular piece of software distributed in a file-sharing network that needs to be a) downloaded b) burnt or mounted as an image file and c) installed before the attack actually commences. Low effort-attacks would be attacks where it is enough to download the file-sharing software to be afflicted. An example would be a computer virus designed to affect only the Kazaa-client or to erase mp3-files.29

An alternative to this categorization would be to try to discern what kind of behavior that triggers that attack. In principle, it would seem to be possible to categorize attacks on the basis of whether they are triggered by infringing or non-infringing behavior.

29 Such viruses actually exist (Leyden 2007).
Is it conceivable to design attacks so that they only trigger when a user has committed what would constitute an infringement of copyright, for example? Such attacks would then be automated responses to illegal behavior, much like electric fences for cattle.

The problem is that this idea builds on the premise that it is easy to know what constitutes illegal behavior and what does not. Imagine for example someone who has bought a CD issued by Sony BMG. The buyer then reads about the rootkit and security problems created by Sony’s technology and chooses to download the CD as mp3-files for listening to on his or her computer (Russinovic 2005).

The behavior, seen as a sequence of actions – downloading the files and then playing them – might be construed as legal private copying permitted under current copyright rules. But it can also be construed as illegal copying and playing of pirated files. It seems far from clear that there is any simple way of singling out a sequence of actions as legal or illegal in this case.

In general, attacks can also be categorized according to their purpose. Christin, Weigend and Chuang (2005) distinguish between poisoning and pollution – a useful distinction where poisoning is the directed attempt to reduce availability of a certain item and pollution is an attempt to fill the network with noise in general. Studies suggest that a significant portion of the content found in, for example, the Fasttrack-network is unusable (Liang, et al. 2005).

Poisoning can be done in a number of different ways. It is possible to use poisoning for marketing, for example. By simply issuing files that contain small samples of the content in question, poisoning can actually work as a form of advertising. It can also be used as an attempt at communication with downloaders. The most well-known example of this is probably pop-singer Madonna’s interesting attempt to morally educate the file-sharers with a large copy of what looked like her single American Life. When played, the file simply turned out to be a short phrase (“What the fuck do you think you’re doing!”) followed by silence for several minutes.

The object of the noise attack can also be used to categorize different attacks. One possibility is to attack the content of the network (poisoning the network with fakes for example), but it is also possible to attack the network as such and try to bring it down (Daswani and Garcia-Molina 2002). It is thus useful to distinguish between attacks that target content and those that target the communication capabilities of the network.

With these different attacks in mind we can turn to the development of file-sharing to see how effective different attacks are and are likely to become with the technological evolution.

Often, in speaking of file-sharing, several different technologies are lumped together under one concept. These technologies, or architectures, are however
different and open to different kinds of attacks. It thus becomes necessary to discuss how the systems work in order to discuss what different kinds of attacks are possible.

File-sharing networks are really not new at all, and the basic model offered in the networks is not technologically complex, but these networks have still had an enormous importance for the development of the legal discourse on law, information technology and the Internet. A history of file-sharing technologies and networks shows clearly that noise tactics will become less and less powerful over time.

One way of sketching the history of file-sharing architectures would be to speak of five different generations, and to point out how these different generations could be controlled.

Firstly, there was the Napster-generation. These architectures had a central control point, a server which could be targeted. In the case of Napster the architecture’s legal superstructure – a company – made it even simpler to control. All the copyright holders had to do was to take control over the central parts of the architecture by suing the company. File-sharing in architectures such as the Napster one is no real threat to a copyright holder with the means to acquire legal help and to sue the companies involved. Noise tactics could also be used efficiently, since no efficient rating systems were available.

The second generation of technologies proved harder to control. This generation – one could call it the Gnutella-generation – did not have any one simple central point that could be controlled. Networks such as Grokster and Kazaa turned out to have a legal superstructure that was vulnerable to legal action in some cases, but the results were more dramatic for the software makers than for the file-sharers. An attack at the software provider did not shut down the network as efficiently as in the Napster case.

Already here, in the second generation file-sharing architectures, it becomes necessary to find other means of control than simple lawsuits to ensure control over copyrighted materials. And it is here that noise has been used most efficiently. Both passive attacks and active attacks, pollution and poisoning turn out to be tactics that reduce the value of the file-sharing networks for users.

It is interesting to note that the file-sharing networks quickly evolved responses to noise tactics. Kazaa introduced a rating system early on that allowed users to rate the quality of files on the network, a counter-move intended to reveal obvious fakes on the networks.

This severely limited the potency of noise tactics. The rating systems may have been overly complicated, however. In fact, studies now show that it seems enough to rank files according to their availability and distribution in the system in order
to eliminate noise. The key problem will be to estimate what time it takes for a file to reach such distribution and be evaluated by users so that searches based on distribution can be used instead of rating systems.

Noise attacks could still be successful – albeit not in the long run. That might not have been the aim, on the other hand. Although it is hard to prove, it seems rational to assume that noise introduced on the networks always was intended to slow them down in order not to harm the initial sales of a single or a record, for example, rather than to render the file-sharing networks inoperable.

The third generation file-sharing networks changed the architecture from one large open network to semi-closed small networks. This generation, the Direct Connect-generation of networks used software such as Direct Connect to create small networks, where filesharing could be controlled in a higher degree. These networks of course turned out to be highly resistant to noise attacks, since the network owners could easily control who contributed what. More open Direct Connect-networks used simple access rules – where the user had to contribute a certain amount of software, movies, music and other files to be admitted. Here many contributed less valuable material in order to gain access, but minimize complicity. This, however, was no conscious noise tactic, but rather an extension of the already prevalent free-riding strategies evident in many file-sharing networks (Adar and Huberman 2000).

These networks are hard to detect, and even harder to police for the copyright holders. However, if the hub or network is semi-open and admits new users, then they can of course be detected. Naive users of these networks are easy to detect, and a number of court cases in Sweden involve users who have in fact used Direct Connect.

The fourth generation networks are networks that employ an architecture that is both highly decentralized as well as encrypted. This generation could be represented by Freenet – a project that aims at creating a network where individual users will be undetectable. The Freenet-generation of network designers is a generation that openly strives to design the network in order to make policing it difficult.

The fifth generation of file-sharing networks, or rather technologies in this case, might be the Bittorrent-generation. Here the idea is no longer to be connected to a certain network, but rather to distribute and download individual files in an efficient manner. The closest thing to a central point that this generation exhibits are the so-called tracker sites that publish lists over distributed files. These tracker-sites, however, only point at other parties distributing files. They do not distribute the files themselves.

The tracker-sites offer a simple way of controlling the quality of the content and that is a comment page at the bottom of the individual page listing the torrent-file.
Here noise tactics are thwarted by users simply not distributing noise files in any larger extent, so that these files are naturally eliminated from the tracker sites.

Noise files simply fail to survive the selection process for torrents and are filtered out by users over time. In the fifth and fourth generation of technologies noise tactics – at least the simple ones – have ceased to be efficient counter-moves to file-sharing.

It may well be considered strange to ask if the noise tactics described here are legal or under what conditions they are legal. The whole file sharing scene is filled with risks and it seems only fair, to some, that copyright holders defend themselves any which way they can. This view will however not hold, for several reasons.

Firstly, there are legitimate uses of file-sharing. It is important to remember that not all of the content in file-sharing networks is pirated copies of music. In fact, a lot of the content is distributed legally and with the consent of relevant rights holders. Any attack on the systems themselves endanger these legitimate uses in a way that is not acceptable.

Secondly, it is less than clear what actions are actually illegal. Downloading copies of music or movies that you own in new and different formats may well fall under the exemptions for private copying or fair use. If files obtained in this manner turn out to be harmful, the harm may well be visited upon someone who has done nothing wrong.

Thirdly, and as a matter of course, all work to enforce copyright must be done within the borders of what is legal. One crime does not legitimatize another, and even if there have been suggestions in the US and even draft bills for a right of self-defense for copyright holders, no such right exists today (Electronic Frontier Foundation n.d., Berman 2002).

It is important to note that this holds no matter what kind of effort-level is defined for the attacks. Even a virus that requires a high user effort to activate is illegal and cannot be covered under any exemptions or self-defense rules as long as it was indeed intended to infect certain users.

In many cases, the use of a file-sharing network is subject to conditions set out in a license that the user has to agree to when installing the software. Such click-wraps are interesting and complicated contractual constructions and it can be discussed whether or not they are binding, and how they should be interpreted.

It at least seems clear that the fact that one user fails to abide by the conditions in such licenses by, for example, sharing copyrighted material without the proper clearances for doing so, does not release another party from duties imposed by the license.
So if the license clearly states that the network may not be used to distribute harmful material or viruses, this will still be a breach of the license even if other users distribute copyrighted materials.

A close analysis of the end-user license issued by Kazaa is instructive. The license starts out by prohibiting a number of uses of the software in section 2.

"You agree not to use the Software to:

2.1 Transmit or communicate any data that is unlawful, harmful, threatening, abusive, harassing, defamatory, vulgar, obscene, invasive of another's privacy, hateful, or racially, ethnically or otherwise objectionable;

2.2 Harm minors in any way;

2.3 Impersonate any person or entity or falsely state or otherwise misrepresent your affiliation with a person or entity;

2.4 Forge headers or otherwise manipulate identifiers in order to disguise the origin of any data transmitted to other users;

2.5 Transmit, access or communicate any data that you do not have a right to transmit under any law or under contractual or fiduciary relationships (such as inside information, proprietary and confidential information learned or disclosed as part of employment relationships or under non-disclosure agreements);

2.6 Transmit, access or communicate any data that infringes any patent, trademark, trade secret, copyright or other proprietary rights of any party;

2.7 Transmit or communicate any data that contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment;

2.8 Disrupt the normal flow of dialogue, cause a screen to "scroll" faster than other users are able to type, or otherwise act in a manner that negatively affects other users' ability to engage in real time exchanges;

2.9 Interfere with or disrupt the Software;

2.10 Intentionally or unintentionally violate any applicable local, state, national or international law, including securities exchange and any regulations requirements, procedures or policies in force from time to time relating to the Software;

2.11 Monitor traffic or make search requests in order to accumulate information about individual users;

2.12 "Stalk" or otherwise harass another;

The license is available at http://www.kazaa.com/us/eula.htm (accessed [2007-01-06])
2.13 Modify, delete or damage any information contained on the personal computer of any Kazaa user;

2.14 Collect or store personal data or other information about other users; or

2.15 Intentionally make available spoofed files or files with information designed to misidentify the actual content of the file."

Many of the noise tactics discussed here will thus be prohibited by the end-user license agreement. It is, for example, not possible to use aggressive noise tactics and viruses, since this would violate – explicitly – section 2.7. Neither would it be possible to erase content or otherwise attack computers under the rules of the license.

The key section, however, is of course 2.15. This section clearly rules out item poisoning and seems to limit the possible noise tactics to an absolute minimum (correctly named files with low quality). All in all it seems pretty clear that anyone who uses the software is limited in the extreme in the use of noise tactics under the existing license. How is this analysis affected by massive volumes of illegal file-sharing? Can the fact that the software manufacturer knows that the network is used in ways that are not compliant with the license affect also other parties duty to follow the conditions set out in the license?

One possible argument would be that the end-user license agreement should be considered non-binding since the software manufacturer clearly is not enforcing it. The argument would point out that the software is used in massive infringements of copyright, even though section 2.6 clearly prohibits this. The failure of the company to enforce section 2.6 would then be used to support that the company had no intention to enforce any of the other sections and that the license, as a matter of use, is no license at all but rather a statement or a wish on behalf of the software manufacturer.

This argument is weak in the extreme. It seems less than clear why all parts of a license must be enforced in order for the license to be regarded as valid. In fact, if this argument were to hold, the massive file-sharing of pirated copies of music could be taken to mean that the music industry in fact did not intend their licenses as licenses either. It is in no way possible to argue that massive disregard of a license renders it legally non-binding.

The conclusion then seems to be that it is not possible to use noise tactics and follow the rules of the license in at least this case. Other file-sharing networks have similar license agreements, but there are of course examples where this will not apply. Both aggressive, passive, high and low effort attacks seem to be ruled out. Both pollution and poisioning as well.
The fifth generation file-sharing networks, Bittorrent, lack any common license. Here it seems that no license or contract would prohibit rights holders from distributing noise content.

In discussing attacks on file-sharing networks it is easy to forget that there is a large volume of files that are shared legally. Any attack on the networks as such, any attack on their communication capabilities, thus becomes a matter that goes beyond fighting copyright infringements and may be subject to a number of provisions in criminal law. Different noise tactics may be illegal from a criminal law standpoint. Here it becomes difficult to be specific, since the provisions differ from country to country, but a number of general legal observations can be made. Noise tactics that involve the writing and distribution of computer viruses of different kinds will be illegal to the same extent these practices are illegal in general. Under Swedish law rules concerning computer intrusion, corruption of data and illegal use of hardware will be relevant. Rules on fraud may also be relevant, even if the case for this seems weak. The argument for considering rules on fraud or forgery would be that files in the system have both a financial and evidentiary value.

Consider the following case: a person is brought to court for having downloaded and distributed a piece of music through the use of a file-sharing application. The user argues that he has done no such thing, but the copyright holder submits screen dumps to the court to show that a file by that name has indeed been downloaded from the user’s computer, or at least from the relevant IP-address that the user had at the time the screen dump was taken. The court now has to decide the case on the evidence in the case, i.e. the screen image or screen dump. If the court now finds the man guilty on the basis of the screen image showing a file by the same name as the copyrighted work, the naming of the file becomes important. If someone then has issued false files – injected noise into the system, consciously misnamed in order to pollute a network, then the file that was downloaded and distributed (often automatically from a default folder) will in fact be convicted on the basis of having downloaded only a file with the same name as a copyrighted work, not the work itself.

In this sense the practice of network pollution becomes counter-productive, to say the least. The evidentiary value of screen images with images of files with the same name as popular films and songs must be considered nil, or at least very small. A copyright holder basically has to show that the file downloaded was in fact the copyrighted work and not a noise file with the same name as the copyrighted work. The only way of doing this is to download the entire file and then secure evidence pertaining to the download.

What, then, of the case where the file in the screen image entered into evidence is indeed not the copyrighted work, but a noise file with the same name as a copyrighted work? It seems obvious that the issuer of the noise file in this case has committed some sort of forgery or evidence tampering, even if it was not directed
at a single user. Rules for determining exactly what the issuer of a noise file has done will vary from jurisdiction to jurisdiction, however. Courts may have to consider the frequency of noise files in future cases when trying to decide the evidentiary value of screen dumps, even if they have not done so in recent cases (it has not been introduced as an argument by the defense, either).

It should of course also be noted that all noise files or noise tactics that involve components that register personal data fall under the rules of the relevant national and international rules on data protection. It is easy to imagine a network pollution strategy that uses a file that actually contains a copyrighted work, but also a piece of software that records everything that can be found on the relevant computer and sends it back to a supervisor or a database for later processing of legal claims.

The Swedish Anti-Piracy Bureau – a private organization - tried a similar tactic in fighting piracy and collected IP-addresses of users sharing files with names that corresponded with the names of copyrighted works. The Swedish Data Protection Board found that such collection practices indeed falls under the Swedish law implementing the data protection directive. The anti-piracy bureau applied for an exemption under the rules of the same law and was controversially granted one for the collection of IP-addresses of copyright infringers. This decision was however limiting in that it only allowed the Swedish Anti-Piracy Bureau to collect information about distributors and only in severe cases, and for a limited time (Datainspektionen 2005).

It would lead to far from our subject to discuss this in detail, but suffice it to say that noise files or network pollution with an active content that distributes personal data in any matter, way or form must abide by the national and international privacy rules that apply.

Copyright law is of course also relevant. There are three basics areas of copyright law that need to be addressed in discussing noise tactics. Firstly, the issuer of a noise file that merely contains a low quality version of a work offers an intriguing problem. If that issuer lacks the relevant rights to do so, he or she may themselves infringe on the rights of the copyright holders. The issuing of files with low quality, or even looped samples, may actually be subject to rights clearance requirements. But even if these rights are indeed cleared and an artist has licensed use of his or her work for noise tactics in file-sharing networks, the practice may be doubtful. Under Swedish law, for example, downloading is now illegal if the user knows or should have realized that the file he or she is downloading is being distributed through, for example, the Internet without the consent of the copyright holder.

Determining if the user knew or should have known that a certain file was put in distribution with or without the consent of the rights holder is significantly more complicated if there exits a set of low quality noise files that the user knows have been put on the filesharing networks with the consent of the rights holders.
The user might argue that she thought that the quality of the file downloaded was so low that it was only a marketing specimen or a noise file, and if the portion of noise files grows more, that may actually be a reasonable expectation in some circumstances. By issuing low quality versions of a file or versions with irritating noise, the rights holder is in fact distributing the work in the file-sharing networks with all the legal consequences that this entails. It should also be noted that distortions, noise, loops and other such manipulations of a work may infringe on the moral rights of an author, even if this seems as a less than likely case in practice.

Noise tactics are tempting and interesting for rights holders that see their own control over copyrighted works disappear into more and more complex file-sharing networks with less and less possibility of tracing distributors or downloaders. Noise tactics, on the surface, seem to offer a way to fight the machine by putting noise in to the communication machinery. They are also evidence of a recognition in the rights holders' community of a loss of control over distribution.

There are numerous ways of generating noise, pollution or poisoning in a network. It is, however, questionable if these tactics are legal. Concerns relating to criminal, privacy, copyright and contractual law should be taken seriously, not only because it is the law. The rights holders may otherwise risk further eroding the respect for the very body of law that they depend on, and create a future in which copyright will be a war between vigilante rights holders and pirates with ever evolving technologies.

How, then, should policy makers address issues like these? How should policy makers address new companies like Media defender\textsuperscript{31} that explicitly say that they aim to insert noise into file-sharing networks? The information society model fails here. This model assumed that networks could be controlled but this is far from the case.

Peer-to-peer networks and file-sharing has clearly shown that the amount of control exercised over information distribution in our society is slight. Information flows in numerous networks, some anonymized and encrypted, some open and free. The idea that information distribution could be controlled in different ways permeates early thinking about the information society, and this central idea has shaped some of the early policy responses. This idea, fundamentally Bellian, is one of the perhaps most important themes of control in the policy discourse on the information society.

Policy makers are now witnessing the rise of uncontrolled distribution, and the metaphors to describe this trend reveal the obviously scary nature of uncontrollable networks: some even speak of “darknets” (Biddle, et al. 2002):

\textsuperscript{31} See \texttt{http://www.mediadefender.com} (2007-09-27)
Throughout this paper, we will call the shared items (e.g. software programs, songs, movies, books, etc.) objects. The persons who copy objects will be called users of the darknet, and the computers used to share objects will be called hosts.

The idea of the darknet is based upon three assumptions:

1. Any widely distributed object will be available to a fraction of users in a form that permits copying.
2. Users will copy objects if it is possible and interesting to do so.
3. Users are connected by high-bandwidth channels

The darknet is the distribution network that emerges from the injection of objects according to assumption 1 and the distribution of those objects according to assumptions 2 and 3.

One implication of the first assumption is that any content protection system will leak popular or interesting content into the darknet, because some fraction of users—possibly experts—will overcome any copy prevention mechanism or because the object will enter the darknet before copy protection occurs.

The change in discourse is tangible, and the loss of control evident in the language as well as in the concept. Note that systems here “leak” content, they are broken, fragile. Darknets are anomalies in the information society model: control is difficult, distribution quick and legality questionable. But it is at the same time hard to eliminate these networks:

There is evidence that the darknet will continue to exist and provide low cost, high-quality service to a large group of consumers. This means that in many markets, the darknet will be a competitor to legal commerce. From the point of view of economic theory, this has profound implications for business strategy: for example, increased security (e.g. stronger DRM systems) may act as a disincentive to legal commerce. Consider an MP3 file sold on a web site: this costs money, but the purchased object is as useful as a version acquired from the darknet. However, a securely DRM-wrapped song is strictly less attractive: although the industry is striving for flexible licensing rules, customers will be restricted in their actions if the system is to provide meaningful security. This means that a vendor will probably make more money by selling unprotected objects than protected objects. In short, if you are competing with the darknet, you must compete on the darknet’s own terms: that is convenience and low cost rather than additional security.

This is a far cry from the self-confidence of the system designers engaged in negotiating the Electronic Copyright Management Systems. And the idea that policy makers must meet the terms of autonomous technology is intriguing and significant – but it is also a failure of the information society model.
Privacy – crisis and failures

Background – rights of privacy

The right of privacy has a long and diversified history. It has variously been described as a “right to be let alone” and as a complex and multifaceted right to one’s own personal data constructed very much like intellectual property. Laws, cases and writings exist in abundance. There is an enormous amount of different theories and writers that have given the subject their attention.

There are international principles of privacy that allow us to examine the concept at its most general level. The Organization for Economic Cooperation and

---

32 When speaking of privacy I feel that it is important to start with a note on terminology. In studying privacy the student faces a large number of terms that are more or less overlapping and none too well-defined.

The three terms that I feel are most important are “data protection”, “privacy” and “integrity”. The last term is difficult and seldom used in scholarship. It is a term that sometimes is used as a quick translation of the Swedish concept “personlig integritet”, but the best translation of this concept may be “data protection” or “privacy”. The mis-translation is useful, however, as we shall see later.

There are several different ways of understanding the different terms. One way is to say that privacy is a consequence of data protection, or that privacy is a delimited problem space that constitutes a subset of the larger data protection problem space. To worsen the linguistic confusion it seems as if privacy is more often used in the US and data protection more of a European term.

My own choice in discussing the issues has been to use privacy and data protection interchangeably. It can be argued that this confuses the reader and that it creates problems. I think, however, that it is safe to say that for the purposes I use the two terms no such confusion of any meaningful character is likely to arise. Where such a confusion is likely to arise I have noted so and tried to solve the problems specifically.
Development (OECD) has published a series of guidelines that are essential to understanding the concept of privacy as it has developed in western society. The OECD principles are useful in trying to delineate the concept of privacy and developing this concept into one that can be used operatively in the research effort.

The OECD developed a number of principles which they feel would be useful to any discussion of privacy, and also to any legislation (OECD 1980). The standing of these principles is unquestionably still strong. They are for example reflected in the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The principles are:

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) with the consent of the data subject; or

b) by the authority of law.

Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of
establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

13. An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him within a reasonable time;

at a charge, if any, that is not excessive; in a reasonable manner; and

in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

These principles, then, give us a general idea of what privacy is, but they do not give us any exact notion of what it is that is being protected. There are, however, other more useful taxonomies of privacy to employ in our analysis. Philosopher Beate Rössler outlines three concepts that are useful in our study of privacy in both the information society and the noise society in her book The Value of Privacy (2005(2001)). Rössler works with three different concepts of privacy: decisional, informational and local(Rössler 2005(2001)) .

Decisional privacy is defined as privacy that “establishes a space for manoeuvre in social action that is necessary for individual autonomy” (Rössler 2005(2001), 80) and Rössler uses this concept to show what the actual value of privacy to the individual is. When bereft of privacy the individuals space for social action dissolves.

Informational privacy relates to the “control of the information relating to [a] person” (Rössler 2005(2001), 111) and is a more abstract kind of privacy concept. This concept is much less instrumental than that of decisional privacy and, Rössler notes, also what is usually considered the core concept of privacy.
Local privacy is “the classic, traditional one, even if it is open to dispute whether this meaning of ‘privacy’ really does spam all cultures and historical periods” and it is “the privacy of the household”. (Rössler 2005(2001), 142)

The division of privacy into decisional, informational and local offers us a different and useful understanding of privacy. Rössler’s trichotomy is subject to strong pressures in the current policy debate as well, as we shall see.

Privacy in crisis
In choosing privacy as a subject for study I claimed that it is a policy subject in crisis. In the following short sections I will attempt to show some of the current debate and substantiate that claim.

Privacy has been counted out so many times that this very defeatism should be the object of a study all on its own. One of the really large privacy debates has more or less subsided. The debate about the right to use encryption has – more or less – been won by the privacy interests (Diffie and Landau 2007) (Diffie & Landau, Privacy on the Line: The Politics of Wiretapping and Encryption- updated and expanded edition, 2007). The battle against government backdoors to encryption and against regulating access to encryption (culminating with the Clipper chip debacle) was won by privacy interests.33 These battles showed with all desirable clarity that code can be controversial, but they also showed that it is hard to regulate the use of technologies. This debate is a background against which much of the present-day literature must be read.

In 1999, the debate about privacy, in spite of the victory on encryption, reached some sort of low point. Two books were issued with the name The End of Privacy, and both books were extremely pessimistic about the possibilities of creating an information society that had a private sphere intact (Sykes 1999, Whitaker 1999). A third book on the same subject came out a year later, and it was no more cheerful in its attitude, it even proclaimed the Death of Privacy (Garfinkel 2000).

The first of these books, The End of Privacy by Reg Whitaker, takes the idea of surveillance as power as its starting point, and extends the discussion on Bentham’s curious prison – the panopticon – to something that he calls the participatory panopticon.34

Whitaker’s point is important. He writes that we are now living in what could be termed the consensual panopticon, in which we agree to being watched and submitted to surveillance and monitoring – and all because of a sense of security

---

33 Even if it is true that some regulation of encryption persists in international dual-use control agreements, like Wassenaar.

34 Whitaker 1999 pp 139-159
that stems from the idea that when watched we are at least safe. In an ironic twist
Whitaker takes Santa Claus as an example and points out he really is the very
model of infringing privacy in a good way that encourages accountability. But, he
notes, it is far from obvious that the surveillance society also is what he paints as a
Santa Claus society.

Charles Sykes, in his book that carries the same title as Whitaker’s, has a broader
and perhaps less philosophical perspective (Sykes 1999). He is also more alarmist,
and speaks of a developing exposure culture. He joins many other privacy scholars
in using the Clinton-affair as an example of the “tell-all society”. Sykes also states
that he believes that privacy is an absolute condition for the renewal of civil society
(Sykes 1999, 258):

But respect for the individual and of the family is only a first step. Respect for
privacy will be at the heart of any renewal of a civil society. For it is privacy that
gives us control over our lives, enables us to be individuals, and thus allows us
to fulfil our public as well as our private duties.

Sykes argument is more moral and perhaps conservative than Whitakers and is
essentially an argument from basic rights.

These three books, and a great number of articles, seemed to start from the same
premises: privacy is valuable, and it is being eroded to the brink of extinction and
there is nothing we can do about it. This main line of argument got a public
representative in SUNs Scott McNealy who off-handedly commented on some
privacy concerns by replying (Sprenger 1999): “you have zero privacy anyway --
get over it”. His statement drew quite some criticism, but there were those that felt
that he was correct. A year earlier, physicist, science fiction writer and self-styled
privacy scholar David Brin had released a peculiar book called The Transparent
Society: Will Technology Force Us to Choose Between Privacy And Freedom (Perseus
1998). In this book Brin outlined an argument that accepts the alarmist theses of
the abovementioned observers as premises. He grants them that privacy, as a
concept, is hopelessly lost. In the introduction he writes of a choice between two
cities of the future. In both cities privacy is utterly lost in a panopticon of cameras,
databases and monitoring technologies, but there is still choice. The choice now
stands between living in a world where but a few have access to the data collected
and a world in which everyone has access to data about everyone.

Brins tantalizing argument is that we should strive for a world in which the death
of privacy coincides with the rise of a transparent society, and he strengthens the
argument by stating that it is important to realise that this will be – in many ways –
a welcome change: transparency encourages responsibility and accountability.

This may be only partly true, however. Consider the sad case of Amy Boyer, in
which a young psychopath by the name of Liam Youens stalked and ultimately
murdered Boyer, and he tracked her down with the help of an online search agency
that helped him find the girl after that she had moved from the town where he
lived. Boyer’s parents later sued the information and search agency, and the New Hampshire Supreme Court acknowledged in its decision that there should be a certain liability for soliciting information in certain circumstances. The whole affair was complicated and made even more horrifying by the fact that the murderer had published his plans on the Internet beforehand for everyone to see (Helen Remsburg, Administratrix of the Estate of Amy Lynn Boyer v. Docusearch, Inc., d/b/a Docusearch.com, 2003). Transparency may not guarantee anything else than that we know who did what and why. The increase in accountability may only have marginal effects on the behaviour of the seriously disturbed.

The debate on privacy today is polarized, and heavily so: one one hand we encounter those who argue that privacy is more threatened than ever before, and that we stand before the end/death of privacy. On the other we find debaters and pundits who declare that privacy is a moot issue for all honest citizens and only an issue if you have got something to hide.

There is also a third viewpoint, as explicated by Amitai Etzioni in his work *The Limits of Privacy* (1999). Etzioni argues for a communitarian view and compromise of the subject of privacy in which the interests of the collective must be weighed against those of the individual. Etzioni’s work is a compromise between the extreme positions outlined above, and characterised by a respect for the intricate balances that need to be struck in safe-guarding privacy while still protecting the interests of society. As an example Etzioni mentions the identity of sex offenders, and refers to the so-called Megan Laws, that require the identity of known sex offenders to be publicized. Again, the background is tragic: Megan Kanka was murdered by a convicted sex offender that under the protection of privacy could move into a regular neighbourhood and there strangle and assault Megan (Etzioni 1999, 43-74). Etzioni’s position is made clear in his attempt to construct what he calls a “contemporary conception of privacy” (Etzioni 1999, 216):

> Above all, a communitarian approach to privacy avoids the failings of static conceptions by taking into account sociohistorical changes. For instance, it recognizes that the more privacy is granted from informal social controls in a given period, the more state controls will be necessary in the following years to sustain the same level of social order.

Etzioni’s view of privacy as an obstacle to social control is in tune with Brins reasoning, but his argument for privacy is less clear. Why would privacy at all be necessary? What Etzioni could argue for here is that he would accept Rössler’s decisional and local privacy, but that the more formal informational privacy she describes needs to be tempered.

In summary the current debate is very polarized, with the exception of a minority who with Etzioni strive for some sort of compromise. It is, however, not certain if the concept of privacy lends itself to compromise or not; it might be very much like the concept of pregnancy: either you are or you aren’t. Either you have or you haven’t got privacy.
Technology has long been intertwined with the on-going discussion about privacy. In George Orwells dystopian novel 1984 technologies of surveillance are an important part of the picture that Orwell wants to paint of a future that is largely a horror-version of an overwhelming and invasive government.

The idea of big brother was mainly inspired by fear of an architecture of control employed by the government, but it largely ignored the risks that private enterprise and businesses would be interested in the individual’s preferences or personal data. The idea behind the surveillance society was that the surveillance would be the state’s prerogative (Flaherty 1989).

This was a mistake made because it was not realised that personal data would quickly become a commodity, produced by the architectures of surveillance and monitoring. Andrew Shapiro, in the book The Control Revolution (1999), discusses this phenomenon in some detail and notes that there are even those who argue that we need only accept that personal data has a value and introduce a market for that value to balance the privacy issue. In a section called “The Market for Privacy” Shapiro writes (Shapiro 1999, 159):

Just as there is demand for consumer data among the corporations, so there is counterdemand on the part of individuals to keep information private. The answer, these privacy advocates claim, is to have consumers embrace this market and bargain with vendors over acceptable rules for data collection and use.

Shapiro, however, stresses that this might be “dangerously naïve”. He also notes that it “assumes that individuals can use technology and the market to achieve a task of such complexity that it has, to date, confounded most governments.” Shapiro’s reasoning supports the idea that privacy is in crisis, not least because it is unclear what citizens can do to protect themselves.

The architecture that supports the little brothers35 is not wholly different from tracking and surveillance mechanisms developed for big brothers, but they differ in one important respect: they are not centralized to one single entity that has total control, even if there are such tendencies in some solutions. But the little brothers architecture is also much harder to open up for access, since it is not one single point of access that is required, but thousands of companies that have access to more or less personal data.

The balance between privacy and security has been in the focus of much of the post 9/11-debate and a number of different articles and books have discussed the measures put in place by different governments (Davies 2006, Wai San Wong 2002, Swire 2006, Olsson 2003). One significant change from the earlier

35 A common term used to signify the many private companies, organizations and others that collect and process personal data.
information society debate – where the future of privacy was the focus – is that the new debate focuses on security.

This has strengthened the strain on privacy as a policy subject. There are now two forces at work here: both the digitization of personal data, the collection and production of new forms of personal data and the increased pressure to collect, monitor and analyze the same data. Privacy is thus doubly under siege in the sense that we now not only can produce large data sets about citizens, we also see a growing demand from security experts and others for that same data.

**Data protection policy failures**
The data protection directive has not been able to control the erosion of privacy in society. It is hard to imagine any law that could have done this and so this failure is perhaps not indicative of anything else than the fact that privacy is being eroded quickly, and that it happens by choice for many.

What is more serious and perhaps more interesting is that the data protection directive has not really succeeded in protecting personal data and maintaining identities. Identity theft is a growing problem, and for many the fact that they cannot control what is written about them on the net is a severe infringement of their freedom (Bosworth, 2007). The data protection directive is a failure in the sense that it has hardly resulted in improved data quality, and it has neither succeeded in protecting privacy to the degree it was originally crafted to do.

In a cost/benefit analysis the data protection directive is also sometimes attacked because its processing rules are costly to comply with and the benefits arising from them questionable. Companies have several times pointed to the extreme costs associated with the application of the data protection directive, and continue to consider it – in this regard – as a failure, even if the initial assessments of costs were much higher (five times higher) than the current ones (Young, 2007; Department of Constitutional Affairs, 2006).

Formal review of the directive has mainly dealt with transposition issues and there are failures here too, but they do not relate to the kinds of failures I am looking for.37

The scarce and incomplete usage statistics on P3P (see above) available seem to indicate that the standard is not widely used, and this must be taken as a kind of failure. As evidenced by the large amount of companies de-funct in the privacy enhancing technology market, it seems obvious that the underlying assumptions

36 Issues of whether or not the directive has been implemented in the same way in the different Member States.

37 Failures of implementations cannot be taken as evidence of a failed set of heuristics other than indirectly. I will not do so here.
and the model used by these companies were deeply problematic. It suffices to see that privacy enhancing technologies are not flourishing after years of evangelizing, and they seem nowhere near universal adoption. The idea that policy making could be reduced to product development or protocol design has proven difficult to sustain and seems to have failed.

Privacy, as copyright, is a policy subject in crisis – in search of new heuristics, a new model, and the way the information society model breaks down may help us design and construct such an alternative model. I will now examine two examples of where the information society model at least is an insufficient tool for the policy maker, and I will do so by discussing two concrete issues: societal forgetting and identity cohesion.

**The privacy of a cow**

The right of privacy, then, has a long and diversified history. We have seen that it has variously been described as a “right to be let alone” and as a complex and multifaceted right to one’s own personal data constructed very much like intellectual property. Laws, cases and writings exist in abundance. There is an enormous amount of different theories and writers that have given the subject their attention.

If the information society model breaks down both for information production and distribution in copyright, and for valuation of digital goods as well – since it becomes harder to value information when it is not scarce anymore – it becomes interesting to see if it also breaks down when examining issues of privacy.

Professor Viktor Mayer-Schönberger has written an important paper discussing the role of forgetting in a modern information society (Mayer-Schönberger 2007). He argues that our society has left the default of forgetting and moved into a default of remembering – and that this is one of the problems for privacy in the information society.

While Mayer-Schönberger points to an important problem I feel that he gets it wrong in several respects. The issue of privacy is indeed intimately related to the issue of forgetting, but not in exactly the way that Mayer-Schönberger envisions. And his proposal leaves much to be desired in terms of qualitative privacy and an open society.

Here I will attempt a response to Mayer-Schönbergers paper and a summary of the points where I find myself in disagreement with his argument, as well as the reasons for this. This said, I think that bringing the issue of forgetfulness and forgetting to the privacy debate is more than valuable and something that gives us new ground to cover, so even if I do not mention the points where I fully agree with or simply learn from Mayer-Schönberger, I find his paper an important contribution to the privacy debate. Not least because it shows many interesting points about the information society model.
One of the basic premises in Mayer-Schönbergers paper is that we have left the default of forgetting and moved into a regime where the new default is remembering. But this is simply not true. The regime may be retaining data – but this is a different proposition altogether. Retaining (or as composer Palle Dahlstedt suggested in discussions as an alternative term, *recording*) is never the same thing as remembering. The idea that society remembers is an idea that builds on the themes of control in the information society model, however.

Mayer-Schönberger tries to make the point that we live in a society where we remember everything, but remembering is different from recording or retaining. Remembered data is data available to an individual, data that the individual uses to form a judgment or state a proposition of some kind. Remembering is a conscious act.

Retained or recorded data is only *potentially* remembered data. A recording is the result of a mechanical or digital process. Recording is a necessary condition for remembering, but not a sufficient condition. In an age of information overload, data retention or recording can actually become a hindrance to the act of remembering. How can I remember when the amount of data retained and recorded is so vast that there is no way to search, index and structure it effectively for remembering?

Mayer-Schönberger writes (p 6):

> This is the temporal version of a panoptic society, in which everything is being watched (note omitted); it is a society in which most of what is being recorded and collected is being preserved. Regardless of other concerns we may have, it is hard to see how such an unforgetting world could offer us the open society that we are used to today.

But everything is not being watched by someone. There are no remembering individuals, no watchers that have the capability to watch all the data being retained and recorded. Information grows at growth rate, as we have seen, and there are not watchers enough around to be able to handle this deluge of information. There is no control over information production or distribution, no structuring of the personal information.

Policy makers instead need to think about concepts such as copyright, privacy and freedom of speech from a perspective that assumes not scarcity of works, personal data and speech as much as an excess of these three categories of production.

Mayer-Schönberger's argument seems to presuppose an omniscient being, able to remember, watch and observe through the haze of noise rising from the databases, the search engines and the ever-present cameras and confuses the fact that the amount of data collected grows quickly with the supposition that we are more transparent than ever. But the new forms of control that are supposed to follow from the growth in data are not the all-encompassing big-brother technologies that
everyone expected. They are far more narrow, and almost presuppose that you know who you are looking for.

Three important conclusions follow from the objection that remembering is not the same as retention or recording. Firstly, retaining data gives rise to a new form of forgetting, a forgetting-in-noise, that needs to be understood in more detail (this is explored in detail below). Secondly, when we speak of forgetting and remembering we need to focus on who does the forgetting and remembering. I think that it is easier to speak of societal forgetting than it is to speak of societal remembering. Forgetting is much more of a spontaneous process, and I think that Mayer-Schönberger is right to assume that forgetting can be understood as an emergent epiphenomenon of our individual choices to remember. If so remembering is a practice based on and limited by the fundamental scarcity of time available to all citizens. Forgetting is a practice that is not at all governed by scarcity – since it requires no actual act or time to forget something. Thirdly, Mayer-Schönberger is almost correct in pointing out that data retention has become the default in our societies. This is a consequence of sinking costs for digital storage, as well as of a general “you never know what you may need the data for”-mentality that can certainly be questioned, on many grounds, as Mayer-Schönberger notes. But it is not retention in a conscious way, it is not controlled, but rather autonomous retention.

The issue of data quality alone is puzzling bordering on the bizarre. It can be assumed that many sets of data degrade quickly, and that data quality has a half-life that is much shorter than the average storage times. It does becomes something of a mystery why some companies choose to fill their hard drives with quickly rotting data sets that will do little or nothing for their business models or their economic future. Unless they argue the opposite of course – that people never change, and that “old habits die hard” – so hard in fact that age-old data can be used to predict new patterns of behavior.

In summary then: our society does not remember by default. It retains and records data by default. And that presents us with a slightly different problem, which calls for another kind of solution. This problem challenges the information society model. Far from abolishing forgetting, the information society has created new forms of forgetting. As any digital preservationist will tell you, it is difficult to enable the future to remember a society based on digital material.

There are at least three new forms of forgetting that need to be understood in some detail, for us to acknowledge that forgetting is indeed still a large part of the information society.

The first is simply what we could call format forgetting. Much of the data retained is in formats that can only be used by applications that are now nowhere to be found. Gigabytes, if not terabytes, of data is inaccessible to all but those few who still run original software or expensive software emulators. National archives all
over the world lament the fact that we seem to have forgotten large parts of our present because of the quick generational shifts in software and formats. Often the emulators will only be able to run standard documents, and they may even not be able to find images or other included material in those formats that support similar functions.

The second is decentralised forgetting. Many people balk at the idea that they should have saved their email. They have erased it either because they changed computers or because it took up too much space at one time or another. They are the sole decision makers when it comes to deciding whether or not to archive the material they control, and they often simply do not find the material worth anything. This fact, that archiving decisions have been highly decentralised, is a new source of forgetting that creates new blank spots in public memory and private histories. Another form of decentralised forgetting, of course, is simple hardware failure and lack of backups. Lots of data has been lost, forever, this way.

The third form of forgetting is based on an excess of information rather than lack of information. We could call this noise forgetting. We all know of the phenomenon where we seem to have a word right beyond our grasp. This forgetfulness is peculiar in that we know that we know, but we just cannot actualize that knowledge, make it accessible in an act of remembering, recall the word. Much of what is retained in the information society is data like that. We know that we probably have all the information needed digitally stored to wipe many terrorist organizations of the face of the earth. But we lack the mechanisms for actualizing the knowledge, for “remembering” – in the sense Plato would have used the word: recalling – where the information is.

These new forms of forgetting are strong and present elements in today’s information society. We see them every day, and they point to a different interpretation of Mayer-Schönbergers observation that data retention leads to a default of remembering. In fact, we could argue, our excessive data retention is dangerous because it hinders us from remembering.

Mayer-Schönberger not only points to an important problem. He also suggests a course for action for us if we want to move from remembering to forgetting again. He writes:

I propose that we shift the default when storing personal information back to where it has been for millennia, from remembering forever to forgetting over time. I suggest that we achieve this reversal with a combination of law and software. The primary role of law in my proposal is to mandate that those who create software that collects and stores data build into their code not only the ability to forget with time, but make such forgetting the default. The technical principle is similarly simple: Data is associated with meta-data that defines how long the underlying personal information ought to be stored. Once data has reached its expiry date, it will be deleted automatically by software, by Lessig’s West Coast Code.
This is an interesting suggestion. A proto-version of this exists. There is actually support in the HTML-standard for certain kinds of expiration dates. If I use a date that has passed and write something like this:

```html
<META HTTP-EQUIV="expires" CONTENT="Wed, 09 Aug 2000 08:21:57 GMT">
```

The page will not be cached locally after the expiration date, which induces local client forgetting in a sense. This is of course not the expiration date that Mayer-Schönberger has in mind, but it has a small privacy enhancing effect in that if we set the date far back in the past, as I did, the page will not be cached in the individual user’s computer.

Mayer-Schönberger also argues that there may be room for legislative action in this realm:

Legislatures could – if they wanted to go beyond the minimum of what I suggest – mandate that organizations that store personal information only use software that can manage expiry meta-data (likely on a record rather than file level) and that they keep the appropriate expiry data up-to-date.

It should be noted that under the European data protection directive this is probably true today, even without meta data. Article 6 e) of the directive clearly states that there is a limit on how long data can be stored and kept:

```
[...]kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.
```

This implies that organizations today actually have an obligation of forgetting or at least remembering differently at a regular basis. It would be interesting to interview a sample of companies that have to comply with the law to see what mechanisms of forgetting they have implemented in their data protection regimes – I do not doubt that many of them would be found wanting.

But they would also have a number of legitimate questions to ask. One of which would be: how do we decide what time frames are “necessary” for different sets of personal data? This is not a formal question, or a snide remark. It actually becomes the pivotal question for anyone that wants to introduce practices of forgetting into an organization and much more so into a society.

What kinds of material should be forgotten, and when? Mayer-Schönberger could answer that this is a problem of application and not of principle, but I think that this is wrong. The principle we need to examine is the idea that we could decide when to forget something. That is not forgetting. That is what the freudians of this
world would refer to as repression or suppression, a conscious act of putting something out of your mind. Active forgetting, if you will.

Suddenly the idea of institutionalised forgetting acquires an ominous edge. Do we want societal suppression of information? Is this really a cure for the malaise of information overload and excessive data retention? Of course not. The very idea that we could decide what we forget and when it should be forgotten is very hard to defend when we take into account that these decisions must be made on a case-by-case basis by imperfect human beings. There seem to be few if any reasons to put that kind of power into the hands of anyone. To legislate forgetting cycles is even more ominous. What if a state legislated forgetting cycles which are shorter than election cycles? In order to escape accountability for actions during their reign? It is a simple example, but suffices to at least cause some worry for most of us.

This should not be interpreted as a defense for the position that we should retain all forms of data. On the contrary I think that this also runs a risk of eroding our responsibilities and our reputation for future generations. On a very large scale it should be observed that the decisions on what to archive and preserve are among the most important and meaningful decisions a society can make. So far, in humanity, we have designed specific institutions – such as libraries and archives – for this function. They have not only retained data for future generations to remember. They have filtered and selected the information they would like to retain. Since we have decentralised these decisions we can learn at least as much from differences in libraries’ collections and archival content as we can from what was actually saved.

The penumbra of works discarded speaks volumes about a time. But to institutionalize the production of the penumbra seems both dangerous and impractical. In the information society model this is a viable way forward, however. In that model policy makers have the tools and resources needed to implement a reasonable forgetfulness mechanism.

If we as a society do not reintroduce the practices of forgetting, what can then be done for protecting privacy in our time? How could the information society model help policy makers address this problem? The answer is not at all. This kind of problem is alien to the information society model and it fails when trying to address it. This is a problem that arises because of a lack of control over production, distribution and structuring of information. This is a problem that arises from the failure of the value function of information inherent in the information society model. One may argue that the actual problem policy makers face is one of information overload, rather than one of information control. It may well be that we have to shift focus in our work with data protection – from protecting individuals from “collection” or limiting said collection to a renewed focus on the rights associated with data quality.
David Brin’s transparent society (Brin 1998) is as much a fiction as Orwell’s 1984. Both are fictions because they build on the erroneous idea that we may have “just enough” information about individuals. In fact, all of us are surrounded by clouds of noise filled with faulty, irrelevant or simply redundant information about us.

There is another problem with the idea of forgetting as a basis of privacy. Even if we accept all the premises of Mayer-Schönberger’s argument it seems less satisfactory to simply indulge in privacy that comes from a society that suffers from self-induced amnesia. Nietzsche observes that the key to happiness indeed is forgetting, and there are many lessons to be learnt from this observation. But the example he uses of simple happiness in forgetting is that of a cow. Nietzsche writes (Pearson and Large 2006, 126):

> Observe the herd as it grazes past you: it cannot distinguish yesterday from today, leaps about, eats, sleeps, digests, leaps some more, and carries on like this from morning to night and from day to day, tethered by the short leash of its pleasures and displeasures to the stake of the moment, and thus it is neither melancholy nor bored. It is hard on the human being to observe this, because he boasts about the superiority of his humanity over animals and yet looks enviously on their happiness –for the one and only thing he desires is to live like an animal, neither bored nor in pain, and yet he desires this in vain, because he does not desire it in the same way as does the animal. The human being might ask the animal: “Why do you just look at me like that instead of telling me about your happiness?” The animal wanted to answer: “Because I always immediately forget what I wanted to say” – but it had already forgotten this answer and hence said nothing, so that the human being was left to wonder.

But he also wondered about himself and how he was unable to learn to forget and always clung to what was past; no matter how far or how fast he runs, that chain runs with him. It is cause for wonder: the moment, here in a flash, gone in a flash, before it nothing, after it nothing, does after all, return as a ghost and disturbs the peace of a later moment. Over and over a leaf is loosened from the scroll of time, falls out, flutters away- and suddenly flutters back into the human being’s lap. Then the human being says “I remember” and he envies the animal that immediately forgets and that sees how every moment actually dies, sinks back into fog and night, and is extinguished forever.

It is a provoking, and not a little pretentious, statement to make, but perhaps, just perhaps, we need to embrace the pain and problems of remembering in order to be human at all. The big question, the one Mayer-Schönberger has put his finger on with such accuracy, is how we combine being historical and human with at least a small measure of privacy. The answer is far from clear. But it we cannot come any closer to it by using the information society model.

**Found in mistranslation**
The discussion about data protection has so far been concentrated on the issue of privacy and largely assumed a case where an individual has control over his or her information, and where some external party reveals that information to another –
it has been based on the information society model. The image of privacy in this case is close to that of the personal sphere, or “the right to be let alone” famously alluded to in the American legal tradition (Brandeis and Warren 1890).

This is a relevant and important discussion, but it does not exhaust the issue of data protection-related problems in the information society. In this paper we will focus on a slightly different, although still important issue – the issue of personal integrity. This is partly a new focus, and it forces us to think more about being accurately represented, than about remaining anonymous.

When translated into Swedish privacy often becomes “personlig integritet” and it is not unusual to see some Swedish writers translate privacy as “personal integrity”. In some sense this has often been treated as a mistranslation, and corrected, but there is much in this alleged mistranslation that deserves to be examined closer.

The reason that we should interest ourselves in the concept of personal integrity – closely modeled on the concept of data integrity – is that we live in a society where there is no scarcity of information. In fact, I consistently argue that we have too much information, and our main problem is to filter out the bits and pieces that are truly useful to us. As I have argued elsewhere in this work this new societal model leads us to expect a situation where the individual should adopt slightly different strategies of personal data protection – ranging from hiding in the noise to using steganography instead of encryption.

Here we will examine in detail how problems of personal integrity arise and what existing laws protect us against losing personal integrity, the wholeness and relevance of our digital persona. I will then proceed to examine a suggestion for a new kind of policy response protecting personal integrity, and what problems and opportunities such policy responses would present.

In order to examine the idea of personal integrity it helps to employ a small thought-experiment. Remember the idea launched by the company PrivaSeek? They invented a digital persona that you could use to reveal yourself according to your own preferences. The company is now defunct, but the idea is still useful. As a matter of fact we all have such personas, but they are not constructed by us, but rather by everyone else. Our identity, our self, is constructed by society. We are products of sociological processes that create our sense of self (Mead 1967 (1934)).

The production of your digital persona is a question that should worry you. At least employers regularly examine your online presence closely to see what kind of

---

38 Science fiction writer Peter Hamilton suggests that in the far off future we will all have shadows (u-shadows he calls them) that we interact with on the net. Our digital personas will become agents, actors and integrated parts of our society.
person you are (Ars Technica 2007) and usually even romantic dates are checked out on the web (Quality Dating Resources, Blog 2007).

A user can claim loss of personal integrity when the digital persona in some way reflects a different individual than the one he claims to be. Note that we do not have to ascertain whether or not he or she is right – this is a tricky issue that we will return to in the discussion – but only note that he claims to have lost personal integrity. Neither do we claim that a loss of personal integrity has to be intentional – there does not have to be an attacker stripping you of your personal integrity.

But before we discuss the loss of personal integrity, it needs to be defined more closely. When would we say that the personal integrity of a digital persona is intact? What different criteria can be applied to analyze the quality of integrity in different cases? I suggest we start with three different criteria.

Firstly, we need to look at the veracity of the information offered in the digital persona. Is the information given true? If it is not this is interestingly not a privacy infringement, since privacy can only be infringed by revealing true personal data about somebody.

Secondly we need to find some criteria of relevance. Is the information given in the digital persona relevant? Is it information that is relevant to who I am? This is tricky, since it presupposes that it is easy or at least possible to discern relevant from irrelevant information. Let us analyze this further: relevant information is not necessarily information that increases my freedom of action.

Thirdly personal integrity depends on the information being updated and timely. If correct and relevant, but outdated, the information will still be harmful to my personal integrity. My integrity, so to say, has an extension in time that needs to be respected.

If these three criteria apply to the digital persona, i.e. it shows true, relevant and updated information about me, it seems reasonable to state that my personal integrity is intact.

Why is this then important? What is the value of having intact personal integrity? Interestingly at least one of the values inherent in good personal integrity is a degree of autonomy. In assessing the value of privacy it is frequently noted that this may well be the chief reason we protect privacy, since privacy is a prerequisite of autonomy (Rössler 2005(2001)).

The greater the degree of privacy, the greater the autonomy – at least on the surface of the argument. But is this true? There is at least one possible counter-argument in which what provides autonomy and freedom is not privacy so much as personal integrity. The argument can be phrased simply: what autonomy do I have if I have complete privacy – i.e. no-one knows anything about me? The answer
seems to be, perhaps paradoxically, that I have no freedom or autonomy if I have perfect privacy. Who would interact with a complete stranger? What we need is identity, and the integrity of that identity. We need not be completely transparent, but we need a persistent reputation in order to have an action space, autonomy and freedom.

So while privacy is often argued to provide autonomy, I would argue that it is in fact personal integrity that delivers on that promise. The command of a consistently emerging identity from a sea of noise is a greater asset than the ability to stay hidden in that same noise.

Personal integrity – the acquisition of an identity – provides us with autonomy and freedom. When we dissolve into noise we become shifty, shadowy characters that no-one really trusts.

Personal integrity can be lost in a number of different ways. In the following sections some of the ways in which an individual can lose his or her personal integrity is examined more closely, to give an idea of what it would entail to be denied personal integrity and to provide some examples for the discussion.

The simplest form of loss of personal integrity is when there is no coherent identity to be found in the first ten hits on the large search engines. This occurs naturally in a number of cases – for example when someone has a common name. The individual reflected may be a collection of other persons with the same name or simply the most famous individual with the same name. Here the user’s identity has simply been denied, and there is no digital persona to speak of.

Another more subtle form of loss of personal integrity occurs when the first ten hits are about the user and correct, but irrelevant. The hits in the digital persona may be data about a class he once went to, or something else, but it says nothing significant about the user, it is simply trivial nonsense.

This form of loss of integrity leaves the user with a digital persona that will be of no use and of no consequence.

A third kind of loss of personal integrity is the case where a name is associated with defamatory material of some kind. This is an implausible attack but it could consist in someone entering your name in the meta-information in porn-related web content or perhaps associate you with a crime in some manner that is simply false and defamatory. This attack is conscious and aims at crowding out legitimate hits in order to ensure that your digital persona gives a defamatory impression.

A malignant version of this is what has been termed a Google Bomb (Horowitz 2007). The idea behind this concept is that someone widely uses discussion boards and other websites to link an individual’s name to something else than that individual or even to something denigrating.
Are there possibilities to address noise attacks today? Are there “noise crimes” in the sense that we can see the criminalization of such attacks on personal integrity we have examined?

The European data protection directive is, as noted, based on a management/processing model that includes all processing, whether trivial or not, to be contrasted with a more narrow abuse model advocated by some Member States today. An abuse-model is based on regulating the processing of data where there is actual and relevant harm, rather than endorsing a regime where all processing of data has to fulfill certain requirements, no matter if there is actual or potential harm.

Are there, then, rules in the data protection directive which address the issue of personal integrity? The closest we come to such rules are rules governing data quality. Article 12 in the directive states:

Article 12

Right of access

Member States shall guarantee every data subject the right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:

-confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

-communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,

-knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

Note points b and c, which come close to a legal obligation to ensure that a data subject’s personal integrity at least is validated as to veracity, even if it is not validated in terms of relevance.
The directive says nothing about updating (although it can be assumed that data wildly out of date would be considered data that could be rectified), and it is hard to see how these rules could be applied to, for example search engines.

What would this mean in practice? Assume that someone has published defamatory information about a user, and that the user’s personal integrity has – as a consequence – been harmed. The user has found legal recourse and forced the original publisher to take down the original content. A large search engine, however, still caches the content and thus continues to disrupt the personal integrity – the correct, relevant and updated information about – the individual in question. In principle there then exists a right for the individual to rectify the erroneous data, even if it is hard to see exactly how that would work in practice.

In criminal law a number of different provisions may arguably be said to protect personal integrity – wholeness and relevancy – of an individual’s digital persona.

Firstly, the different provisions of libel apply to the web as to any other medium. The challenge here, however, is to find the source of the libel. Can a search engine be guilty of libel if it has only picked up what somebody else has written? Search engines index automatically, social networking sites like Linked In are filled in by the individual himself and it seems hard to argue that a libelous digital persona would be something that service providers would have to answer for, since there is no criminal intent.

(This does not, however, imply that there is no legal obligation to take down information that has been found to be libelous, but this is a side issue.)

Other provisions in criminal law that may apply to the idea of personal integrity are for example the provisions on different kinds of fraud. It may, in fact, be a crime or an element in an criminal act, to doctor your digital persona so that it makes it possible for you to defraud somebody else.

This illustrates something that is perhaps not surprising, but should be added to our discussion for the sake of completeness. Personal integrity can sometimes be destroyed in a way that benefits the individual. Demolishing and hiding a reputation for fraudulent behavior may well require destroying your personal integrity, but it does not necessarily harm you.

In addition to protecting privacy we may have to protect personal integrity as well. But the choice of pronoun is deceiving. Who is this “we” that has to protect personal integrity? I have used the idea of a digital persona here to illustrate a point, but it is a point that offers little or no guidance in designing new policy responses.

39 The relevant legal locution here has become “notice and take-down”. 
One possibility would be to offer identity services, where the integrity of an individual is guaranteed. Individuality or identity services would give out personal information without discrimination, but only that information that had been chosen and carefully reviewed by the individual in question. Such identity services would of course imply interesting problems – how would veracity and completeness be ascertained?

One example is the birth of new companies like Reputation defender that promise to help you clean up your digital persona.40 There is an embryo of such identity services in social networking services like Facebook, LinkedIn and MySpace. These services are identity constructing tools where I can choose to build my identity and reveal myself as I am. But even these structures can break down and become worthless.

Researcher and writer danah boyd describes acutely how she “lost context” in Facebook (boyd 2007):

Le sigh. I lost control over my Facebook tonight. Or rather, the context got destroyed. For months, I’ve been ignoring most friend requests. Tonight, I gave up and accepted most of them. I have been facing the precise dilemma that I write about in my articles: what constitutes a “friend”? Where’s the line? For Facebook, I had been only accepting friend requests from people that I went to school with and folks who have socialized at my house. But what about people that I enjoy talking with at conferences? What about people who so kindly read and comment on this blog? What about people I respect? What about people who appreciate my research but whom I have not yet met? I started feeling guilty as people poked me and emailed me to ask why I hadn’t accepted their friend request. My personal boundaries didn’t matter - my act of ignorance was deemed rude by those that didn’t share my social expectations.

In a sense this is also a loss of personal integrity, and one that increases the noise in our existence. The inability to keep social filters intact is another aspect of personal integrity that needs to be examined more closely. It also hints at another emerging interesting theme, examined by boyd, where the concept of identity is changing rapidly. Many users now have several identities or proto-identities in different situations and the number of identities is multiplying quickly. Returning to Mead’s concept of the self as constructed by others it would be reasonable to say that there are more identity construction grounds today than ever before.

The autonomy of individuals is dependent on personal integrity. There is thus a clear relationship between “decisional privacy” in Rössler’s sense and the idea of personal integrity – the ability to choose autonomously depends on a certain level of personal integrity. On a more philosophical level it can be asked what an identity, or a digital persona, really is. Is it merely a set of search results pertaining to an individual? Or can it be classified as some kind of intellectual property?

---

Consider a carefully crafted persona, or identity, which contains a number of complex and interesting descriptions of an almost fictional nature. Why should such an identity be exempt from intellectual property protection? There seems to be no natural or ex ante reason to assume that identities are not works of intellectual property.

If an identity or a digital persona is thought to be a work, and protected by copyright, the integrity of the work would be protected by the moral rights. This construction is actually worth examining in closer detail, since it offers an interesting regulatory model of how personal integrity could be handled.

The moral rights, as designed in the European Union, provide a right for the author of a work to be mentioned and to have the work attributed to him or her. The moral rights also, however, contain a right not to have the integrity of one's work destroyed. This right could be used as a template for constructing legislation protecting personal integrity.

Article 6bis states:

(1) Independently of the author's economic rights, and even after the transfer of the said rights, the author shall have the right to claim authorship of the work and to object to any distortion, mutilation or other modification of, or other derogatory action in relation to, the said work, which would be prejudicial to his honor or reputation.

An alternative regulatory regime for privacy – based on an abuse model rather than a processing model41 - could be designed starting with article 6 bis in the Berne convention. By merely changing a few words, the end result becomes an interesting starting point for such a regulatory reform:

(1) The data subject shall have the right to object to any distortion, mutilation or other modification of, or other derogatory action in relation to, his personal integrity, which would be prejudicial to his honor or reputation.

Note that the rule would protect honor and/or reputation and thus focus on any detrimental effects to the autonomy of those who have their personal integrity violated. What would be needed to accompany this rule would be a rule to guarantee a simple process of objecting to any such distortion, mutilation or modification of one's personal integrity.

While privacy, in the sense of a private sphere, is still an important theme in any discussion of what future society citizens want to live in, most would do well not to forget that entirely new problems arise in a society where the rate of information growth has exploded. In a society characterized by an excess of information the

41 These concepts have been introduced: abuse models concentrate on actual abuse and processing models on actual use and potential abuse.
consequences of being obliterated by noise is often more detrimental to one’s autonomy than regular privacy infringements. The old metaphor of a private sphere needs to be exchanged, and a new model of communication installed. Privacy is worth nothing if it does not enable us to communicate with others, grow a reputation and a persistent presence to act from.

Again, this is a challenge that the information society model does help us with. The distributed production of personal data in unstructured ways cannot be handled by a set of rules of thumb assuming control. The model fails.

**Examining the systematic bias of the failures**

What do the failures of the information society model in these chapters teach? Firstly, the model failed to cope with excessive creativity. Secondly, it failed to cope with out-of-control distribution networks or darknets. Thirdly, it failed to handle the excess of production of personal data and fourthly, it failed to address the need for integrity in a society where information scarcity is replaced by abundance.

The failures consistently are failures in control. But what kind of control is it that becomes hard to enforce? And why? We need to re-connect the analysis of how the information society model fails with the theoretical foundations presented earlier. The main explanation for the failures exhibited in this chapter is based on the small-scale autonomy of technology. Remember the diagram:

![Categories of Social Change](image)

*The failures indicate a consistency in what kind of social change is occurring*
Creativity has blossomed because of the enormous growth in supportive technologies: computers for writing and making music, digital cameras, mp3-recorders and video cams – all these small-scale technologies are producing a wealth of information today. They are not *individually* autonomous (no digital camera takes pictures on its own), but the macro-effect of their use, the spontaneous order generated by them (photo sharing web sites, amateur press photography, photo communication), is autonomous in the sense that it is not controlled centrally by any one person.

File-sharing networks exhibit small-scale autonomy and are spontaneously ordered. The data retention of society is a phenomenon directly related to the sinking costs of storage, allowing everyone to own a piece of retention technology and the disintegration of identities can be traced back to a multitude of information producers, using technology to communicate about each-other.

The way the model fails indicates that the social change expected is change of type B, where society is ordered spontaneously and small-scale technologies – individually controllable, but collectively autonomous – contribute to change. The systems are autonomous, not controlled, and that allows us to identify the society the new model should be designed for.

Previously I have presented both Bell’s information society, or post-industrial society, as well as the information society model that we have been able to find in the policy documents of the European Union. They resemble each-other closely; both dominated by a theme of control. The salient difference between them is that the European documents imagine this theme of control as something that chiefly applies to the technological element in the economy. With technology we can choose what to do and how to do it. But this choice is framed as a choice taking place on a free and open market. Bell, on the other hand, seems to have had a more consistent view where technology and economy were both systems that would be brought under control as a consequence of the technical developments.

This model fails, however, in at least the two important fields that I have studied. Privacy and copyright continues to pose significant policy challenges that the model does not seem able to manage. These failures indicate that the social change we as a society are experiencing is one where spontaneous orders arise as a consequence of the wide-spread dissemination of small-scale technology that becomes autonomous.

If this is the *mode of change*, what kind of *societal model* should we then expect? The answer is a society characterized by autonomy and kosmos, by technics “out of control” and a spontaneous order. In this societal model the themes of control break down and are replaced by themes of autonomy – but not the large-scale autonomy of technological dystopias where a single system or machine detaches itself from our control. The new theme I will examine is a theme of small-scale
autonomy and spontaneous order. Returning to the simple categorization of societies, this is our “Society A”:

Categories of Societies

The new model should be a model of Society A.

What kind of society is this? And what new policy discourses will it lead to?
7. A new model – the noise society

Introduction
The old information society model is failing in a number of different cases. Not only in the ones reviewed in the previous chapter, but also in handling freedom of speech and other difficult policy questions where assuming control of information production, distribution and structure no longer is a successful strategy. Policymakers need if not a new, then at least a complementary model for cases where control is lost. The remaining chapter of this work will be devoted to outlining how such a model could be designed, and what discourses it may lead to.

What, then, do we call the society indicated by the failures of the information society model? It is a society where technology is autonomous and order spontaneously organized. It is a society where small-scale technologies allow for the rich production of media and content as well as for dissolving control over distribution networks in different ways. As has already been hinted at it is a society characterized by noise rather than information.

This society – I call it the noise society – is one where information is produced predominantly by individuals, where structures are temporary and distribution uncontrolled. It is also a society where the value function does not hold. It is a society where more information is better, but only to a point, when it becomes a cost. Information overload leads to a collapse in value, to noise externalities and costs.

I think that it may be useful to review some of the statistics that I think support this idea of a noise society. Note that this is not an attempt to prove anything. It is just a way of framing the concept of the noise society with reference to some statistics.

It is natural to start our investigation with the Berkeley-study How much information. The researchers behind this study “estimate that new stored information grew about 30% a year between 1999 and 2002”, which would mean
that the amount of digitally stored information doubles every three years (Lyman and Varian 2003). The total amount of data produced in 2002 is assessed as five exabytes new information, and the total available data flowing in communication channels like TV, the Internet and radio is estimated around 18 exabyte. Other findings from the study include:

The World Wide Web contains about 170 terabytes of information on its surface; in volume this is seventeen times the size of the Library of Congress print collections.

Instant messaging generates five billion messages a day (750GB), or 274 Terabytes a year.

Email generates about 400,000 terabytes of new information each year worldwide.

P2P file exchange on the Internet is growing rapidly. Seven percent of users provide files for sharing, while 93% of P2P users only download files. The largest files exchanged are video files larger than 100 MB, but the most frequently exchanged files contain music (MP3 files).

Bear in mind that these figures are from 2002. In a more recent report the numbers are even more staggering. IDC reports that (IDC 2007):

In 2006, the amount of digital information created, captured, and replicated was $1,288 \times 10^{18}$ bits. In computer parlance, that's 161 exabytes or 161 billion gigabytes. This is about 3 million times the information in all the books ever written.

Between 2006 and 2010, the information added annually to the digital universe will increase more than six fold from 161 exabytes to 988 exabytes.

Three major analog to digital conversions are powering this growth – film to digital image capture, analog to digital voice, and analog to digital TV.

Images, captured by more than 1 billion devices in the world, from digital cameras and camera phones to medical scanners and security cameras, comprise the largest component of the digital universe. They are replicated over the Internet, on private organizational networks, by PCs and servers, in data centers, in digital TV broadcasts, and on digital projection movie screens.

IDC predicts that by 2010, while nearly 70% of the digital universe will be created by individuals, organizations (businesses of all sizes, agencies, governments, associations, etc.) will be responsible for the security, privacy, reliability, and compliance of at least 85% of that same digital universe.

Note the last paragraph: if we needed data to corroborate that information production will not be centralized and that control will be difficult, we hardly needed better evidence than this. If we look at other recent phenomena like the growth of the blogosphere we find the same growth rates (Sifry 2006):
Today, the blogosphere is doubling in size every 200 days, or about once every 6 and a half months.

From January 2004 until July 2006, the number of blogs that Technorati tracks has continued to double every 5-7 months.

About 175,000 new weblogs were created each day, which means that on average, there are more than 2 blogs created each second of each day.

The recent 2007 figures show no significant decline (Sifry, Sifry’s Alerts: State of the Live Web April 2007 2007):

Technorati is now tracking over 70 million weblogs, and we're seeing about 120,000 new weblogs being created worldwide each day. That's about 1.4 blogs created every second of every day.

Technorati, a blog search engine, (founded by Sifry) has also found evidence of user tagging, distributed structuring of the net:

The explosive growth that we see in the Technorati index is mirrored in social media sites throughout the Web, including Flickr, YouTube, and the like. This shared phenomenon allows us to marry the wealth of information in our index with the wealth of that stored on social media sites across the Live Web through the shared construct of tags.

For the uninitiated, a tag is a category or descriptor that someone (often the creator) assigns to it. This descriptor literally hangs off the media that's published to the Web much in the same way a luggage tag hangs off your suitcase -- easily identifying the bag.

The bottom line: we're seeing explosive growth in the tags index. People are clicking on tags, people are using tags, Google features tagged media in its results pages. Tags adoption has become a phenomenon across the Live Web, and we are seeing a correlative explosive growth at Technorati. [...] As of February 2007, About 35% of all posts Technorati tracks use tags.

This is an interesting observation since one of the indicators of a noise society is that central semantics will break down, no centralized information structure will survive. Tags embody decentralized information models. And the growth of the blogosphere also shows clearly that the number of information producers is growing quickly.

Spam, another noise phenomenon, was thought to be stabilizing a few years back (Dunn 2005), but this summer was recently christened the “Summer of Spam” and reports now claim that close to 90 percent of all e-mail traffic is spam, and 11 percent of this is so-called PDF-spam (with attached PDFs) (Garretson 2007).

If we look at internet growth we also find staggering figures. The average growth of the internet in the years 2000-2007 is 225 percent (Miniwatts Marketing Group n.d.). Considering the fact that the share of information production, for example
blogs, that is Asian is still very small, it is no daring guess that information growth will continue.

This is, admittedly, what is sometimes derisively called “anecdotal evidence”, but as such it at least offers a backdrop for our discussions about a noise society.

In order to examine more closely how a noise society model could look I will now present first a grammar of information and noise – in order to show how these two concepts relate and how they move together in language. I will then introduce two examples of problems that exemplify emerging discourses in the noise society: discourse about filters and search. Finally the noise society model will be outlined in some more detail.
The grammar of information and noise

Defining information and noise narrowly or decisively is neither possible nor desirable. Both concepts are broad concepts that can only be mapped or sketched in a way that establishes family-likenesses between different uses of them, rather than a specific and precise meaning. In this section I intend to sketch the use of the words information and noise in order to flesh out the language games in which they both figure. Information relates to noise and vice versa. The concepts are not exactly opposites but their meanings are interconnected in surprising ways.

The purpose of this examination is to outline the multiple meanings inherent in the two concepts and to show how they can be understood in the rest of our analysis of the information society and the noise society.

Most definitions of a word as general as “information” will be weak. Even if not all theorists agree, it is even possible to argue that defining information more extensively than policymakers trivially understand it will limit the worth of the study undertaken. Doing so implies that the researcher aims to leave the broader understanding of the word, the fuzzy and undefined understanding of the word, in favor of an understanding that is precise but so narrow as to be useless to the policymaker. There is no single authoritative definition of information outside the limited realms of Shannon’s and Weaver’s information theory. What is offered here is rather a number of basic traits in the information concept that are useful to remember in the coming discussions.

Information is ordered, relational. The concept of information can be thought of as ordered data. Information is in some sense ordered in relations, data is raw. The concept of unordered information would then, in this sense, be meaningless and self-contradictory. This also implies that information is something complex and composed of many different small units. This is at least one of the more common interpretations of what is often referred to as the DIKW-hierarchy (data-information-knowledge-wisdom) in Ackoff (1989).

Information can be reduced to data. Other usages of the concept of information and data assume that data is information expressed or formally represented (Dahlbom and Mathiassen 1995, 23-46). This is partly a different usage – information is then something that needs to be represented in data to be accessible or usable in, for example, computer processing. Dahlbom and Mathiassen define information as an intermediary form between knowledge and data: knowledge is turned into information and represented as data (p 29).

Information is the result of interpretation. Langefors (1995) in his infological equation uses a definition of information where information is indeed structured data, but individually structured by an interpretation process. The equation is simple: \( I = i(D,S,t) \) – the information received is the result of the interpretative
process I working on data D with the existing knowledge S during time t. In this perspective there would be no information without interpretation. This view is slightly different from Ackoff’s in that Ackoff only seems to require relations between data to call something information. Langefors concept is richer, and more like Ackoff’s knowledge. Langefors extends his analysis to different other aspects and in some texts end up with an information concept that again seems to take data as the representation of information in signs, but not as information (p 108). Langefors’ concept seems not to put heavy emphasis on ordering or relations in sets of data.

Machines can produce information. Information can be produced by machines and other artifacts. Log files, automatic recommendation lists or simple error messages are information and they can be produced by machines. The reason this is important is that it explains how humans, with a scarcity of attention, is able to produce more information than humans can consume. The amplifying effect of information technologies allow us to produce immense amounts of information with very little or no attention as a basic input.

Information is a product, a commodity. Information is sold and bought. Information has value. How policymakers assess this value is an important part in understanding how they view the society they are responding to. Information brokers are important social figures in both the information society and the noise society.

Information is stored and communicated. The kind of information we will speak of here is not potential information or platonic information that could be conveyed from the world of ideas, but actual information that takes up space on digital storage mediums. The reason this is important to understand is that the quick decline in storage prices is an important driver in the growth of the information sets in society.

Information is a non-excludable and non-rivalrous commodity (Shavell 2004). This implies that consuming information does not reduce the amount of information around.

Braman (2006) in her work uses a similar enumeration and the definitions she highlights are: information as resource, commodity, perception of pattern (patterned data), agent (information is often depicted as acting, changing or otherwise interacting with society), basin of possibility (information is, she claims, in a sense a probability) and a constitutive force in society (Braman 2006, 12-20). Braman’s emphasis on information as an agent and a possibility highlights the diversified role information has actually come to play in policy making.

What, then, is *noise* and how does it relate to information? One very specific answer is given by the branch of mathematics known as information theory. According to a simplified interpretation of the model launched by Claude Shannon...
we could say that noise is anything that distorts or destroys the communication process (Shannon 1948).

**Simplified rendition of Shannon’s model**

Shannon describes two kinds of noise, distortion and noise:

We now consider the case where the signal is perturbed by noise during transmission or at one or the other of the terminals. This means that the received signal is not necessarily the same as that sent out by the transmitter. Two cases may be distinguished. If a particular transmitted signal always produces the same received signal, i.e., the received signal is a definite function of the transmitted signal, then the effect may be called distortion. If this function has an inverse — no two transmitted signals producing the same received signal — distortion may be corrected, at least in principle, by merely performing the inverse functional operation on the received signal.

The case of interest here is that in which the signal does not always undergo the same change in transmission.

In this case we may assume the received signal $E$ to be a function of the transmitted signal $S$ and a second variable, the noise $N$.

$$E = f(S;N)$$

The noise is considered to be a chance variable just as the message was above. In general it may be represented by a suitable stochastic process.
Shannon’s theory is a starting point but I need to expand the notion and concept of noise as to be at least as broad as that of the concept “information” in the combination the “information society”, and thus we will look at alternative definitions of noise below.

We could argue that noise is the effect of too much information and connect the concept of noise with the fairly straight-forward concept of information overload. The idea then is that at a certain point information sets grow so large as to become useless and they then collapse in on themselves much like black holes and become noise sets. One typical definition of information overload is found in (Jordan 1999, 101):

\textit{Information overload}

Having too much information can make use of information impossible. This can occur in two ways. First, there can simply be too much information to absorb. Second, information can be so poorly organized that finding any particular piece of information becomes impossible. (\textit{italics and formatting in original})

I agree with this definition in part. We could also devise numerous tests for when this happens to a specific information set, the most obvious of which is a simple economic one: when the cost of the time needed to locate the information needed exceeds the value of that specific piece of information a system has reached its breaking point and collapsed to noise. This noise “schwarzschild radius” is both subjective and continuously changing, but it remains a sort of litmus test available to anyone who wants to examine the concept closer.

Connecting noise with information overload in this way also allows us to connect it with Herbert Simon’s (1971) notion of attention scarcity. Simon famously noted that the only absolute scarcity is scarcity of attention, and when information grows as quickly as it does today we would need to prioritize heavily in consuming information. Our attention would then become the ultimate competitive prize for all actors in the information society (Simon 1971).

This definition is both operational and useful. It also has the advantage of ease-of-use, but we need to make a few qualifications before we can adopt it.

The perhaps most important qualification is that noise in this study will be treated as primary and information secondary. Information is filtered out of noise, refined from noise. The reason for this order of things is simple: we do not start out with an empty society. Society has been filled with information for ages, and is still being filled at a phenomenal rate with new information. That means that we do not run the risk of becoming victims of information overload, we have since long passed the point where information overload became a fact.

Indeed, it would be correct to say as Cary Wolfe does in his introduction to Michel Serres \textit{The Parasite} that “‘Noise’ is always already a part of the signal” (Wolfe 2007,
Serres’ work presents a fundamental vision of noise as intrinsic to any social system in a multitude of ways, and explores the notions of noise as a necessary component in creating meaning. Wolfe (2007) notes the close relationship with sociologist Niklas Luhmann’s (1984) analysis of noise in which Luhmann states that “[t]he difference between meaning and world is formed for this process of the continual self-determination of meaning as the difference between order and perturbation, between information and noise. Both are, and both remain, necessary”.

On a simpler level this is trivially true. With the rate of information production that we are witnessing, information overload occurred at an established, historical point and then noise became the default state of our society. The basic condition of our society is that it is mired and saturated in noise. We live in a sea of unordered data, another definition of noise, available to us everywhere. This is the new basic and general commodity of our age, more like electricity than anything else. And like electricity noise needs order and filters to function and produce value. This reversal of the order of information and noise is also the methodological key to asking questions about law in the noise society. Society, we will claim, is organized from noise.

One way of using this idea would be to speak of policy making as making sense of noise or extracting order from noise in different ways that are valuable to the members of society. Another idea is to follow Grimmelman (2007) in analyzing society has The Library of Babel and to discuss what regulation should apply to the librarians.

Another possibility is to treat noise as a negative externality in the economic sense of the word. This approach leads to interesting results. In his interesting paper Copyright in an Era of Information Overload: Toward the Privileging of Categorizers, Frank Pasquale of Seton Hall university suggests that it is possible to analyze noise or information overload as a classic case of pollution or as a negative externality (Pasquaule 2007).

Pasquale argues that information producers pollute and disseminate information so much as to create a negative externality, noise. This, he also claims, could be the basis for granting different categorizers (search engines, catalogues, wikis et cetera) exemptions from copyright based on fair use.

One way of extending this metaphor is to view noise as pollution of our shared information space. Polluters – information producers of different kinds – could then be held responsible under certain possible legal regimes and the idea of noise as pollution raises many interesting questions about the idea of a noise society as well as about the role of filters. Pollution is a powerful metaphor in addressing the noise society and as metaphor it is becoming more and more common (Nagle 2007).
Another possibility is to view noise as information that no longer has any value. We could argue that information gets its value from asymmetries between actors on a market and that once information is everywhere it rots or degenerates into useless noise.

Information available to everyone loses some of its competitive value. Some writers argue that this has given rise to a special brand of technologies or inscriptions that create friction to ensure that certain elites still can maintain information asymmetries to their favor. (MacKenzie 2002).

The idea that information that is accessible to everyone is worthless is based on the premise that we have an asymmetrical information advantage if we know what other actors do not. When information is symmetrically distributed between actors it would, according to this theory, lose its value and become noise.

Another useful perspective is offered by Mark C Taylor in The Moment of Complexity: Emerging Network Culture, where he traces the etymology of the word noise back to the Latin and shows that it has the same root as the world nausea, sickness. From this he then constructs a useful table of contradictory terms (Taylor 2001) p 101:

<table>
<thead>
<tr>
<th>Information</th>
<th>Noise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Difference</td>
<td>Indifference</td>
</tr>
<tr>
<td>Order</td>
<td>Disorder</td>
</tr>
<tr>
<td>Organization</td>
<td>Disorganization</td>
</tr>
<tr>
<td>Form</td>
<td>Chaos</td>
</tr>
<tr>
<td>Improbability</td>
<td>Probability</td>
</tr>
<tr>
<td>Negentropy</td>
<td>Entropy</td>
</tr>
<tr>
<td>Heterogeneity</td>
<td>Homogeneity</td>
</tr>
</tbody>
</table>

These terms can be used as endpoints in defining the conceptual space in which the concepts of information and noise move.

Taylor writes:

> When information becomes the noise that engenders nausea, distinctions, differences, and oppositions that once seemed to fix the world and make it secure become unstable.

This sense of loss of security is an important part of our definition of noise, since exactly this insecurity needs to be taken into account when formulating a legislative response to the noise society.

The most common use of the word “noise” is in denoting an auditory phenomenon, and the idea of “noise pollution” and noise destroying our society is taken literally by some. Sometimes auditory noise pollution is taken as an overall metaphor for noise in society and culture. In the recently published A Manifesto for Silence we find an interesting example of the auditory analysis of noise in society (Sim 2007).
We can extend this to technological design and examine how the opposite of noise technologies would look – how would *silent* technologies look?

A specific version of the idea that noise is information overload is the idea that noise is a part of what Pierre Lévy has termed “the second deluge” (Lévy 2001). Lévy succeeds very well in describing at least one aspect of the model I have in mind when thinking about the noise society – its incessant growth and persistence. He writes:

> The World Wide Web is a flux. Its innumerable sources, its turbulence, its irresistible swell provide us with a striking image of the contemporary flood of information. Every memory store, every group, every individual, every object can become a transmitter and swell the flood. [...] For better or worse this flood will never subside. We will have to learn to accommodate to its profusion and disorder. Aside from some cultural catastrophe, no sense of order, no central authority will be able to lead us back to the terra firma or the stable and well-delineated landscapes that existed before the flood. (p 140-141).

This is actually as good a description of the noise society as we can ask for. Lévy continues to make the salient point that in this flood our perspective is not the systemic, not one where we can access everything, but where we will have to choose what to *save*.

> What should we save from the flood? To assume that we can construct an ark that would only contain the most “important” items would be to yield to the illusion of totality. (p 141)

And finally, Lévy also notes that the main metaphors we need to analyse this society are not “global systems” or “information access”, but rather navigation and filtering (p 224). The world Levy describes is that of the ciborionic bricoleur, tinkering and tactically saving some information here, employing some technology there in improvising negotiations in policy making.

In Levy we find the sense of change and instability that I think is one of the more important, general characteristics of the noise society and his work gives an important contribution to the overall understanding of the concept noise.

With this exploration of the grammar of information and noise we have set the background against which we can begin to approach the concepts of both information society and noise society and put some flesh on the bones of “Society A” suggested in the theoretical foundations.

**Filters**

The filter metaphor is a powerful metaphor for policy instruments in the noise society. In a noise society policy makers would do well to examine different filters closely in order to understand how they distribute power and how they make policy. As witnessed in the study of noise tactics, filters can develop to a degree that almost ensures the noise resilience of a system or a network. Filtering out the
irrelevant from our digital personas is another kind of defense against getting lost in the noise when one doesn’t want to disappear.

Filters of different kinds – then – become the instruments of choice for a policy maker in a noise society. But what are they? How do they work? How do policymakers evaluate them for democratic and legal values? These are the questions I will now look into, in order to show how an emerging discourse could look. In answering them we will have accomplished the task set out for the thesis: we have established that many policy responses have been designed with an information society model in mind, and we have established that another model, the noise society model, may give us a different perspective and explain failures of certain early policy responses (guiding us towards other solutions, specifically filters).

With the analysis of filters as policy instruments we can then finish with recommending that policy makers at least use the noise society model and evaluate filters as policy instruments in future policy making.

Another interesting possibility is to use filters as a legal sanction. If we, for example, allow a court to hand down decisions in which the implementation of filters is demanded, we offer the court a powerful way of rebuilding architecture.

There are some indications that this has been tried. Look, for example, at the interesting case decided in Australia a few years back, where the court decided that Kazaa must be adjusted with a filter that enabled filtering out copyrighted materials (Smith 2005). Sharman Networks appealed and the case settled with Sharman paying damages at an undisclosed amount thought to exceed US$ 100 million (Clune and Kocemba 2006).

This kind of ruling is powerful, but also very hard to follow. It requires not only rewriting the code, but it also requires getting everyone to update their software – something that is immensely hard. Kazaa was to be re-distributed with a non-optional list of keywords, and of course this never worked – the actual effect on file-sharing technologies was scarce if any (Deare 2005).

The chapter begins with a general definition of filters, and I then move on to two policy fields where filters have been used for quite some time: regulating harmful content and spam. The reason I want to review these fields is that they offer lessons for understanding how filters work as policy instruments and the risks involved. After having examined how filters are used in combating spam and harmful content I try to formulate a general framework for analyzing filters and apply it to two different filters, in order to show how policy makers could begin analyzing filters.

Filters, here, will be defined as any kind of instrument or function that takes a certain set of information (or noise) and produces another smaller set of information.
This is an extremely broad definition. The reason for defining filters so broadly is that the essence of the filter is exactly this – they extract, manipulate, order, select, transform or create information for us in different ways. Let’s look at some examples of filters:

- Search results filter out what is relevant for us using different methods and algorithms.
- Social networking sites filter out contacts and allow us to select and filter our contacts (in LinkedIn according to business sector for example).
- Blogs filter information and aggregate it in different ways, as do RSS-readers.
- Wikis filter collaborative knowledge production.
- Recommendation filters filter out products for us to buy based on preferences.
- Spam filters manage the flow of e-mail.
- Content filters protect different groups identified as vulnerable or censor information for others.
- Digg and other sites filter news for us using recommendation filters.
- Mash-ups filter different information sources into new ones, selecting information sets and combining them for us to use.
- LastFM.com and other social radio services filter music for us to listen to according to our tastes and the tastes of others like us.

Filters are policy instruments that draw upon the strengths of both architecture regulation and legal responses. They are governed by rules and they are embodied in architecture.

There is a fundamental difference between technological responses that aim at total control and those that aim at filtering. We can live without control. The control implemented in PETs or DRMs is not an essential, necessary component of a system. But all information systems have to filter in some sense or another.

Another way to put it is to work with the notion of alignment (Gillespie 2007) or compliance Wu (2003). DRMs are not aligned with the usage inscribed in entertainment products. Users want to listen to and share music, so when someone tries to protect a song they come into conflict with the intended use, with the script of the entertainment product. Users then choose not to comply with the scripts.

But filtering is aligned with most products and most services. Even in file-sharing applications users want to search and filter out materials they need from those that they do not want. In looking for personal information users filter, search and collect information in the same complex act of privacy invasion. I run the risk of becoming metaphysical (in a bad sense) here, but filtering is a part of how users must interact with the noise society. We can only interact through interfaces that in
some sense filter, we must comply with some kind of filter. That is why policymakers need to examine filters closely.

Filters are sometimes analyzed as instruments of censorship and this is another way of approaching the problem. Since I have assumed a noise society, filtering is necessary and I will treat censorship as a special case of filtering. For a more complete discussion on access, censorship and autonomy see Klang (2006) pp 184-204.

The battle against illegal and harmful content on the Internet is as old as the Internet itself. No sooner do societies offer information distribution possibilities than someone uses them to distribute what some argue is harmful, improper, wrong, dangerous or just plain stupid.

There have been numerous policy responses to this tendency, and some of them have included filters in interesting ways. The most radical form of filtering seen so far, I think, is the idea of splinternets. The idea, originally launched by Clyde Wayne Crews at the Cato Institute (Crews 2001), was that citizens need more than one Internet since there is so much disagreement about what actually constitutes harmful content. Extending Crews idea suggests a scenario in which the Internet fragments into several different networks, or splinters of a network (splinternets). In part this could be said to be what is happening with the national filtering we see in countries like China and Saudi-Arabia (Bambauer, et al. 2005, Zittrain and Edelman, Internet Filtering in China 2003, Zittrain and Edelman, Documentation of Internet Filtering Worldwide 2003).

These two latter examples point to one of the major difficulties with using filters as policy responses. Choosing what to filter is not as simple as one may think. Filtering rules for harmful content are hard to agree on globally.

Technological solutions range from the settings available in Internet Explorer 7.0 to advanced filtering technologies like Cybersitter. The latter technologies are often termed censorware, and the difference between censorware and filters is that censorware is a subset of filters that are designed for “one person to use on another person” (The Censorware Project 2004).

Filters have been a semi-useful way to stop the dissemination of harmful content. In fact, the filtering provisions for libraries was the only part of the reviled Common Decency Act in the US that actually survived as the Supreme Court struck down all other provisions in the act. Some of the filters have succeeded fairly well, others are easily circumvented.

In this context one must mention PICS – the Platform for Internet Content Selection (W3C website 2005). PICS was a model, devised around 1997, for content-labeling that encouraged self-regulation. It was designed to enable web site owners to signal that a certain “signer believes statement about information resource”. This
sounds innocent enough, but the filtering data models it would allow would be quite powerful. Witness the following excerpt from a data model envisioned by Safe-Surf, a parental organization, that had “established a rating system that is used for self-rating by a large and growing number of sites on the Internet. They have provided a machine-readable version of their service to PICS as a demonstration of a more complex rating system that includes sub-categories as well as a document classification system. The following specification includes a full description of the rating part of the SafeSurf system, with only a small stub to represent the classifications.” (Rating Services and Rating Systems (and Their Machine Readable Descriptions) 1996):

(category (transmit-as "SS--002") (name "Heterosexual Themes")
(label (name "Subtle Innuendo") (description "Subtly Implied through the use of metaphor") (value 1))
(label (name "Strong Innuendo") (description "Explicitly implied (not described) through the use of metaphor") (value 2))
(label (name "Technical Reference") (description "Dictionary, encyclopedic, news, medical references") (value 3))
(label (name "Non-Graphic-Artistic") (description "Limited metaphoric descriptions used in a artistic fashion") (value 4))
(label (name "Graphic-Artistic") (description "Metaphoric descriptions used in a artistic fashion") (value 5))
(label (name "Graphic") (description "Descriptions of intimate sexual acts") (value 6))
(label (name "Detailed Graphic") (description "Descriptions of intimate details of sexual acts") (value 7))
(label (name "Explicit Vulgarity") (description "Explicit Descriptions of intimate details of sexual acts designed to arouse. Inviting interactive sexual participation. Unsupervised Sexual Chat Rooms or Newsgroups") (value 8))
(label (name "Explicit and Crude") (description "Profane Graphic Descriptions of intimate details of sexual acts designed to arouse. Inviting interactive sexual participation. Unsupervised Sexual Chat Rooms or Newsgroups") (value 9))

(category (transmit-as "SS--003") (name "Homosexual Themes")
(label (name "Subtle Innuendo") (description "Subtly Implied through the use of metaphor") (value 1))
(label (name "Strong Innuendo") (description "Explicitly implied (not described) through the use of metaphor") (value 2))
(label (name "Technical Reference") (description "Dictionary, encyclopedic, news, medical references") (value 3))
(name "Non-Graphic-Artistic")
(description "Limited metaphoric descriptions used in a artistic fashion")
(value 4))
(label
(name "Graphic-Artistic")
(description "Metaphoric descriptions used in a artistic fashion")
(value 5))
(label
(name "Graphic")
(description "Descriptions of intimate sexual acts")
(value 6))
(label
(name "Detailed Graphic")
(description "Descriptions of intimate details of sexual acts")
(value 7))
(label
(name "Explicit Vulgarity")
(description "Explicit Descriptions of intimate details of sexual acts designed to arouse. Inviting interactive sexual participation. Unsupervised Sexual Chat Rooms or Newsgroups")
(value 8))
(label
(name "Explicit and Crude")
(description "Profane Graphic Descriptions of intimate details of sexual acts designed to arouse. Inviting interactive sexual participation. Unsupervised Sexual Chat Rooms or Newsgroups")
(value 9))

The example shows what this standard could actually do in differentiating content and labeling it. The distinction between homosexual and heterosexual content is in itself enough to raise the liberal eyebrow. Note also the subtlety in content labeling that takes into account “[m]etaphoric descriptions used in a artistic fashion”.

PICS was heavily opposed by writers who argued that the effect would be to make it much easier for governments to impose filtering on citizens. If there is a standard for labeling, and a filtering technology to use that standard, the end result will be increased governmental control. We may add to this that it presumed a level of compliance, to speak with Wu (2003) that is unlikely. The alignment required within the policy space for a standard such as this to succeed is complex and improbable.

Early reactions to PICS were, as I’ve indicated, quite negative and harsh (Lessig, What Things Regulate Speech ver 3.01 1998), but the chief-designer, Paul Resnick, maintained that PICS was a valuable contribution to ensure individualized filtering rather than centralized filtering. Resnick wrote one of the first articles advocating filtering on the Internet (Resnick 1997) and in his FAQ on PICS he advocates the position that any common filtering standard offers the individual control over content filtering, which is superior to centralized control (Resnick 2002).

Ideas of filtering and labeling content have been around for quite some time, but most models – PICS included – have relied on a notion of a top down standard or a centralized solution. The power a filter affords its user is a crucial part of the analysis of the filter. The PICS-solution did succeed with a stunning feat of alignment, however, in the hands of the Recreational Software Advisory Council (RSAC). The organization developed a rating system called RSCAi and convinced Microsoft to implement it in their popular browser Internet Explorer (Slevin 2000, 226-229).
Other examples of content-based filtering are special wikis, designed for certain ideological perspectives. One such example is the Conservapedia – an attempt at a Wikipedia-like solution but with views adapted to a certain brand of conservatism. The web site explains (Conservapedia: The Trustworthy Encyclopedia 2007):

Conservapedia is a Wiki-based encyclopedia coming from a conservative point of view, and does not pretend to be neutral, but does strive to be accurate and fair, and allow other points of view. It is also designed to be a useful resource for students and therefore a family-friendly one, which means that some topics will not be allowed.

Content-based filtering like this illustrates the problem with defining what harmful content actually is.

Another example of a filtering discourse is spam. Spam is not a well-defined concept. Spam is the noise of the network, unsolicited communications, junk mail and a vehicle for fraud and porn. Spam has been called everything from legitimate marketing to rape.42

Different proposals for laws have been introduced on a broad basis. In the US there is a wide variety of laws.43 The European Commission has introduced provisions in the reformed telecommunications regulation package and in the new directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) the new provision clearly states that:44

The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.

The first and most basic question that must be answered in dealing with spam is of course definitional. What is spam? Is it only unsolicited commercial email, as some organisations would prefer to define it, or can other classes of information be included in the concept as well? This is the first problem any policy response involving filters has to ask: what is the set of phenomena to be filtered? There are different theories:

42 See (Mann 2000). Mann defines spam as a crime and says that the closest we come is “Rape ("spam") the victim through unwanted informatic insemination. This Rape (spamming) involves the violation of the victim’s solitude, peace, or “right to be left alone”.”

43 See for an overview SpamLaws (http://www.spamlaws.com[2003-04-05])

44 Article 13 aforementioned directive.
• **The content based theories.** Content based theories of spam focus on the content of the messages. One possible avenue of attack is to state that all messages that contain commercial information (yet another concept that then needs to be qualified) and that have not been solicited are spam. Another possibility is to restrict the concept of spam to messages the content of which is aimed at defrauding or tricking the user in some way.

• **The sender based theories.** Another definition of spam would instead focus on who sent the e-mail. If the sender is a commercial party, and if the sender has no prior relation to the receiver, this set of theories might prefer to term the message spam on the basis of this simple fact.

• **The value based theories.** These theories focus on the effect and simply state that spam is any message that reduces the value of the network as a communications medium. Not only commercial messages are included in this definition, but also mass-mailings of hate speech or meaningless information. Spam in these theories equate with noise.

In choosing between the different theories we must try to find a definition that allows us to address the issue in a way that gives clear and quantifiable measures of the damage done by spam. From this reason it may be recommendable to work with the third category of definitions, the value based definitions, since this also legitimises the discussion of the spam problem in terms of pure economic damage, and it allows us to merge the discussion of spam with the discussion on architecture regulation and cost structures.

Policy makers have tried to regulate the spam phenomenon in several different ways. Among the more common policy responses the following categories can be found:

• **Legislation.** As shown, this form of regulation takes as its starting point the idea that legal provisions against spam (any definition of spam) will be used and then enforced.

• **Self-regulation.** The industry is encouraged to set up codes of conduct and frameworks for dealing with spam on their own.

• **Architectural regulation.** By using and modifying the basic architectures of the Internet some argue that we can eliminate the problem of spam.

It is, however, important to realise that here it matters that the concept of what spam is, is a moving target. In the first request for comments (RFC) in the Internet Engineering Task Force where unwanted e-mail was discussed back in 1975, the idea of what the problem might be was slightly different from the one we are dealing with today. In this spam teaches us something important about noise: noise is not a static set of data that can be filtered out, it lies in the very nature of
noise to be context-dependent. What is noise in one setting is not necessarily noise in another.

The externalities and costs of the spam-market – if indeed we can speak of such a market - are easily found in the reduced value of the Internet, and e-mail in particular, as a communication medium. Spam, or the noise it reduces to, lowers and erodes the value of e-mail as communication medium, and thus also as a marketing medium (Ayres and Funk 2002).

The user is forced to sift through and filter his or her emails to find the relevant and informative content. The time this takes is crucial in understanding the costs of spam. One can even construct a breaking point or noise point: when the value of the content and communication in e-mail systems is less than the value of the time needed to sort and search these same communications, it will be rational to abandon this type of communication, or re-design the systems as not to allow do much noise.

Architecture regulation through filters of different kinds have proven to be the most efficient policy response to spam. There are many different filtering solutions and it is instructive to look at how they have been designed. Blacklists are simple to use, and they are interesting constructions. In principle the idea is trivial. Take all the senders that are caught sending spam and put them on a list, then share that list between you and stop all e-mail from these senders.

There are several interesting problems connected with this approach, however.

*What level of sender?* It is possible today to block not only a given e-mail address such as nicklas_lundblad@hotmail.com, but also to block an entire domain: hotmail.com. What level is suitable for a blacklist, and how can it be tailored to eliminate spam, but ensure that legitimate e-mail gets through?

*What level of block?* Should the blocks be implemented on global network level (and how, if that is the case?), Internet service provider level or user level?

*What process?* If policymakers decide to set up a blacklist we will have to decide to set up a process for getting on the list, and probably also for getting of the list. Who will decide who gets on the list? Who gets off? Will there be attempts at due process? In one intriguing example the MAPS RBL has published its process online to enable those who want to report someone or get off the list to follow what is essentially an entrepreneurial justice system. See (http://mail-abuse.org/rbl/candidacy.html[2007-04-05]) Read what they write about the process: “When a professional spammer gets a leased line, we find out about it when they start spamming us, and we track down every network object they own and we blackhole all or nearly all of them. Mail servers, web servers, name servers, terminal servers, usenet servers -- everything. If a professional spammer owns it, we don’t want it talking to us, no matter what the protocol. When an ISP sells a
shell account to a spammer, we try hard to reason with the ISP. Please disconnect them and strengthen your AUP, we often say. Go to hell you fascist censoring dog! and Stop whining, a little spam won't hurt you are the usual replies. Welcome to the MAPS RBLSM is our final statement in that kind of conversation. But note: we try."

These different choices vary among the different blacklist providers. The end result is that there is a market of technology solutions competing to become architecture solutions right now. The actors on these markets are internet service providers and blacklist providers. The filtering is almost always done on ISP-level, and the blacklists are chosen in many cases by the ISPs. There are comparisons of blacklists available on the Internet for anyone interested in the relative functionality of these technologies. The overall impression of these comparisons and studies is indeed that they reduce the amount of spam received. Over time, the blacklists have been forced to evolve. In a fascinating history of blacklists in general and one blacklist specifically, MAPS RBL, we find the following description:

The original focus of the RBLSM when it began operations in mid-1997 was on identifying the sources of dedicated, professional spammers. Over time, the success of the RBLSM forced abusers to resort to other channels for distributing spam such as third party relaying and direct-to-MX contacts.

These countermeasures to our defenses, as well as newly emerging sources of abuse have made it necessary to modify our own strategies in response. We will describe the RBLSM strategies in its earliest days before discussing the more recent and more insidious forms of e-mail abuse MAPSSM is attempting to control.

It is worthwhile to note that the blacklists are being followed closely by the spammers, and that this is as much an arms race in digital design as the copyright situation.

Whitelists are simply the reverse of blacklists. They are filters that offer the user the opportunity to set up lists of accredited senders and then only accept e-mails from these senders. The simplest way is to filter at user level(Oskoboiny 2000). Whitelists are the reversal of the open architecture of the Internet in many ways, and there is some work being performed to formulate standards in this area.

Another possibility is to construct a white list that contains some extensions. By including social network analysis it is possible, for example, to have a whitelist where I can set the a threshold in my network beyond which I will not accept e-mail. I may accept e-mail from friends and friends of a friend, but stop at this second circle of friends. These technologies – friend of a friend (FOAF) – are promising to let us design filters that mirror our social networks (Brinkley 2001).

45 See Blacklists Compared (http://www.sdsc.edu/~jeff/spam/cbc.html[2003-04-05])
Other social filters developed in research assign importance to senders and can have messages filtered according to roles in an organization or perceived importance of a customer, for example.

There are many combinations, other solutions and technologies available for trying to eliminate spam. Among the more popular we find SpamCatcher and SpamAssassin.

There are also a number of interesting research projects on tools and technologies for eliminating spam. Research on reputation based filtering is one promising avenue of development (Damiani, et al. 2002).

If filtering harmful content showed that filters are both legal and technological phenomena, it should be realized when looking at the spam wars that the organization of the entire administration of filtering mechanisms is an extremely important part of the design of filters as policy responses. Filters exist in an administrative context and they flourish as such.

Spam filters of different kinds are examples of filters that have develop their own rule systems. The rules around getting removed from blacklists, for example, are often reminiscent of the rules governing public authorities. There are requirements for due process, notifications and other similar rule sets. Witness the attitude of the MAPS RBL and others and how filtering evolves into a tool for exercising power – we need to have mechanisms and routines in place that put checks and balances on any filtering policy instruments.

In many different papers, books and newspaper articles the issue of censorship on the web is discussed, and there are many academic projects seeking to ascertain just what is censored and by whom. Censorship is not solely a phenomenon in dictatorships. Some go so far as to state that current application of copyright law amounts to a form of censorship and that it often has a “chilling effect” on both innovation and exploration. Others speak about censorware and claim that any kind of software that limits access for someone on the account of somebody else is a kind of censorship.

But what is the alternative to filtering or even to censorship of different kinds? What would a completely unfiltered version of the Internet look like? Could we even imagine what that would be? Is it not in fact necessary for us to create filters under the onslaught of information growth to be able to cope with the growing amount of noise in our information systems?

It would probably be hard to use the internet without filtering, and in some cases users may need others to set up our filters for them. Users may still be free to change them, but they may also lack the ability and knowledge required to do so. Again the default settings exercise their silent power over users.
How, then, do policy makers evaluate different filters and their legitimacy? It seems clear that there is a need for an analytical model for examining and analysing different filtering regimes, at least if policy makers have the ambition to use filters as policy responses in different situations.

In a noise society policy makers have to discuss the need for filters and suggest a framework for evaluating the legitimacy of a filter. Here I will examine two different kinds of filters and suggest a general model for evaluating filters of different kinds.

The first filter I will examine is the filter used by many (but not all) Swedish ISPs to filter out web sites with child pornography. The second filter is Akismet spam, a simple spam filter for WordPress.

The architectures of search, categorization, storage, linking and manipulating information regulate. As Lessig (1999) has shown the design of architecture is a powerful regulator, and so much the more so in a society that is under the constant risk of information overload. All the information in the information society is in a sense mediated through these architectures. The way they index, find and tag information will be the major factors in deciding what is actually possible to access for citizens and companies.

These architectures are filters in my definition. They are in a sense the means of production in the information society: they produce information out of noise, out of the uncategorized and unordered bits of data flowing around in the global networks.

Filters have here been described as functions that produces a (smaller) set of information a out of the information set b, and the resulting formal description has some value for the discussion of filters, so I will employ it where necessary (without claiming anything else than clarity).

In Sweden child pornography has been banned with powerful legislation. Even if there has been some debate about this, the overall impression of following the debate is that opposition is weak or non-existent. The reason, of course, lies in the nature of the crime: the sexual abuse of children is not perceived as something anyone wants to protect or defend in the least, even if it demands a law that may be seen as a limitation on freedom of speech.

Policy makers give the benefit of the doubt to those who fight child pornography in legislating. This benefit, however, has now been extended to a most peculiar construction: that of a special contract between some internet service providers in Sweden and the Swedish police.

The contents of this contract are said to specify that ISPs will willingly block access to a list of web sites. This list is compiled by the police and distributed to the
signatory ISPs. The contract is interesting to examine in detail, since it sets out the rules around one of the most extensive public-private filtering programmes in the world.

The contract starts with a paragraph setting out the background and idea behind the collaboration:

This cooperation project lays down rules for cooperation between the National Criminal Police (henceforth abbreviated NCP) and the Internet Provider in order to restrict the commercial distribution of documented sexual abuse of children. The aim is to regulate the actions of the Internet Provider and to ensure that computer contents do not go astray. It must be emphasized that this agreement cannot be extended to include any other Internet contents, illegal or not.

In any legal analysis this sounds extremely strange. What is actually meant by the second paragraph? Why should the police ever need to contract with someone about illegal content?

Contents of the contract are described in the second paragraph:

The agreement includes the NCP lists of Internet addresses which the NCP has identified as containing documented sexual abuse of children and where the distribution is illegal under Swedish law as well as payment functions if exclusively intended for the purchase of such material. It shall not be for the Internet Provider to decide whether or not the material is contrary to Swedish law but only to act in accordance with the criteria of judgement adopted by the NCP in this regard.

The agreement is quite broad. The rest of the contract contains rules on contacting the internet service provider and the appointment of contacts at the RKP. The actual list is then transferred to the internet service provider in encrypted format. When the contract comes to the responsibilities of the RKP these are listed as:

The NCP undertakes to:

Transmit updated lists to the Internet Provider. The blacklist is updated frequently and promptly due to the inflow of new information to the NCP.

Verify and confirm that the blacklist refers exclusively to addresses making accessible documented sexual abuse of children which are in violation of Swedish law, and addresses with payment functions, as defined under the heading Contents of Agreement.

Store documentation showing or explaining the reason for entering an Internet address on the blacklist. All assessments as to what material should have access

---

46 Note that the version of the contract I have has not been verified as the correct one by the police, but by someone at one of the participating ISPs.

47 The translation kindly provided by Patrik Hiselius at TeliaSonera.
blocked are made by the NCP. The Internet Provider can choose to publicize this fact on their home page or similar or in any other context.

Encrypt the list in accordance with agreement under the heading

*Transmission of blacklist.*

Provide a standard page in both Swedish and English version which the customer will find when looking for Internet addresses included on the NCP blacklist.

Next we come to the internet service provider’s responsibilities according to the contract, and they are:

The Internet provider undertakes to:

Update the blacklist as soon as possible after receipt and make no changes in the list.

Use the standard page supplied by the NCP.

However, the Internet Provider is free to adapt the standard page by adding information, logo and telephone numbers, etc., for customer service purposes.

Information to customers referring to any specific blocking of Internet content shall be unbiased and not for instance intimate that the products offered are superior to that of other Internet Providers.

To keep the list confidential and not let anyone but the contact persons and the technical personnel needed to install the blacklist have access to the list.

There are some general rules as well, the internet service provider undertakes to deliver statistics over the number of users that have tried to access the web sites blocked under the agreement every fourteenth day the first three months and then each month. The RKP agrees to anonymize the statistics.

The parties can at any time choose to discontinue participation in the programme after having – in writing – explained why. The lists must then be returned and all other information erased.

This programme, as I am sure that most analysts would agree, is well worth studying. We will evaluate it in some detail below. Suffice it to say here that it is one of the most amazing examples of using filters as policy instruments that found today.

**Akismet blog spam filtering**

The second filter I would like to examine is altogether different, but very important to the large population of WordPress users. The Akismet spam filter was

48 WordPress is a powerful and popular blogging tool. See http://www.wordpress.org
designed to manage the growing flood of so-called blog spam that littered blogs all over the world with comments linking to porn sites, poker sites and medicine sale sites among other things.

The blog spam phenomenon quickly became disturbing and Akismet was developed to address this problem. Today the filter is used by several thousands of WordPress users and it is configured locally in the WordPress installation. Spam is caught and kept for fifteen days for evaluation and then erased.

The actual architecture relies heavily on collaboration and on central checking. All comments are sent to a web service where they are evaluated and then sent back to the local user with a thumbs up or down. When something is missed by Akismet and marked-up as spam the system learns from this and develops its filter accordingly.

Akismet has its largest user base among WordPress users, but is open to adaption to wikis, chats and forums of different kinds and thus qualifies as an application independent filter technology. As such it is interesting to examine more closely in an attempt to formulate a framework for evaluating filters.

In order to compare filters and to discuss their different qualities and their effects on the legal system we need a formal framework that enables us to compare filtering policies. I have introduced the simplified definition of a filter as a logical function $F$ which has two arguments $a$ and $b$. $F(a,b)$ is the general notational form of a filter and this would be read as any set $a$ filtered results in the (smaller) set $b$. This notation is useful in extending a framework in which we can discuss certain features in filters and their use. Below I will develop a set of questions that can be used to examine filters as policy measures or responses.

**Is the filter mandatory or voluntary?** This is a basic question that needs to be answered in order to examine the legitimacy of the filter. The answer to this question also determines the level of transparency among other things that we might want to seek.

**Does the actual filtering take place locally on a server somewhere?** We will say that a filter is local if filtering is entirely on the client side without accessing databases or any central resources.

**Are filters transparent?** Transparency is another important part of filter design. It could be defined thus:

(i) A filter $F$ is *transparent* if and only if the function $F$ is openly accessible, available and reproducible for all parties who wish to examine it.

This definition is harsh, and excludes some of the indexing algorithms used today since they are not openly revealed nor accessible to all. But transpranecy is an
important quality of a filter nonetheless since it is the prerequisite for a democratic discussion of the production of information.

*Is filtering predictable?* Predictability is of course closely connected with transparency, but it also concerns the maintenance of the filter. I will define predictability thus:

(ii) A filter is *predictable* if and only if \( F(a,b) \) produces the same set \( b \) for the same set \( a \) over time.

Note that a filter can be predictable without being transparent. It may be possible to attempt to reverse engineer a predictable filter but this can never be done with a hundred percent certainty.

Here it is reasonable to ask over what timeframe a filter needs to be consistent in order to qualify as predictable. The answer may well vary, but it seems unproblematic to note that if a filter changes very quickly, on a daily basis or so, it is not predictable.

*Is the filter content-neutral?* In evaluating filters another interesting aspect is whether or not the nature of the content filtered affects the filtering.

(iii) A filter \( F \) is *content neutral* if and only if it produces the set \( b \) from set \( a \) without regard to the content of set \( a \) or \( b \).

This implies that a filter that processes sets of pornography differently than sets of scientific papers is not neutral. Now, some filters are of course invented merely not to be content neutral and only the simplest filters are, but that a filter is designed to target one type of content is interesting.

*Is the filter actor-neutral?* If the individual who uses the filter affects the result of the filtering, this is also an interesting factor to evaluate.

(iv) A filter \( F \) is *actor neutral* if and only if it produces the same set \( b \) from the same set \( b \) regardless who uses the filter.

Filters that produce results that are different for children and adults are not actor neutral. Neither are filters that produce different results for citizens and non-citizens, men or women or Caucasians and non-Caucasians.

*How are disputes about the design of the filter handled?* Are there processes and routines in place? Are there possibilities – formal or non-formal – to appeal the decision to be filtered in or out?

Among the other qualities of filters that could be interesting to examine are *malleability* – defined as the openness to change. A filter could be defined as malleable if the filtering process is open to change and if there exists processes to
modify the resulting set b in different ways. Malleability may be mandated by law but it can also be a matter of choice. Wikis are examples of filtering architectures that rely heavily on malleability.

Whether a filter is open to review is another matter that would be interesting to examine. To be open to review a filter would have to fulfil some basic requirements of documentation. Being able to examine historic filtering results, statistics and usage patterns may be one part of such openness.

It would also be interesting to discuss the way a filter is maintained and owned. A discussion of open source or proprietary filters could probably have important implications for the evaluation of a certain filter.

Standardisation or the lack thereof is yet another factor.

I will now endeavour to use the question framework to analyse the Swedish ISP-filtering system. This is an instructive exercise in looking at the different aspects in any policy response where filters are used.

Voluntary/mandatory. The filter or blocking mechanism imposed by the agreement is voluntary for the ISPs to use. They can – albeit after explaining why – withdraw from the agreement. Some Swedish ISPs – like Bahnhof – make an explicit point of not participating and motivate this with concern for the freedom of speech and what they describe as the fuzzy description of what can be blocked and why.

Architectural features. The ISP-blocking systems may be designed and implemented differently with different ISPs. They do have a number of architectural traits in common. The first is that they are imposed centrally by the ISP. The ISP is not offering the individual to turn this feature on or off, but they accept the architectural responsibility for blocking, even if they explicitly distance themselves from the editorial responsibility for what is happening.

Transparency. One of the perhaps most problematic things about the Swedish system is its lack of transparency. The list is secret and encrypted – the reason being that it is a list of sources of child pornography and that disseminating it would be encouraging people to visit these sites (unclear why, really). And not only is the list secret, the processes by which one ends up on the list also seems very opaque. In July 2007 the police announced that they were about to include the Swedish bit-torrent site Pirate Bay on the list. The reason, they stated, was that they had found questionable materials available through the web site (Eriksson 2007). In answering how they found it a representative of the police off-handedly mentioned that it had been reported to them by someone. The process for deciding whether a site is included in the list or not seems very malleable and lacks transparency in the extreme. The Pirate Bay questioned the assertion that they were in any way making questionable pornography available, and after what can only be described as a massive blogging revolt the police actually backed down and
admitted that they now saw no reason to include the site on its updated list (For an example of the blogging response the Swedish speaking will enjoy Oscar Swartz influential blog Texplorer (Swartz 2007).

Predictability. As the foregoing shows the Swedish ISP-filtering scores low on predictability. Since there is little or next to nothing known about how the filter is designed and how the police decides what to include on the list the predictability necessarily becomes low.

Content neutrality. The ISP-filtering system is specifically designed to exclude only documented child abuse. The system has a history of having problems with maintaining even this limited content neutrality and filtered out a web site advocating copyright reform (kopimi.se) on the grounds that it contained a naked dancing child. Again the system shows tendencies of sliding down a slippery slope in a way that is perhaps should be worrying to those who hope that it would be possible to attack only child abuse and still limit the filtering to that material.

Actor neutrality. Not all ISP:s (althought all major ISPs are committed) are signatories the filters are not completely actors neutral. They do not, however, differentiate individually. Individuals self-select: those who think that the filters will be useful and support them can go to the ISP:s committed to the agreement. Others can find an ISP that will not engage in filtering. One problem here that is even implied by the agreement is that most people will not be happy at all with any kind of filtering. The agreement thus tries to prohibit the ISPs from informing customers of this choice. The contract, as we remember, actually contains a clause preventing ISPs from pointing out that this feature is not nationally proscribed, but voluntarily agreed upon.

Dispute resolution. Here the system scores extremely low. As mentioned the only reason that the Pirate Bay was not included on the list was massive negative response from the media – both new and old. The police then claimed that the Pirate Bay had complied with their demands to remove the material supposedly containing documented child abuse, and stated that they would not include the torrent site after all. The process lacks all openness and accessibility for individuals blocked.

In summary the filtering system is a problematic policy response, and one that needs to be thought through carefully.

What is this list? The list is kept by a section of the police, a government agency, and then a number of ISP:s agree to block the sites on the list. The list must be some kind of government decision, and thus it should follow all the basic rules for government decisions – there should be a clear mandate for making the decision, there should be rules governing how the decision can and cannot be revoked and there should be transparency in the process. The legal status of the list is curious for several reasons.
It seems, as noted, to be open to changes after “public contact”. In a recent interview comment the police noted that they had put the Pirate Bay on the list, or notified them of such future inclusion, after having been contacted by a concerned member of the public. This is interesting from a legal standpoint: does anybody – anonymous or not – have the legal capacity to report a web site to the police for inclusion on the list? This becomes even more puzzling when considering that such a report would actually be the reporting of a crime – since possession of child pornography is a crime in Sweden (16 kap §10a Swedish Criminal Law) – and this is where it becomes really confusing.

If (and this is a big if since the transparency of the process leaves something to be desired) a web site can be included on the list without a proper legal investigation and an open trial, it would seem as if policy makers have a situation where the police can choose to not investigate a crime, but decide on a punishment anyway. This seems suspiciously like not granting due process. Assume citizens report any other crime and the police choose not to investigate but they add the suspect to a list used by a third party to harm the suspect – would this be acceptable?

Take the case of fraud. I report to the police that you have – I claim – defrauded me, and claim that you have defrauded me by e-mail, claiming to be sick and in need of money. I am a friendly soul (if somewhat gullible) and sent you several thousands of dollars before getting that I was being hoaxed. When I discovered I had been fooled, and you were in fact a con man, I report the alleged crime and your identity. The police examine the evidence, say that the case will be hard to prosecute and end the investigation. But, they say, they will include the alleged fraudster on a list they share – by a contract – with all ISP:s, banks and other private businesses on alleged fraudsters. Banks, ISP:s and other private businesses have agreed to use and check against this list before offering any of their services.

Would this be acceptable?

I think it is possible to argue that it is not. The list would simply be another form of punishment, and to have it meted out by the police without due process is simply hard to defend under the rule of law.

Why is the list with alleged distributors & possessors of child pornography different? There are a number of possible answers to this question, a number of possible defenses for “the Swedish model” - all of them legally interesting from a research perspective.

The nature of the crime. The perhaps most obvious defense for the list is that child pornography is a crime such that the public opinion accepts that the mere suspicion can form the basis for exceptions from the rule of law.

Perhaps most people find child pornography horrible and can live with the fact that both possession, production and distribution of child pornography is illegal.
They may have no need to side with the legal thinkers who argue that this is an unacceptable attack on the freedom of speech, and simply note that there are those who argue that all that can be printed is not necessarily speech. But this does not lead to the conclusion that policy makers should accept the suspension of the rule of law for the cases where child pornography is involved, much as they shouldn’t accept suspension of the rule of law in the case of child murder. However tempting it may be.

The reason is twofold.

Firstly, policy makers would open up the legal system for “crying witch” crimes - a crime where the mere pointing of fingers or the crying of “witch” could lead to legal consequences for the attacked party. Sometimes without any merit whatsoever. Some would argue that this is what has happened already with the Swedish model, stating that the only reason the Pirate Bay is being included in the list is that they are one of the largest tracker sites for torrents in the world – and repeatedly pointed to as a menace for the copyright industries. The conspiracy theory here is that the copyright industry has agreed with the police that they will cry “child pornography” and the police will use the list to end the consistent pain in the rear that Pirate Bay has become to them. If this is true or not is less interesting. What is likely is that any legal system deteriorates quickly if “crying witch”-crimes are intrdouced, and one could argue that policy makers should not allow such destruction of the system no matter how heinous the alleged crimes are. A legal system open to such arbitrariness is dead.

Secondly, such a filtering regime would create a sense of false accomplishment. Presumably, what citizens want is for the police to really examine and allocate resources to fight child abuse. They do not need a short cut that offers a way for the police to look tough on child pornography without actually accomplishing anything. It is striking that the contract between the police and the ISP:s contain a reporting duty for statistics on how many access attempts were made to the blocked web sites – this could be interpreted by suspicious minds as a sign that some consider it more important to be seen as fighting child pornography than to actually do something about the problem.

Because of the general abhorrence of the crime the suspects are rarely likely to stand up and defend themselves publicly. In some – perhaps even most – cases this is because they are indeed guilty of the alleged crime. In other cases because they know that the mere suspicion of a crime like this is likely to harm them.

This actually worsens the effects of the list, because when someone does speak up or refuse to accept the allegations, they will have to meet a double challenge. First they will have to show that they are indeed not guilty of the alleged crimes (and this will have to be done in the court of public opinion since there seems to be no clear rules about how to challenge or revoke decisions on how to be included on the list) and second they will have to show why they are different from all the
others included on the list. The police may even take the negative “hit rate” of the list – the number of blocked sites that have not complained, as evidence that the list works well!

Proportionality. Another defense of the list would be that it is a question of proportionality. The blocking of a web site is a small and careful legal measure if compared with the widespread sharing of the fraudster list in our thought experiment.

This argument mixes two steps, however. Policy makers sometimes do use the argument from proportionality to examine punishments or consequences in our legal system, but this is done under the assumption that the punishment is decided by a court of law after due process under the rule of law. To use the same argument of proportionality from suspicion is hardly acceptable. In fact, it could be argued that there are no proportional legal consequences that follow from suspicion of a crime alone. Even holding someone for interrogation is something that is strictly regulated in most legal systems.

To say that this is simply a legal consequence decided by the police in an on-going investigation and that as such it is proportional is also different. If the police are actually investigating a web site for distributing child pornography there may be a case for an intermediate legal measure to stop further distribution. Such a measure would then be something regulated in law and decided by the court. This is in essence different from having a legal consequence that can be decided by the police no matter if an investigation is on-going or even started.

The defense from proportionality fails, since there can be no proportionality at all in a consequence decided without due process! To realize this it is enough to imagine a “wimp dictatorship” that at the will of a dictator can subject you to tickling. Just because it is merely tickling, not, say, decapitation does not make it proportional in any meaningful sense.

Freedom of contract. A third possibility would be to argue that this is not a legal consequence at all, but simply a contract between the police and some ISP:s. The main gist of this argument would be that not all contracts a government agency enters into amount to the exercise of government power or authority. The ISP:s are free to contract with the police, and the ISP:s are free to enter into any agreements they wish with any party whatsoever. The ISP:s can even make the use of the list a selling point in their offers of services by pointing out that they run a child pornography safe service with the assistance of the Swedish police. This is perhaps what the government would argue today, and this is what some people think is the reason that the list is included in a contract.

But does this hold? Examine, again, another case, a thought experiment.
What would happen if the Swedish police kept a list of papers and magazines with content that could be seen as racist, and if they entered into a contract with the newspaper and magazine distributors in Sweden (Sweden has but two large such distributors, actually) stating that these papers and magazines would not be distributed in the future.

When challenged about this practice, the police simply would answer that they had the freedom to enter into any kind of contract, and that this had nothing to do with the freedom of speech. When queried about how magazines were selected for the list the police simply stated that sometimes the public lets us know if they find racist content. And when asked how a magazine could act to be removed from the list the police would vaguely say something about emailing them.

Would citizens or policy makers accept this under the freedom of contract? It seems unlikely.

One reason, one could argue, is that the list as such has legal consequences for a third party and if drawn up by a government agency the list is not drawn up under the freedom of contract, but as an act of government. The inclusion of the list in a contract is then secondary to this first exercise of governmental power and never free from it. (Again, imagine that this defence for the list would be followed with variations on the defences based on the nature of the crime and proportionality.)

It would seem that this analysis also applies to the list of alleged child pornography providers.

The freedom of contract applies to the police. But one could argue that there are limits to what the police can contract about. There are obvious cases where most citizens would object to the police contracting freely – such as selling “get out of jail”-cards to criminals or outsourcing apprehension of criminals (at least in Sweden this would be dubious).

What can then be done? Let us assume that the list does fill some kind of purpose, and that policy makers want to save it. In a best case scenario the list would then be regulated as a legal consequence in criminal law, and inclusion on the list be something left to a court of law. This could be done in a way that was open to notification, challenge and transparency – without actually making the process too cumbersome. And it should be realized that the fact that a process is cumbersome really never cuts it as an argument against the rule of law. (It is cumbersome to charge murderers as opposed to lynching them. This is not a defense for lynching.)

This would allow for a discussion about the criteria for inclusion on the list, for transparency and challenges as well as for durations of inclusion and other important details.
Then again, there is the hard line. Policy makers could, if they were so inclined, ask if it is reasonable that a government committed to public access to information and the freedom of speech outsources what amounts to soft censorship. (Another issue is whether or not it is possible for the ISP:s to contract in this way at all. This is a whole other argument.)

It is useful to compare and look at Akismet as a response to blog spam.

**Voluntary/Mandatory.** The Akismet spam filter is completely voluntary. It does not even have an inkling of the mandatory that comes with something being the default setting since it is not always installed by default. When the user activates the filter it is an active choice.

**Architectural aspects.** The architecture of Akismet exhibits several interesting traits. One is the centrality of the architecture. The spam filter is the hub to which a number of nodes report on spam found and analyzed. The end result is then decided in the hub and disseminated to the applications in the nodes. This distributed architecture is strong and collective, it creates a collaborative filter against spam that works fine. It does, however, also contain some risks. What if, for example, the hub goes offline? Akismet answers this by pointing out that if it does the only thing that happens is that the comments end up where they would end up if they were legitimate – on the web page or in the moderation queue. Akismet is designed to default back to freedom of speech, if you will.

**Transparency.** The filter is transparent in that it shows exactly what is filtered and allows the blogger to decide if he or she wants to erase comments caught as spam or change certain comments’ status to “not-spam”. Exactly how the filter works is not completely clear, however, and since it is both a commercial product and free for non-commercial purposes there is always the risk that the code may be hard to access, even if the WordPress plug-in is licensed under GPL.

**Predictability.** The filter is predictable and its result is possible to check. It checks for spam, that is pretty much it. It never starts to deviate and check for the politically incorrect.

**Actor neutrality.** Akismet is actor neutral in the sense that it does not matter who writes a comment or who installs it to what the results are. An Iranian blogger will get the same spam lists as a Swede, and the spam filtering is targeting spam as a global phenomenon.

**Content neutrality.** Akismet doesn’t care about the content of a message, but about whether or not the content and its structure signals that the message is spam. This allows us to say that it has a kind of content neutrality.

**Dispute resolution.** If you as an editor of a blog find that something is not spam you simply redefine it and it is published as any other comment. This feature solves
dispute resolution only between the blog publisher and the filter, not between the publisher and the commenter, however. The filter gives the right in deciding what is spam and not to the individual blogger. This may be a dubious practice in some cases. Consider the case where the blog publisher is a public authority for example. Would it be proper that the authority arbitrarily decides what is spam and what is not? Probably not. We would like there to be more rigorous rules on process in that case.

Akismet, to sum up, is a kind of carefully designed policy response with a more architectural emphasis and it works through transparency and usability.

Using filters as policy responses is naturally not a quick fix. Filtering responses are complex to design and they demand that policy makers think carefully at least about the different characteristics listed in the previous section. There are a number of hard, difficult questions that must still be addressed to make filters a more appetizing policy option in the politicians toolbox.

The first problem is that noise is gender, culture and context dependent. If policy makers design a filter for filtering in personal data into a digital persona they need to know for whom the persona is designed, why and in what culture. Filtering in Saudi Arabia is different from filtering in Sweden.

All the differences citizens can encounter must be taken into account not to neglect anyone’s rights. A Swede has a certain expectation of filtering and other countries have other expectations of filtering. Describing these expectations may also be important to establish design principles for filtering in different contexts.

Let’s imagine that policy makers implement a number of filters to eliminate access to racist propaganda. Who then decides what to filter out? Is it racist to claim the Swedes are sexually liberal? Is it racism to claim that Brits are stuck-up? Policy makers using the information society model lack good ways of deciding on what gets filtered and what can pass through. As seen in the Kazaa-case this should probably not be decided by courts. For courts to become semi-legislative filter-designing assemblies is not a great solution by any measure. Society lacks policy processes to decide collectively on what to filter. What is available is collaborative technologies aggregating our assessments of, say, spam and implementing the mean assessment. This is, in a sense, also a kind of democratic process. It is the democratic, autonomous process of collective architecture design.

The emerging discourse of filters becomes more important in the orders of discourse in the information society. Filters confirm to the theoretical model where small-scale technologies autonomously drive change, but if policy makers confirm to the old model of control they may be tempted to use large-scale centralized filter technologies. How this discourse settles, stabilizes, is an important element in the on-going social change witnessed today.
Search

The characterization of our society as an information society is, I have claimed, problematic. Indeed, there exists vast amounts of ever-growing information repositories around the globe in websites, databases and other digital forms, but this by itself does not provide the foundations for an information society. Instead, policy makers and others are facing a noise society where the information we need is always out of grasp, in the exploding noise.

In order to examine how policy making cases could look in the noise society, and to show in practice how policy makers could change their mindset I have included a case-study where an actual problem is used to show how policy makers may need to think about policy responses in a society that resembles a noise society more than an information society.

Under these circumstances search becomes an essential social function. Between the sea of noise and the information society stands filters of different kinds, and search engines provide one very special kind of filtering tool. These filters allow users to filter out much of the information overload and find what they need, quickly as well as with some accuracy. The growing utility of search also makes it important to ask questions about search engines and their practices. It becomes essential to examine the mechanisms of search, the consequences of being searchable as well as not being searchable and the long-term changes search policies can effect. The design of search architecture becomes an important policy response.

This chapter will focus on one very narrow aspect of this growing subject area, the relationship between the public sector and search, especially in terms of transparency. Public sector agencies and other bodies, such as public universities or research institutions, are under legal obligations to establish a certain amount of transparency. But to what extent can they actually choose not to be searchable? Not be indexed or not be crawled by popular search engines?

And specifically: to what extent can a public agency or body use the so-called robots exclusion standard to escape being indexed? What different legal aspects exist on the use, in the public sector, of the robots exclusion standard? Is it possible for a public agency to exclude only one search engine, and welcome others? Can a publicly funded research institution exclude some parts of its website from indexing because researchers or their donors request this? Or is there a general

---

49 This section is based on (Lundblad, e-Exclusion and Bot Rights 2007) and serves to exhibit another discourse, the discourse on access and search as it is developing today.
obligation for public bodies to be searchable and indexed by as many robots and other agents as possible?

The chapter focuses on a Swedish context, which holds some extra value, since Sweden has a strong principle of public access to information. It will concentrate on two legal aspects: the principle of public access in Sweden and the Public Sector Information-directive. A survey of different uses and practices at Swedish public agencies and bodies is presented.

The *robots exclusion standard* is very simple to understand. It consists of a simple text file placed in the root directory of a server. The text file is named robots.txt and defines a policy for search bots that signals whether or not a certain directory can or cannot be indexed by a robot.

The policy is formulated in a simple way, and the simplest possible application of the standard is a file that stops all bots. Such a file would be formatted thus:

```
# go away
User-agent: *
Disallow: /
```

This, put in a robots.txt-file, signals that the site owner does not want the site to be indexed at all. The end result is a very simple standard that can be used by anyone, containing only two different functions: "user-agent" and "disallow". These two functions take as arguments different user-agents, that is different bots from different search facilitators, and different directories or files. The "disallow"-function can be global, as it is in the example, or local, with defined directories that the site owner wants to be exempt from search.

Another important point to make is that using the robot exclusion standard is quite legitimate. There are cases where indexing becomes burdensome on server capacity or where one does simply not want certain folders indexed by public search engines. The method is not fool-proof, but offers an opportunity to control access to information and control server load.

It can be assumed that the robot exclusion standard is rarely, if ever, used to conceal information. There are far more efficient and simpler ways of accomplishing this. But there is a difference between concealing information and restricting structured access that is interesting to examine closer. What the standard does do is that it restricts the probability that the information will be found by someone who does not know that it exists or where to search for it. This is a kind of pseudo-concealment that can have adverse effects.

---

The robots exclusion standard is not a formal standard. If anything it has become a de facto standard, respected by many search engines and effectively implemented in many pieces of search software. The web site holding the standard notes:51

This document represents a consensus on 30 June 1994 on the robots mailing list (robots-request@nexor.co.uk) [Note the Robots mailing list has relocated to WebCrawler. See the Robots pages at WebCrawler for details], between the majority of robot authors and other people with an interest in robots. It has also been open for discussion on the Technical World Wide Web mailing list (www-talk@info.cern.ch). This document is based on a previous working draft under the same title.

It is not an official standard backed by a standards body, or owned by any commercial organisation. It is not enforced by anybody, and there no guarantee that all current and future robots will use it. Consider it a common facility the majority of robot authors offer the WWW community to protect WWW server against unwanted accesses by their robots.

There exist some extensions and modifications of the standard, but these will not be mentioned in detail here.52

Aside from using the robots exclusion standard it is also possible to use so-called meta tags on a page to stop bots from indexing the pages or following the links published within these pages. This method poses many of the same questions as the robots exclusion standard, but will not be dealt with here.53

What, then, are the legal implications of using a robots.txt-file on ones web server? Is there a legal obligation for bots to respect a self-declared standard that is neither formal nor codified in any of the larger standards organizations outside of the formal standards structure? The short answer is that no-one knows. But there are examples that can be thought of as analogous and that can be used to explore the issue. One close analogy can be found by studying the practice of “acceptable use”-policies on web sites, and what legal worth they have been found to have. An “acceptable use”-policy is any kind of policy available at a web site and published with the intent of declaring what uses the website and the information on the website may be put to.

In a number of cases at least American courts have signalled that they take the content of these use policies seriously and that they consider them to have serious legal effects. In particular, these use policies have become associated with the legal doctrine sometimes called “cyberspace-as-place”, or the idea that a visitor to a website may well be, in some sense a trespasser (Lemley 2003, J. Cohen, Cyberspace As/And Place 2007, Hunter 2007, O'Rourke 2001).


52 See http://www.conman.org/people/spc/robots2.html#format.directives.disallow (visited 2007-05-01)

53 See http://www.google.com/support/webmasters/bin/answer.py?answer=61050
There are, of course, many differences between an acceptable use policy and a robots.txt-file, not the least of which is that it is possible that a human visitor to a website never notices the robots.txt-file (even if this might apply to some acceptable use policies as well, if they are hidden in strange places on the website). But these differences are not so large as to negate the possibility of an argument ex analogia where the robots.txt-file is seen as an acceptable use policy for bots and crawlers of different kinds.

The important question, of course, becomes whether or not a bot can be seen as trespassing or if you have to be human to be able to trespass. Could a train trespass? A car? What, then, about a bot? These seem almost childish questions, but they illustrate the great difficulties in solving problems related to the new technological architecture society is facing. Curiously, the idea that bots could trespass seems to strengthen the legitimacy of the cyberspace metaphor, and of the image of cyberspace as a separate domain so enamoured by the early cyberlibertarians (Barlow, A Declaration of Independence of Cyberspace 2001 (1996), Post and Johnson, Law and Borders in Cyberspace: The Rise of Law in Cyberspace 2001).

Since in at least one case a bot was seen as trespassing (Lemley, 2002 supra note 22) it seems reasonable to assume that ignoring the robots.txt-file could be seen as digital trespass, even if it has not been established, or at least not established in Swedish law.

The question about the legal status of self-declared bot policies depend on two parties: the web site being indexed and the search engine. Up until now I have assumed that the party behind the indexing crawler has declared nothing about its position on the use of the robots exclusion standard. But what if a search engine has explicitly recommended the use of the standard and publicly said that it will respect the standard?

This is the case with, for example, Google. In their advice to web masters they clearly state:

To remove your site from search engines and prevent all robots from crawling it in the future, place the following robots.txt file in your server root:

```
User-agent: *
Disallow: /
```

To remove your site from Google only and prevent just Googlebot from crawling your site in the future, place the following robots.txt file in your server root:

```
User-agent: Googlebot
Disallow: /
```

Each port must have its own robots.txt file. In particular, if you serve content via both http and https, you'll need a separate robots.txt file for each of these protocols. For example, to allow Googlebot to index all http pages but no https pages, you'd use the robots.txt files below.

For your http protocol (http://yourserver.com/robots.txt):

User-agent: *
Allow: /

For the https protocol (https://yourserver.com/robots.txt):

User-agent: *
Disallow: /

Does this affect the legal analysis of the status of the standard? Is this support page a binding promise from Google to respect the robots exclusion standard? If this is assumed to be the case a host of new questions become important: how soon after a change in the bot-policy of a web site must this change be reflected in the index at Google? And is this self-declared compliance binding over time? Or can Google at anytime change its compliance?

It may be reasonable to assume that this support page has some legal relevance. A one-sided attempt at committing Google to follow the standard may seem a weak basis to build the legal effects of the robots exclusion standard on, but it remains a possible step in establishing that Google, and other search engines which commit in the same way, actually assumes a legal obligation to the respect the standard when they point to it as an important measure available to websites unwilling to be indexed.

In the end it will be up to courts to decide what the status of a robots.txt-file should be. In Sweden such legal precedents are lacking and policy makers are left to guesswork. This need not be a problem. Here I will assume that the use of the robots exclusion standard binds a search engine or other search software legally. This premise will be used to concentrate on the true subject of our research – if public agencies and other public sector bodies can indeed use the standard and if so, in what ways.

The question is not limited to the robots.txt-file. Any other self-declaring policy that is machine-readable will have to be examined in much the same way. One example could be the envisaged standard DPRL – Digital Rights Property Language – designed to express rights about particular digital objects (Stefik 1998). Any other new standard that expresses rights and obligations would have to be examined specifically for its use in the public sector.

A short introduction to the principle of public access to official documents is probably a good starting point for the discussion later.

Sweden has one of the longest legal traditions in the world when it comes to public access to official documents. The first constitutional law that contains the principle was crafted and put into force back in the year 1766. This law contained a right to
public access to official documents that has since been expanded and renewed. In the current legislation it is found in the first paragraph of the second chapter of the Freedom of the Press Act:

To encourage the free exchange of opinion and availability of comprehensive information, every Swedish citizen shall be entitled to have free access to official documents.

The principle is very extensive and has a wide scope. There are several precedents and a large body of literature on the application of the process.

The principle is fairly simple to explain, but the devil is in the details. Somewhat simplified, all Swedish citizens have the right to public access to official documents if these have not been classified or if giving them out would constitute an infringement of privacy. A public official that refuses to give out information must show clearly on what exact legal grounds his decision is founded. A failure to comply with the principle is a crime and is punishable by criminal law.

Much of the law and precedent hinges on the definition and understanding of what actually constitutes an official document or act. This is difficult to decide, but the concept has been applied broadly. It is uncontroversial to note that documents or other information on a computer is covered by the definition. The content of a website is normally to be regarded as an official document.

The exemptions allowed for in the Freedom of the Press Act are narrow and the most practical exemption – besides classified information and certain privacy infringements – are draft documents and memoranda. It would take us too far to delve more deeply into the principle and the associated literature here.

There is no obligation to allow access to information or official documents in a certain format. It does not follow from the principle of public access that a public agency must employ the broadest possible means of information access to all its information. But if information is available in a certain format, it normally means that a citizen has the right to acquire it in that format.

It follows that there is no obligation for public sector information holders to convert, scan or otherwise manipulate data in order for it to be available on the web. This is an important fact to keep in mind when discussing the question of a duty to be searchable.

The European Commission has stated that it believes that public sector information could be used by entrepreneurs to open up a whole new market for public sector information in various forms. To ensure that states make information available, and to safe-guard private enterprise against unfair competition from public sector actors that sell information, the Commission has crafted a directive on the re-use of public sector information. The result, Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of
public sector information, is now being implemented throughout the European Union.\textsuperscript{55} The directive is applies to all public sector bodies but exempts a number of different sectors. Research, archives and public service broadcasters, for example, do not have to comply with the directive, or at least not to the extent they act within these roles and do not themselves engage in commercial re-use of their own information.\textsuperscript{56} The general principle is found in Article 3:

> Member States shall ensure that, where the re-use of documents held by public sector bodies is allowed, these documents shall be re-usable for commercial or non-commercial purposes in accordance with the conditions set out in Chapters III and IV. Where possible, documents shall be made available through electronic means.

The directive then sets out specific rules on requests and conditions for reuse, as well as non-discrimination and fair trading. These rules lay down principles on prompt reply to requests, fair conditions, and competitive practices that all aim to create the preconditions for entrepreneurial innovation in the public sector information field.

The general question of this paper could have been discussed and examined without empirical evidence. The empirical evidence, however, helps to suggest different categories of use of the robots exclusion standards, and gives us good examples to work with in the discussion. Therefore a short empirical investigation was initiated.

A number of public agency websites were searched (selected pseudo-randomly for size) for the robots.txt-file. Where such a file was found it was copied and printed out. The different files were then examined and categorized.

The survey was not complete, nor was the intention to make definitive statements about the frequency of use of the robots exclusion standard. The collection of samples is merely intended to give a rough idea of different practices and formulations of the robots.txt-file. The public sector bodies examined and found to have a robots.txt-file were:

\textsuperscript{55} The European Commission recently saw itself forced to open infringement proceedings against a number of countries who have not as of yet implemented the directive in national law.

\textsuperscript{56} This is a controversial point. One may argue that the exemptions are absolute and that archives, for example, are given a carte blanche to engage in unfair competition whenever they want to in selling information. This, however, seems an extreme interpretation of the exemptions.
These public sector bodies all used a robots.txt-file in their root directory. It should be noted that I do not imply that the use of the robots.txt-file has been decided upon by the leadership at these agencies and bodies. Indeed, I think that many have not even reflected on its use at all – which is part of the problem.

Some of the surveyed websites completely disallow, or try to disallow, that robots index their sites. Examples of complete exclusion were found at The Swedish National Financial Management Authority and The Swedish National Agency for Higher Education. Interestingly, none of these attempts at complete exclusion were successfully formatted. If checked with a simple tool they turned out to be defective. The erroneous file looked like this in both cases:

```
User-agent: 
Disallow: 
```

To be formatted correctly the functions would have to have arguments or placeholders (* and /) to signify that all content should be exempt from indexing.

---

57 I used http://tool.motoricerca.info/robots-checker.phtml to check the syntax of the robots.txt-file.
Many of the surveyed web sites excluded parts of their websites. The examples of what was excluded varies.

The Swedish Competition Authority has excluded a directory called “Beslut” which in English translates to “Decisions”:

```
# robots.txt for http://www.kkv.se/
User-agent: *
Disallow: /beslut
```

Uppsala University has excluded a number of different directories, for sometimes unclear reasons:

```
User-agent: *
Disallow: /Titlepage/
Disallow: /Education/Program/
Disallow: /Education/Kurser/
Disallow: /coop/skandia/
Disallow: /Forskning/
Disallow: /oktober/
Disallow: /Internt/old/
Disallow: /Library/
Disallow: /navbar/
Disallow: /Postcards/
```

Another example of an educational facility with research is Karolinska Institute. The Institute has an incredibly old robots.txt-file, amply commented upon:

```
# robots.txt for http://www.ki.se/
# Ulf Kronman 18 jul 95 - 97
User-agent: *
# all robots
Disallow: /SFgate/ # WWW-WAIS scripts
Disallow: /cgi/ # scripts
Disallow: /cgi-bin/ # scripts
Disallow: /s害/ # scripts
Disallow: /form/ # mallar
Disallow: /demo/ # not for external use
Disallow: /it/kurs/test/ # course testing - not for external use
Disallow: /it/select/ # KI software - not for external use
Disallow: /it/торget/ # KI software - not for external use
Disallow: /sys/ # system docs - not for external use
Disallow: /templ/ # templates - not for external use
Disallow: /test/ # testing - not for external use
Disallow: /db/ # databases - not for external use
Disallow: /alex/ # not for external use
Disallow: /usage/# not for external use
Disallow: /usage2/# not for external use
Disallow: /ADSL/ # not for external use
Disallow: /webvval/# not for external use
Disallow: /statistik/ # not for external use
Disallow: /webstat/# not for external use
Disallow: /kemi2/# not for external use
Disallow: /kemi1/# not for external use
Disallow: /static/
Disallow: /php/
Disallow: /styrelseval/
```

The last directory excluded – board election – is interesting as a general example. It points to a series of test elections for the board. It is unclear why they were

58 The directory /oktober/ seems to contain an old backup of somebody called Pelle and a lot of old information.
excluded, but it is possible to ask the general question of whether it is more or less suitable to exclude certain directories based on what they contain.

Regeringen.se – the government’s website – excludes all downloads:

User-agent: *
Disallow: /download/
The reason may be that downloads are heavy PDF-files, and that the indexing of these consumes too much bandwidth, but the exemption is not commented upon.\(^{59}\)

Riksdagen.se – The National Parliament – excludes all URLs containing the phrase Media=Print by using the following code:

User-agent: * 
Disallow: /*Media=Print
This, however, also gets a warning in the syntax-checker. The warning is interesting, because it makes clear that Riksdagen is not using the basic version of the robots exclusion standard, but a version commonly associated with Google:

Disallow: /*Media=Print
The "*" wildchar in file names is not supported by (all) the user-agents addressed by this block of code. You should use the wildchar "*" in a block of code exclusively addressed to spiders that support the wildchar (Eg. Googlebot).

This implies that the robots.txt-file at the Parliament has been designed specifically for Googlebot and other bots that accept that dialect of the robots exclusion standard.

The National Archives exclude a number of different directories:

User-agent: * 
Disallow: /sok/
Disallow: /prog/
Disallow: /javascript/
Disallow: /ra/nad/
The last excluded directory is the directory of the national archives database, which is commercially available through that URL.

Statistics Sweden has an extensive robots.txt-file:

```
#########################
# disallow all folders but
# /gemensamma_filer/
# /grupp/
# /Statistik/
# /templates/
#
User-agent: *
#
# list folders robots are not allowed to index
#
```

\(^{59}\) Based on communication with Staffan Malmgren, at the Swedish Institute for Legal Informatics.
The excluded directories again contain a database directory, but the main statistics directory is left open to indexing.

Swedish Companies Registration Authority has a very simple file, excluding some templates:

```
User-agent: *
Disallow: /_notes/
Disallow: /adm/
Disallow: /Templates/
```

It is far more interesting to examine the contents of the robots.txt-file at the Swedish Data Inspection Board:

```
User-agent: *
Disallow: /cgi-bin
Disallow: /bilder
Disallow: /IMS
Disallow: /ims
Disallow: /javascript
Disallow: /sokhjalp
Disallow: /Templates
Disallow: /tomcat4-webapps/enkat
Disallow: /tomcat4-webapps/sok
Disallow: /om_datainspektionen/om_datainspektionen.shtml
Disallow: /fragar_avar/fragar_avar.shtml
Disallow: /temasidor/temasidor.shtml
Disallow: /lagar/lagar.shtml
Disallow: /lattlast
Disallow: /puo/puo.shtml
Disallow: /phpBB
Disallow: /phpBB
Disallow: /lists
Disallow: /phplist-2.8.6
Disallow: /cgi-bin
Disallow: /poll
Disallow: /lists
Disallow: /toppbanner
Disallow: /sokhjalp/sokhjalp.shtml
Disallow: /webbkarta
Disallow: /utbildning_konferenser/utbildning_konferenser.shtml
Disallow: /utbildning_konferenser/anmalan_inkass02.shtml
Disallow: /nyhetsarkiv/nyhetsarkiv.shtml
Disallow: /anmalan_forhandskontroll/anmalan_forhandskontroll.shtml
Disallow: /tillstand_tillstandshavare/tillstand_tillstandshavare.shtml
Disallow: /info.shtml
Disallow: index4.shtml
Disallow: stilmall.css
Disallow: stilmall2.css
```
Disallow: fel.shtml

Why would the Board want its FAQ to be excluded from search indexing? Or a page with laws on privacy? Or educational resources? Without commenting on the Data Inspection Board directly one could note that it in a worst case scenario it is possible to imagine a search engine company that sells software for website search would like to show a better result than other search engines such as Google. In order to accomplish this they may feel compelled to “fix the competition”. Disallow the pages you want to excel at finding with your search solution and then compare.

“Did Google find the FAQ? No, but our search software did.” – But only because it ignores the robots.txt-file. This scenario is fictional, but not impossible.

The Swedish Armed Forces have a simple robots.txt-file:

User-agent: *
Disallow: /attachments/
Disallow: /images/
User-agent: sitecheck.internetseer.com
Disallow: /

The interesting thing is not that it excludes attachments and images, but rather that it excludes one particular search bot. The agent excluded comes from a site that offers monitoring services:

The monitoring systems remotely check your website from several geographic monitoring stations at selected intervals. If the monitoring system is unable to reach the site, an email, cell phone or pager alert is sent to notify you of the problem.

It is unclear why this user agent is excluded from all directories, but perhaps there is a security problem here: the Swedish Armed Forces does not want anyone else to know when their site might be down, since this may reveal maintenance schedules and other information security weaknesses. Again, this is guesswork.

Another example of a website that excludes different agents is the Royal Institute of Technology. The Institute also has the by far largest robots.txt-file:

User-agent: *
Disallow: /cgi-bin
Disallow: /cgi-perl
Disallow: /internt
Disallow: /info
Disallow: /kthprog
Disallow: /kthcd
Disallow: /student2
Disallow: /kthnytt
Disallow: /kth-nytt
Disallow: /utbildning/vidareutbildning01/
Disallow: /utbildning/vidareutbildning02/
Disallow: /utbildning/vidareutbildning03/
Disallow: /utbildning/vidareutbildning04/
Disallow: /html-files
Disallow: /src
Disallow: /smartsieve

60 http://www.internetseer.com/home/index.xtp;jsessionid=akTzxfN-93z9
This extensive exclusion-file is useful in setting up the discussion section. Firstly it separates between different user-agents, from internal crawlers to external crawler. It goes so far as to exclude one user-agent, Scooter (the old Altavista bot, rarely seen nowadays), from the website altogether. It also has a hierarchy of exclusion: first excluding certain files for all user-agents that are not defined, and then defining exclusion extensively for some identified user-agents. Among these we find Googlebot. Secondly it makes no comment on the directories excluded and thirdly it excludes both directories and single files.

Is use of the robots exclusion standard possible under the principle of public access to official documents? Let us examine the arguments for and against.

The argument against use of the standard would consist of several steps. In the information society the explosion of content has made search engines absolutely necessary to find anything on the internet. All documents on a at least the public part of a public sector body’s website must be presumed to be a) official documents and b) accessible to Swedish citizens under the principle of public access. The use of the robots exclusion standard efficiently makes documents – all or selection of them – unavailable. This is in direct conflict with the principle.
Furthermore using the standard selectively has the same effect as classifying some documents, since they will not be found by anyone if they are not indexed. This means that selective use of the standard cannot be allowed without support by legislation allowing classification of the documents in question as secret.

In addition to this use of the robots exclusion standard is a practice that makes more difficult for citizens to exercise the right of review and control that was intended by the legislator in framing the Freedom of the Press Act. It circumvents not only the actual rules but also the original intent of the legislation. No public website should be allowed to use the robots exclusion standard for any other reasons than purely technical reasons, and they should then be forced to declare publicly on the website what directories and files have been excluded from search engines and on what basis.

The opponent of this argument would point out that it relies on several interpretations of the principle of public access that could be argued to stretch the principle to its limits and beyond.

Firstly, the principle of public access is a right to have certain identified documents, not to have the maximum searchability of an agency’s documents. It does not follow from the principle of public access that the agency must keep a well ordered and simple-to-search archive for every citizen that wants to pursue an investigation in general into the agencies activities. Secondly, the principle applies only to Swedish citizens. This means that in regard to all foreign nationals there exists no obligation to provide public access to official documents. This implies that the scope of a search engine is too wide to be a case where the principle applies. Indeed: search engines sometimes make information available in what in European privacy law is called third countries, and there then exists an obligation not to transmit personal data across borders if the level of data protection cannot be ascertained to be the same as in the European Union. Thirdly, there exists no right to demand access to official documents in a given format. The websites are available through the principle, and need only be requested, but nothing – except the sheer absurdity – stops agencies from providing access to the entire website on paper in printouts. This means that it is impossible to construct an obligation for agencies to provide access to their websites as websites in certain fashion. Fourthly, the principle of public access to official documents is not a right to have access to structured information. It is an access right and not a presentation right. The mistake done by those arguing that public sector bodies cannot use the robots exclusion standard is to assume that there follows from the principle a right of searchability or presentation in search engines. No such right or corresponding obligation exists.

In summary the argument seems in favour of the party claiming that there is no legal obligation here, although the selective use of the robots exclusion standard indeed seems to have something in common with classification of documents.
What, then, of the PSI-directive? Could it be argued that there follows from the articles in the PSI-directive obligations not to use a robots exclusion standard or to use it only in certain ways? The argument for that the PSI-directive makes it impossible to use the robots exclusion standard would probably be based on the idea that searchability is an essential component in fair trading and equal treatment.

Let’s assume that a certain public agency has a lot of desirable map data, and that the agency sells this data on its own website. Further, it uses a proprietary search engine developed within the agency for searching and analysing the map data. This search engine is strong and efficient, and gives excellent results. A company trying to compete with the agency is given access to the agency’s data, but not to its search engine. The company is instead forced to use an another search engine approved by the agency, since the agency blocks all other search engines, including Google, which the company had been thinking to employ to build its own solution.

Would this be in conflict with the provisions of the directive? It seems as if it would at least be possible to attack from the principle of fair competition.

Another possible argument against the use of the standard can be found in Article 5 p 1 of the directive, which states that:

Public sector bodies shall make their documents available in any pre-existing format or language, through electronic means where possible and appropriate. This shall not imply an obligation for public sector bodies to create or adapt documents in order to comply with the request, nor shall it imply an obligation to provide extracts from documents where this would involve disproportionate effort, going beyond a simple operation.

Note the obligation to use electronic means where “possible and appropriate”. This could at least be taken to imply that unnecessary and unwarranted use of the robots exclusion standard is problematic. That extracts can be provided through search technology in a way that does not involve disproportionate effort should also be noted. Furthermore, it seems possible to use the prohibition of exclusive arrangements in Article 11 p 1 to make the argument that the robots exclusion standard – used selectively – discriminates:

The re-use of documents shall be open to all potential actors in the market, even if one or more market players already exploit added-value products based on these documents. Contracts or other arrangements between the public sector bodies holding the documents and third parties shall not grant exclusive rights.

---

61 This would be quite possible under the assumption that the search engine is not public sector information – a reasonable interpretation of the directive.
An agency that excludes certain companies because they want to rely on private search engines indexing of publicly available data should at least have a good argument for doing so under the directive. Overall it seems doubtful to exclude some user-agents, but not others.

There are numerous cases where the PSI-directive could come into conflict with the robots exclusion standard. The outcome of such a conflict would depend on interpretation of not only the articles in the directive, but also of the role of search in establishing the new entrepreneurial sector where re-use of public sector information is the driving force.

Should the robots exclusion standard and the robots.txt-file be categorized as a technological measure as defined by European copyright law (WIPO 1996)? If we accept such a categorization it follows that disobeying the robots.txt-file would constitute illegal circumvention.

But then the next question quickly becomes if public sector bodies and agencies actually have copyright in all or some of the information they hold. And is it possible to have technical measures protecting content that is, by itself, not protected by copyright?

Let us assume – and that is assuming a lot – that public agencies have the copyright of all the information they hold. Then the task becomes one of deciding whether or not the robots exclusion standard and the robots.txt-file constitutes rights management information or a technical measure. The directive defines these two technical terms as:62

For the purposes of this Directive, the expression "technological measures" means any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject-matter, which are not authorised by the rightholder of any copyright or any right related to copyright as provided for by law or the sui generis right provided for in Chapter III of Directive 96/9/EC. Technological measures shall be deemed "effective" where the use of a protected work or other subject-matter is controlled by the rightholders through application of an access control or protection process, such as encryption, scrambling or other transformation of the work or other subject-matter or a copy control mechanism, which achieves the protection objective.

Rights management information is defined as:63


For the purposes of this Directive, the expression "rights-management information" means any information provided by rightholders which identifies the work or other subject-matter referred to in this Directive or covered by the sui generis right provided for in Chapter III of Directive 96/9/EC, the author or any other rightholder, or information about the terms and conditions of use of the work or other subject-matter, and any numbers or codes that represent such information.

The first subparagraph shall apply when any of these items of information is associated with a copy of, or appears in connection with the communication to the public of, a work or other subject-matter referred to in this Directive or covered by the sui generis right provided for in Chapter III of Directive 96/9/EC.

If the concept technological measure is interpreted extensively it seems possible to argue that the robots exclusion standard fulfils the requirements in the directive to be categorized as such a measure. The weak points are possibly that the robots exclusion standard seeks to prevent acts relating not to a specified set of works, but rather to a repository of works (if the website is not seen as a unitary work) and there is certainly the issue of the effectiveness of the measure.

The definition of rights-management information seems to come closer, with the definition “information about the terms and conditions of use of the work or other subject-matter”.

A possible objection would be that the robots exclusion standard does not (normally) refer explicitly to works in any way. It refers to directories where works can be found. This may seem a slight difference, but it is a meaningful one. It is hard to find analogies, but we could ask if a lock on the door of a house is the same thing as a “no trespass”-sign. Note, then, that it is possible to argue that a “no-trespass”-sign is not a technical measure of rights-management information, since it does not refer to or relate to any specific property or work. The sign merely prohibits entry. It says nothing about what you may find on entry, should you disregard this prohibition.

It is a tenuous objection, but it could have some relevance. It could also be met with a counter-objection stating that the robots exclusion standard actually can be used to refer to specific works. It is quite possible to disallow indexing of specific files and works. How such use of the standard should be judged is an even more complicated matter.

The matter of copyright in public sector information raises the question of whether the provisions in the directive cover only works that are copyright protected, or if it possible to protect content contractually where the copyright term has expired, and if it is illegal to circumvent rights-management information or technical measures protecting such works. Rice (2001) offers a discussion about the contractual extension of protection and it cannot be excluded that even if a public sector body does not have copyright in its works, it may in some cases be illegal to
circumvent rights-management information – even if it seems implausible in the extreme.

Another related question is if the robot exclusion standard applies solely to one kind of robot or crawler. One possibility is to limit the applicability of the standard to simple search crawlers catalogued and self-declared as “user agents”. This would then exempt more intelligent\textsuperscript{64} search agents from the standard (Boonk, et al. 2005). Another possibility would be to extend the use of the standard to all automated software traversing the Internet.

The reason this becomes an interesting question is that if the standard was used for simpler bots only, then certain search engines or even search engines in advanced search could allow the user to ignore robots.txt-files. This would then become a user choice to some extent. This, however, presupposes another kind of search and indexing technology than the one used today. Indexing takes time and cannot be done on the fly.

Another issue that will not be explored in detail here is whether or not it is reasonable to assume that different public bodies who are bound by law or who have the mandate to deploy crawlers can, or indeed must, ignore the robot exclusion standard.

Using the robots exclusion standard is, in a sense, no different from using other new and interesting technologies or standards. It carries with it the risk of being found in breach of legal rules interpreted in a novel way in the new environment. But there are certain tactics that can be employed to minimize the risk these new technologies bring and the legal uncertainty associated with them. Using new technology consciously, carefully and in a competitively neutral way is a good start and respecting that search becomes more important in the noise society is probably a good guiding principle.

The implications of the Sitemaps protocol should also be examined more clearly. Is it possible to merely exclude and not use the possibilities in Sitemaps to include relevant information for indexing?

Use of the robots exclusion standard should be a conscious choice. If it is a technological choice, this should be brought to the attention of the management. The reason behind this is twofold: the management needs to have the information to dispel any notion that the standard is used for the wrong purposes, and informing management would reduce the risk that the standard is used in non-acceptable ways, for example to boost search software installed locally.

\textsuperscript{64} This would presume that we find a good way of deciding on the cognitive ability of agents.
Conscious use should be documented, and if possible communicated clearly through the website. One possibility that should not be excluded is that public sector websites have clear acceptable use policies, complete with use by bots as a special paragraph.

The use of the robots exclusion standard should be careful in the sense that the organisation should be informed and possible disadvantages examined beforehand if at all possible. Feedback from external parties should be welcomed, and consulting with technical expertise would eliminate some of the uncertainties associated with the use of the standard.

Considering the status of the standard, and the unclear legal situation, the standard should not be used if there are not compelling reasons to do so.

Any use of the standard must be competitively neutral and must not affect the market for commercial actors in any way. This follows not only for those agencies that compete in commercial information markets, but for all agencies. Should it become known that one search engine is regularly excluded, but another not, this would affect visits and in the end advertising revenue for the excluded search engine.

Filters are already part of the modern policymaker’s toolbox. In the next few years they will become more important and powerful. In preparation for the age of filter politicians we should examine the criteria we need to evaluate filters from a legal and democratic standpoint. The fine-tuning of future filter architectures will decide the shape and form of future democracy. The future may require not a principle of public access so much as a principle of public searchability.

When examining a simple case like this with a noise society model in mind rather than an information society model is that the problems are slightly different: policymakers may need to think more about how we use technology and technologies hitherto thought of as unimportant or inconsequential turn out to be essential in attaining policy goals like openness, participation and inclusion.

Search becomes an important new discourse, and a strong element in policy making – mirroring the importance of filters.

**The noise society model**

What remains to be done, now, is to develop a noise society model. How this model or set of heuristics should look is a difficult question. One possible way to address the question is to use the same variables as in the information society model and change them to accommodate the idea of a noise society. This would result in a model or set of heuristics that could look like this.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Model Assumption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Production</td>
<td>Information growth is out-of-control. Small-</td>
</tr>
</tbody>
</table>
scale autonomous technologies produce a sea of noise from which information must be “saved”

**Structure**

Information is ad hoc-structured and interoperability at different levels is fleeting at best.

**Distribution**

Darknets dominate and controlling distribution is a complex task, often impossible.

**Value**

The value of information increases with the amount of information available, to a limit, where it actually decreases.

This set of heuristics is a good start. Policy makers interested in changing their models need to pay close attention to emerging discourse and examine the failures of the old heuristics closely.

One tentative identification, then, of “Society A” is the noise society:

The noise society is a society where small-scale autonomous technologies and *kosmos* are the governing elements in social change, interacting with each-other in a way that creates a need for a new set of heuristics for policy making.

---

191
8. Summary, Objections and Conclusions

The argument in short
I have argued that many of the policy makers early policy responses to the challenges inherent in the new information and communication technologies were based on a discourse where an ordered, idealized model or set of heuristics of the information society has dominated and where the number of information producers was limited, information growth reasonable, information distribution controlled and information well-structured.

Through the use of de-scripting I have traced the set of scripts inscribed in the legal reforms of the time as well as the scripts of technological attempts at architecture regulation. I argue that they show that at least early policy making was based on such an idealized model. The data protection directive, the information society directive, privacy enhancing technologies and electronic copyright management systems have been analyzed and mined and the scripts unearthed I maintain sustain the hypothesis.

I have also argued that the information society model is flawed and that it needs to be modified, and I have tried to show that the information society model fails in a way that is systematically biased toward another model of society and social change – one characterised by small scale autonomous systems and Hayek’s conception of kosmos or spontaneous order.

I have suggested one alternative model – not excluding the possibilities that there may be others. The model is based on a radical loss of control over information production and distribution coupled with very low levels of structure in information. I called this model the noise society and I have tried to show that such a model is consistent with a) the at least partial failure of the studied policy responses and b) some of the new emerging discourses that can be discerned.

If our society is a noise society, policy makers need to have a framework for evaluating filters as policy responses and seriously grapple with the problems and challenges inherent in filtering. Not because policy makers can or should construct
large filtering solutions to all our policy challenges (this would be information-society-thinking) but because they will see filters emerging everywhere. (As we indeed they do). In analysing some examples of filtering – from ISP-filtering and spam-filtering to the use of the robots exclusion standard or protocol – I have at least substantiated the claim that filters are actually used as policy responses today and that this entails challenges that policy makers must be ready to meet. Policy makers also need to examine the emerging discourse of search in the policy process. Search becomes a value in itself, an important prerequisite for participation, openness and access.

With that I have accomplished the goal I set out to reach, but along the way we have also gained some other insights that I hope will prove valuable. I will try to summarize these below and give an overall idea of how the notion of a noise society can be explored in future research.

The changing nature of ICT-policy making
Policy making is a process that is easily influenced by its subject matter. I have tried to show that in the early policy responses to technological change we saw policy makers assuming the roles of system designer, product developer and protocol designer. The goal for policy makers was to design grand systems and global technological standards that would enable the information society.

The idea of electronic copyright management systems was to fuse policy making and technological innovation into a kind of policy-making-as-system-design approach. Our examination of early Electronic Copyright Management Systems clearly showed the visions of grandeur behind the idea and the following failures have implied that the level of control we have is far less than was imagined back then. The age of the policy-maker-as-system-designer is over.

The alternative, I suggest, is to draw from the writings of Claudio Ciborra and see the policy maker as tinkering with several different tools: organizational, legal, social, technological and economic. The policy-maker-as-tinkerer or bricoleur is a much more apt image today. This does not necessarily imply an overall postmodern view of our society, but I think that as a metaphor for policy making this is a good fit.

In designing privacy enhancing technologies we saw the policy maker become product developer. The fusion of business modelling, innovation and lawmaking into a single policy making process gave rise to companies like Zero Knowledge Systems and PrivaSeek, both now defunct. We have also seen how policy making for a while was reduced to protocol writing, and again how this failed. Again I argue that the failure comes from an exaggerated idea of the level of control exercised over the new technologies.

Looking at more modern approaches to privacy and privacy enhancing technologies we see that they build upon existing structures. I suggested that we
may explore the idea of the policy-maker-as-modder – a policy maker that takes the existing architecture and laws and modifies them slightly to achieve “mods” much like computer game players today modify games in order to adapt them to their own wishes.

Overall the changing method and metaphors for policy making is an important part of the insights I have made writing this thesis, and I think that it may actually contain not only a resignation to a bitter fate where we have lost control, but also another approach to policy making where tinkering and modding actually accomplish much more than the grand architectural schemes envisioned in early policy making.

**New narratives for privacy and copyright**

If we assume that our society resembles a noise society it seems clear that we need to find partly new narratives for privacy and copyright. In the chapters dealing with privacy and copyright I have sketched weaknesses in the current narratives. I consider the arguments presented in those chapters possible starting points for a revision of the policy responses to the challenges to copyright and privacy seen so far.

I have argued that when speaking of privacy, policy makers need to take into account the fact that we no longer live in a society where controlling personal data is an option. It is not even a desired option for many, since they freely share and impart even their most intimate dreams on the web in what more resembles an attempt to produce or construct identities. There is, I think, another part of data protection that policy makers need to look at, and that is personal integrity: the protection of and control of users’ digital persona. Again, not in an information society way, where policy makers would grant rights to control all that is said about a person to that person, and then require consent from everyone that wants to change it – that is no longer possible – but in a noise society way: they may encourage the market or others to provide filters for those that want to use them and can design laws that focus on abuse of personal data. We may provide what I have elsewhere called Jante-technologies (Lundblad, Privacy in the Noise Society 2004) that at least make it harder for others to chart what you are doing. The idea of jante-technologies is simply to design an information persona that resembles the mean within which you can hide. We need to listen to Nietzsche, when he tells us that to speak much of yourself also constitutes a way of hiding. I do not believe in the transparent society sketched by David Brin (1998) – the level of control required to achieve the transparency he envisions is not to be had – but I think that we will live in a society where anyone but not everyone can be watched and charted.

In copyright we need to adapt to a society where the conditions for creativity have changed radically. This is already happening. The projects growing now to protect the public domain or to create and sustain the Creative Commons are just two
examples. The nature of creativity in our society with its information and communication technologies is already the subject of studies and research. What I hope to contribute to that wide and growing field is the contention that creativity seems to be a default setting and that the incentive argument then at least partly fails. When we redesign copyrights we need to acknowledge this and look for ways to examine how copyright can work as a filter.

The noise society model presents scripts that the policy maker needs to take into account, I believe, for the design of future policy responses.

**Coming to terms with filters**

The filter metaphor will be a powerful tool in policy making in the noise society. Filters of different kinds are no longer optional in a noise society, but necessary instruments for the policy maker. Filtering content, personal data, speech and almost any other information is a survival strategy in a society afloat in a sea of noise.

This necessitates that policy makers look closer not only at the legality of individual filters, but at the policy making implications of using filters in different settings and between different actors. The framework I have tried to provide, analyzing the different properties of filters (architecture, transparency, predictability, content neutrality, actor neutrality, dispute resolution mechanisms being the most important ones), is at least a starting point to do so and I offer it for future revision or rejection – but I think that there is at least need for some kind of framework for analysing filters.

As seen in the cases of harmful content, spam, ISP-filtering, blog spam and the robots exclusion protocol the consequences of filtering will vary heavily depending on the design of the filter and its use. I have argued that policy makers must conceive of filters as not only architecture regulation but also look to the policies and rules set in place around their use. In analysing the contract between ISPs and the Swedish police this is clear: the contract governing the filtering is a powerful part of the filtering policy response and even leaves the question of what technology to use open.

*Filtering is as good a metaphor as I can find for policy making in the noise society. Policy makers tinker and mod technologies to filter information according to their policy targets and goals.*

**Objections**

There are a number of objections to the thoughts presented here that I would like to attempt to answer. The objections met in this short section are hardly the only ones, and perhaps not even the strongest ones, but they are ones that I anticipate. This is the reason I have included them. The objections – found below – are of varying strength and intricacy but they are important to face.
Policy makers never have a model of society or a set of heuristics in mind. This is a line of criticism that in its simplest form denies the descriptive part of my thesis. The gist of this criticism comes from the idea that policy makers merely act to maximize their short-term utilities, and this does not involve any kind of model of the society being shaped by technological challenges at all. I think this is a surprisingly strong criticism, and I concur that policy makers never have a very distinct image of the society. The model most policy makers seem to have in mind is a rough one, a sketch more than a finished painting. But they must have this, since otherwise they will simply be lost even in trying to maximize their own utilities. Policy makers must have a kind of vision of what will happen in order to react to it – assuming the opposite is absurd. The simplest case of this is the copyright holders – their model of the future has changed from one where they would control all content flows to one where they need to combat piracy. These agendas imply models of society. But I agree that if we asked policy makers they would probably not have a ready answer to questions like: “what model of society are you working with in your policy work?”. So, while I agree that policy makers rarely have very detailed models of the societies they assume, I think it is blatantly false to argue that they have no models in mind. Without some kind of at least implicit model of society there would be no policy making.

The change from information society to noise society you describe reek of technological determinism. The reason someone would say this is, I assume, that they feel that I have argued that information technology naturally evolves toward fragmentation, information overload and noise. The answer is simply that I have not. There is nothing deterministic in the notion that we have moved from the information society to the noise society, and there is in particular nothing deterministic in arguing that a noise society presents a better model for policy making than an information society.

Noise is a transitory phenomenon and new technologies will eliminate the noise effects you describe. This is a line of arguing that I have often met when discussing the idea of privacy in a noise society. Whenever I argue that the threat to privacy may actually be ameliorated by the huge masses of information available or that eavesdropping may actually be less of an infringement of my rights since the collected information sets are so huge and lack organization, I am met with a blinding faith in technology. There are two versions of this criticism. The first argues that privacy invasive technologies will develop so quickly that they will allow total surveillance in a matter of years, and that the threats to privacy are huge and growing. There is, these people tell me, no way that you can hide in the noise. The noise will simply disappear in the onslaught of these technologies and privacy will be eroded. I grant that this is a possibility. But at the same time I would like to ask those that think so to reflect over the fact that the problem they are now predicting will be so easily solved is analogous to the problem of copyright protection. And no-one ever stands up and says that the issue of piracy is a moot one because copyright protection technologies will develop so quickly as to eradicate all piracy problems. Why is this? Why do people assume that technology
will eliminate all the noise problems and all the control problems when it comes to privacy invasion, but not when it comes to piracy? Well, it might surely be argued that piracy is a much harder problem, and in a sense this may be true – but this does not invalidate the fact that control technologies for both privacy and piracy seem to be far off on the horizon. But in the end this will be an empirical question.

The noise society will not set us free. This is a line of criticism I have sometimes met and it shows my poor ability to point out that I am not an advocate for the noise society. When I argue that we need to look at a different set of policy questions in the noise society this is not said with a sigh of relief, but with a worried look. The noise society does not improve the situation for data subjects, rights holders, surveillance agencies or pirates. It merely necessitates a different approach for all the actors in the policy making process. There is nothing inherently good or bad in a moral sense about either model.

The broader idea of a noise society
The preceding sections have outlined what I think are the contributions of the work I have presented. I would now in closing like to turn to a more speculative section, discussing the metaphor of a noise society in much wider terms to expand the concept and hopefully show that it can be useful in other contexts as well.

In the broader context the noise society is a society where information production is abundant, and the information produced is non-structured. There is not necessarily information overload – in the sense that individuals feel overwhelmed – but there is an abundance of information and filtering through information is a way to create, or perhaps re-create, value out of information.

The noise society is open. The noise society is open in a very real, popperian way, while the information society is closed, opening up dreams of control and tayloristic management. Finite information sets could be used and ordered to create efficient organizations and central planning seemed more plausible than ever. The noise society eliminates all such dreams of control, and the Hayekian observation about the limits of knowledge returns with a vengeance: the knowledge problem is now not one of gathering knowledge, but one of coordinating and producing knowledge out of a myriad of data sources. The noise society is immune to historicism, since there is no one history that can be decisively deduced from the sea of noise.

In the noise society there is more information than can be utilised. One important property of the noise society is that it contains more information than we can use. Even if we applied all our time and all our efforts to sifting through the sum total of information we would not be able to use all the information available. There is – and this is only another way of saying the same thing – more information than users. We become, in a very real sense, the boundary conditions – our time, as we have seen Herbert Simon note, is scarce and that decides the amount of information we can refine into actionable knowledge.
Filters are essential in the noise society. In the noise society filters are used to refine information into actionable knowledge. This is a basic property of the noise society that differentiates it from the information society. In the information society things are filtered to avoid certain types of content and it is assumed that the sum total of all information is available for any user to access or not. Filters become access controls. In the noise society filters become necessary tools to create understandable sets of information that can be turned into actionable knowledge. Business models, art and communication will depend on filters as well. Filtering will be the basic mode of interacting in a very real sense. Noise death – losing the ability to filter – will be a very real danger to us in this society.

Filters are nothing new. This is true. There are organizations that can be usefully thought of as filters in our society today, and this has been true for a long while. Newspapers and publishers are two interesting examples. They filter information and decide what gets published and what remains unpublished. Filters are nothing new. But the dominating role of the filter metaphor or filter role in society is new. When I say that filters are necessary I mean that they are primary in interacting with society. Newspapers have grown more and more important over time, and now their work – and other filters – is necessary to interact with the world.

The noise society accelerates. The amount of information produced and stored in the world is growing at a break-neck pace. The result is a growth curve that is exponential. We do not expect this to change in the coming years, and this means that the noise society or the effects and behavioural patterns necessitated by the noise society will grow and “worsen” over time. Noise does not rot, it does not disappear. It stays with us.

The noise society creates a cyber class society. It is possible that noise will be the main differentiating class factor in the future, or rather that the quality and power of filters available to different groups will be essential to social differentiation into in-the-know strata of society and noised down strata.

The noise society will create its own form of forgetting. Societies forget in different ways. Where previous societies forgot by losing sources, documents or artifacts, the noise society forgets by retaining data. When saving all the data we create a forgetfulness based on noise, on an inability to retrieve what people in a certain age considered important data. The data, markup and use of the data may not be able to show us what was prioritized and what was thought to be inconsequential. We have seen this in discussing the privacy of cows (above) but it is even possible to expand this theme. The new kinds of forgetfulness are already evident and I imagine that examining the institutions of technological forgetting will become more and more important. Today policy makers seem to think that they can force systems to remember and forget at their will: this is the idea behind data retention rules all around the world. But technology remembers in new ways, and it is far from certain that we can control technological memories with large volumes of data.
The noise society creates an economy with filter competition, and perhaps some natural monopolies. The noise society could be expected to create an economy where businesses compete by offering the better filtering technology, at least in the information sectors of the economy. This new filtering economy will exhibit some interesting traits, if I am right, since it will be governed by two things: firstly the quality of the filtering and then the need for social cohesion around filters. We need to use filters that we share with others: both to ensure the quality of the filters and to ensure that we share a common understanding of what is important. The question here becomes if we in the noise economy will see natural monopolies for certain basic filters: these will be filters where the collective, collaborative effort is essential to the quality of the search results and where the need to be able to share a common understanding of different issues drives a high concentration of the market. Search engines come to mind: they need a high collective and collaborative legitimacy to ensure results (if they use algorithms based on collaborative filtering) and they are used in a way that suggests that we need to share the common understanding they create. We need to be able to tell someone to “search for it” and then know that the results will appear in the first ten hits.

The noise society may strengthen and extend identities built on common use of filters. We already see that to some small extent people define themselves as readers of certain newspapers (and newspapers are after all a kind of filter). It is possible that this social identification process will become even stronger in the noise society, since the filters employed will be even more necessary and the knowledge we gain will depend on the filters to a higher degree.

The noise society will change education thoroughly. I concur with science fiction writer Vernor Vinge, who in his recent book Rainbow's End surmised that search and analysis would become essential subjects to teach in school. I also think that being able to use, manipulate and fine-tune filters will be a valuable skill on the future job market.

The noise society will increase the importance of governmental filters. This question is actually not new. Cecilia Magnusson-Sjöberg has pointed out that the question of what e-mails can be filtered away by government authorities is really a question of democratic access (Magnusson-Sjöberg, Nya lydelsen av 5 § förvaltningslagen – inte bara en kodifiering av praxis. 2004) and it is important to realize that this is the case for all public sector use of filtering (my own example with the robots exclusion standard or protocol shows a version of this argument).

The noise society is a set of heuristic principles. One way of conceptualizing the utility of the idea of a noise society is to use it as a policy heuristic. As Wimsatt (2007) points out much of the social sciences – and the policy sciences – should strive for robust heuristics for handling complex and messy problems. The model of the noise society developed here is a rough heuristic for addressing legal and policy problems.
The noise society is not a new phenomenon. The lack of control and the idea of technology drifting are ideas that have been around for some time. The exception from the rule is really the rather utopian view of the information society as a society where we could control and command technology with great accuracy.

With these general suggestions and ideas I end this work. The entire dissertation is available as a wiki on http://www.noisesociety.com and I will endeavour to contribute updates to this web site over time.
References


207


Stenmark, Dick. *Designing the new intranet (Gothenburg studies in informatics 21).* Gothenburg: Gothenburg University, 2002.


Gothenburg Studies in Informatics

ISSN 1400-741X (print), ISSN 1651-8225 (online)


