Privacy in the Noise Society

Nicklas Lundblad

1 Introduction

This article argues that the threat to privacy today is fundamentally different than has been thought to be the case. The costs of control through the use of personal data are such that it is impossible to control an entire society through that mode of control. We live, the article argues, in a noise society where the amounts of information produced can actually work as a kind of protection for privacy.

If this indeed is the case, the legal considerations of privacy and the design of privacy enhancing technologies may well have to be adapted to this new model in different ways.

The rise of the information society has been accompanied by ever increasing worries about the coming erosion of privacy. One of the basic factors behind the fear of "an end of privacy" has been that automated collection and processing of personal data will simplify control to such a degree that it is possible to control entire societies with the help of information technology.[1] Such Orwellian control or surveillance societies would use the data about individuals to manipulate, scare and oppress them.

The fear that such a society may arise can be seen as based on two different assumptions.

The first assumption is that the amounts of information that has to be collected and structured is reasonably manageable in size and complexity. As the personal data and information sets grows, the costs for collecting and structuring data also grows, until they at one point become too burdensome for the would-be surveillance apparatus. It is thus a necessary condition for the rise of a big brother or surveillance state that personal data can be collected and structured within the costs affordable to that society. We will term this assumption an *assumption of cost efficiency*.

The second assumption is about the quality of data. If we assume that data can be used to control people we must assume that the accuracy, depth and sustainability of data are at levels sufficient to to allow the data to be used in a control structure or a control system. If we assume the opposite – data that degrades so quickly that it is inaccurate and passé before it can be used to control anyone – we may well have a random, inaccurate dictatorship, but not an Orwellian big brother society. We will call this second assumption an *assumption of data quality*.

It is useful, in the general discussion about privacy dystopias, to discern between two different kinds of control states. The first is a society that actually bases its control on the collecting, analysis and use of personal data – a society we could call an authentic Orwellian big brother society.

The second kind is a state that does indeed collect enormous amounts of data about its citizens, but where the collection itself is meant to intimidate and control the citizens. In the first kind of society the state uses the erosion of

1 The prediction of an end or death of privacy has become mainstream. *See* for example Whitaker, R., *The End of Privacy: How Total Surveillance is Becoming a Reality*, (The New Press, 1999) and Sykes, Charles, *The End of Privacy* (St Martins Press 1999) *See* also Garfinkel, S., *Database Nation: The Death of Privacy in the 21st Century* (O'Reilly 2000).

privacy to gather information that is then the driving factor in the mechanisms of oppression. In the second kind the information gathered is secondary, and the driving factor is the wide-spread impression that the state collects enormous amounts of information about citizens.

This difference is important, since the quality of data in the second case is basically irrelevant. As long as the citizens can be made to believe that the information gathered about them is truly accurate, they will act as if they lived in a big brother state with accurate information about them, but the basis of power for the second kind of state is this fear of surveillance, rather than the facts gathered through the surveillance itself.

Both these assumptions, of cost efficiency and data quality, can be, I suspect, successfully challenged. This means two things: firstly that we need not fear the rise of an Orwellian Big Brother society, and secondly that we have to restructure our understanding of the threat to privacy, since the threat to privacy in no way is eliminated by the alternative perspective.

In summary: the amount of information in the developing information society is very large and growing quickly. This offers new challenges and perspectives for the privacy discussion. In one possible analysis this growth of information will lead to beneficial effects for privacy by raising the costs for surveillance. This effect, here tentatively termed the *noise effect* will however not protect individuals or increase their *individual expectation* of privacy directly. Instead it will increase the *collective expectation* of privacy. Here the consequences of living in a society with a high collective expectation of privacy, but with a low individual expectation of privacy are described, for the privacy debate and the design of privacy enhancing technologies along with an analysis of the factors leading up to the identification of this class of society.

In other words, this paper seeks to map out the consequences of living in a world where *anyone*, but not *everyone* can be mapped in detail. In such a society we do not have the right to be let alone – as privacy was once defined - but we will most likely be let alone if we do not draw attention to ourselves.[2]

2 A Tale of two Futures

There are at least two major scenarios for the future of privacy clearly discernable in the discussion today.

The first is a scenario in which our society develops efficient technologies of control and where privacy is as good as abolished. This *control society* exists in two different versions: one is an Orwellian society where the consequences are bleak and individuals oppressed with the mechanics of fear or the sedatives of pleasure (Orwell's *1984* and Huxley's *A Brave New World* are good examples of this).

The other is a vision of a transparent society in which individuals are empowered by the new accountability inherent in such a control society. In this second kind of society the loss of privacy is compensated by the rise of a new

2 *See* for this definition of privacy, Warren, S. and Brandeis, L., *The Right to Privacy*, 4 Harvard Law Journal (1890).

accountability, much along the lines sketched in Jeremy Benthams *Panopticon* – which of course depicted a prison rather than a model society. Most writers today seem to gravitate towards the dystopian view of the future.[3]

The other alternative is a *privacy-enabled society* driven by encryption, privacy enhancing technologies, legal frameworks and social awareness of the value of privacy. This scenario has fewer proponents in the literature,[4] but it seems to be the motivating force behind the development of privacy laws and privacy enhancing technologies such as the European Data Protection Directive (95/46/EC).[5]

Both of these scenarios lack in realism, for the same reason. Both describe *high cost societies* that are unstable over time due to the enormous costs inherent in their structures. To prove this in detail is hard, but general estimates can strengthen this hypothesis.

Before we turn to examining these costs in detail, however, it is necessary to discuss what the costs are and how we can model them in general.

3 Data, Information and Knowledge Costs

There is an old trichotomy in informatics that is useful when studying questions about privacy and that is the trichotomy between data, information and knowledge. The differences between the three terms can be summed up, roughly, so: data is structured into information that is interpreted to become knowledge. Data are unstructured facts about the world in general. When they are put into relationships and structured in different ways they become information. When information is interpreted by an information consumer, the information becomes knowledge.[6]

A number of different criticisms against this conceptual model have, probably correctly, been introduced in the debate. In this article, however, the model serves as a useful tool to show the cost structures of privacy invasion.

If we study the process of privacy invasion closely, we find that it is a gradual process. If we apply the three concepts above, we can model privacy invasion as a process with three distinct steps.

1) The collection of personal data. This is the first stage, where data is collected to start the process of mapping an individual or finding out something about him or her.

---

3 David Brin being the notable exception. *See* Brin, David, *The Transparent Society: Will Technology Force Us to Choose between Privacy and Freedom?* (Perseus 1998).

4 Overall it can be noticed that there is little end state utopia discussion in the privacy debate today. The dystopias abound, but the utopias are few.

5 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Communities of 23 November 1995 No L. 281 p. 31.

6 *See* Ackoff, R. L., *From Data to Wisdom,* Journal of Applies Systems Analysis, Volume 16, 1989 p. 3-9. I have not used the two remaining levels in Ackoffs model: understanding and wisdom, even though I think that they may have some application.

2) The structuring of this data into personal information. In this stage the data collected is structured and ordered in relations of different kinds.

3) The interpretation of personal information as to give knowledge about this person. At this stage someone interprets the information resulting from the second step.

These three steps can be complemented –from a privacy invasion perspective – with a fourth step:

4) Dissemination of knowledge about a person. This is an additional stage, where the privacy invasion is continued by further spreading the data at hand.

These steps can then be arranged in a diagram to show how a privacy invasion process actually looks. In a quick sketch:

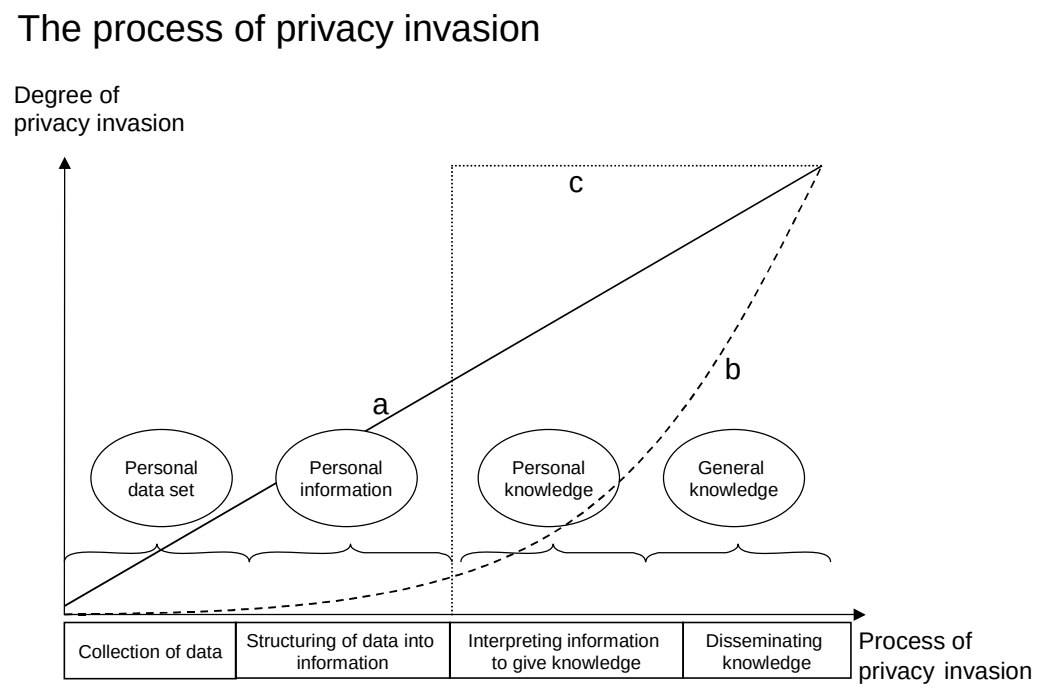

Fig 1: The process of privacy invasion

The four stages of privacy invasion in this simple model have distinctly different costs, and we will return to this issue below in trying to map out costs for the different societies we will study and discuss. The different stages also have different objects of legislation – both processes and results. We can regulate the handling of personal data, personal information and knowledge about a person.

We can also regulate the processes of collecting, structuring, interpreting and disseminating information in different ways.[7]

The sketch also shows that it is possible to have different ideas how and to what degree privacy is invaded. The different curves a, b and c show possible views on what degree of privacy invasion the different steps represent. In short the different curves can be interpreted as follows.

a) *Privacy is invaded gradually, linearly through the different stages of the process*. This curve shows the view of those who mean to say that all stages of the process are equally invasive and that all steps mean equally much.

b) *Privacy is invaded exponentially, and really is invaded only in a more serious sense when the information gathered is interpreted*. This is a view that would probably by argued by those, like myself, who claim that only humans can invade each other's privacy in any more meaningful and harmful way. Up until the point where someone actually interprets the data and personal information generated, the level of privacy invasion is only very low, a potential invasion.

c) *Privacy is invaded only, but totally, when someone interprets personal information*. This is an extreme view that very few people probably agree with. The point of showing this curve is that the point at which the total and utter breach of privacy occurs can of course be varied. The most hardcore privacy position would be to say that at the very moment collection of personal data is initiated – privacy is lost.

Both the stages of privacy invasion and the ideas on how privacy is invaded will be useful later, when we discuss objections to the idea that we are living in a noise society.

4 The Cost of Control Societies

Surveillance or control societies are costly. The costs involved are many, but some of the major *direct* costs are:

- *Collection of data*. Data has to be collected. This may well be a cost that rises linearly with the number of subjects that are under surveillance

- *Classification and structuring of data into information*. Data has to be structured to be searchable and of use to a surveillance society or even a "little brother"-society. This may well be a non-linear cost that grows quicker, the larger the number of subjects under surveillance. Consider the

7 For more on the object of protection and theories on what privacy actually is – *see* Strömholm, Stig, *Integritetsskyddet - Ett försök till internationell lägesbestämning* in SvJT 1971 p. 695.

fact that the more subjects, the more relations between them that have to be mapped and understood.

- *Interpretation of information to achieve knowledge about the subjects under surveillance*. The cost related to actually evaluating and following the information generated from the data collected must not be ignored. The cost of employing surveillance officers of different kinds is one that is not easily reduced by technological innovation.

- *Archiving, format conversions, storage*. Data has to be stored over time to be valuable, and that means format conversions, storage and other such costs have to be covered. A hypothetical surveillance society that started in the early 1970s would be highly inefficient with legacy systems and format problems.

There are also numerous indirect costs. It can be argued that innovation and entrepreneurship would be obliterated in a surveillance society, and that a society constructed along the lines of the panopticon quickly would become economically stagnant. The argument, in short, would be that innovation and entrepreneurship requires a certain amount of privacy to arise and grow. Innovators are motivated by the possibility of making money from their innovations, and in a completely transparent society very few secrets could be kept – thus innovations would possibly be copied and/or stolen before the innovators could benefit from them. Entrepreneurs need to assess and work from information that is not accessible to everyone, and if they could be watched around the clock, a new breed of meta-entrepreneurs could settle down and just observe the entrepreneurs and copy what they did – significantly lowering the incentive for the original entrepreneurs.

Overall these costs would create a heavy burden on the surveillance society, and reduce the economic efficiency of such a society to such a degree as to destabilize the whole society. Orwell's dystopia would collapse on itself due to economic problems.

It should be noted here that this also applies if the information gathered is incorrect, since also incorrect information can be used to exercise control, but that such a society would not be a clear cut Orwellian control society. A society attempting to scare subjects into submission by pretending to know more about them than they do would probably destabilize even more quickly – leading to both transaction costs and surveillance costs in excess. It is less costly to gather incorrect information (one could apply less exacting standards to data collection), but instead it becomes more costly to rely on and act on such data (assuming that someone is trustworthy from incorrect information can lead to direct costs of being defrauded, for example). The threats of such an oppressor would soon be discovered to be empty.

A corollary to the observation that a control society would collapse under its own cost structure is that there exists what we can term a *privacy border* (see fig 2), a point at which the control costs grow so quickly that it is not possible to control more users or citizens.

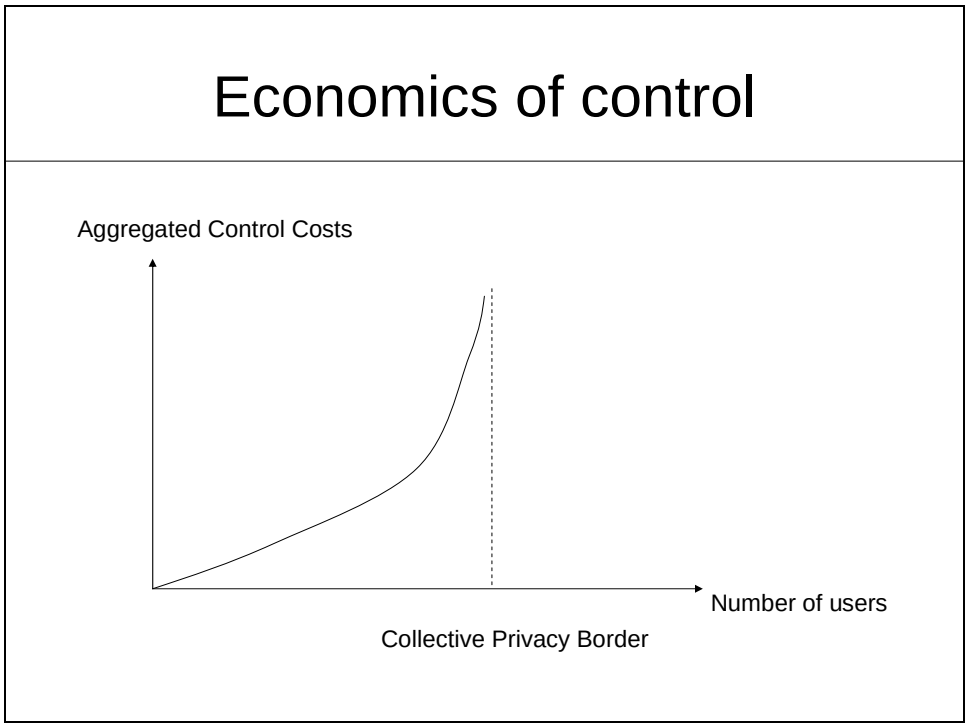

Fig 2: A privacy border

This privacy border is affected by two important tendencies in modern society: the innovation of technology and the growth of information. The first of these produces ever new forms of personal data. The computer, global networks, and the mobile phones have been necessary for computerized records, click-stream data and location data, and in a sense produced these forms of personal data as an unintended consequence of technological innovation.[8] The second ensures that information exists in abundance and that it is costly to collect data on individuals. If we add time to the equation we see that over time it becomes even more complex to control data, since formats, technologies and user patterns change.

8 *See*, on the idea of technology producing the object of privacy protection, for example Blume, Peter, *Privacy as a Theoretical and Practical Concept* in International Review of Law, Computers & Technology Vol 11 No 2 October 1997 p. 195.

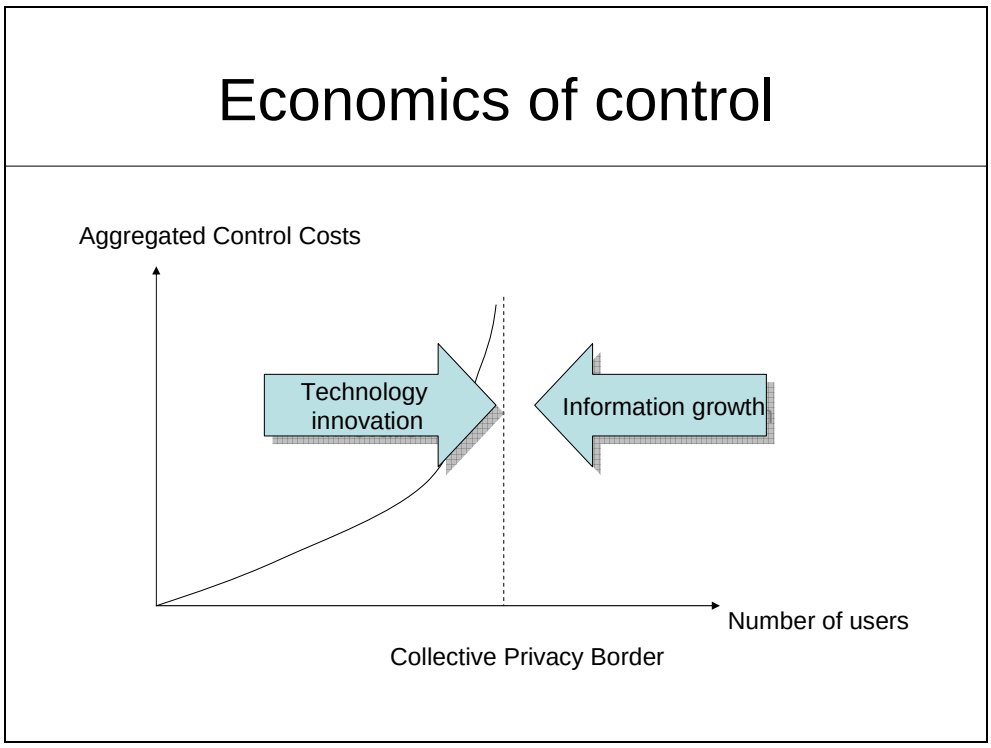

Fig 3: Privacy border forces

Law has to handle this complex interaction, and we will return to a discussion of how this can be done.

In summary then, we see that control societies are high-cost societies that seem unlikely to arise. Should they do so, they seem unstable and likely to collapse. It is perhaps not an unimportant piece of empirical evidence that we see no Orwellian big brother societies in the world today.

5 The Costs of Privacy Societies

Privacy societies are also costly. Managing and safeguarding personal data is not a cheap process. The costs encountered in privacy societies are of a slightly different nature. The direct costs are straightforward:

- *Administration and interpretation of privacy laws*. The European data protection directive has cost enormous amounts of money. Adapting systems, developing interpretations of what is a generally worded law and handling request for personal information from customers is costly.

- *Investments in privacy enhancing technologies*. To be able to maintain the levels of technological development we have reached it would be necessary to invest heavily in privacy enhancing technologies of different kinds to ensure that privacy expectations remain high both collectively and individually.

There are also indirect costs for a privacy society. One of the perhaps most interesting is the expected growth of crime and fraud rates in a society which goes to extremes in protecting personal data. As Richard Posner has pointed out privacy is oftentimes used to conceal less appetizing data about subjects in different ways.[9] These costs could, in the end, also prove destablizing and harmful to the vision of a privacy society. The right to be let alone comes with a price tag that might be higher than usually expected.

Privacy enabled societies might also suffer from indirect costs in that exaggerated levels of privacy may well hamper freedom of the press, knowledge exchange and social life in general. This in itself may well also have innovation dampening effects. It is, however, hard to lead into evidence directly.

6 Noise Society – Our Society?

An analysis of cost structures gives evidence that seems to imply that we live in a society that is neither a privacy nor a surveillance society. Peculiarly we seem to be living in a society that is a mix of both. The reason for this is simple: the cost of amassing data on individuals is significant to any attempt of mapping large populations. We live in a society where it is possible to chart the life of anyone, but not the lives of everyone.

Another way of putting this is to say that we have a *high collective expectation of privacy*, but a relatively *low individual expectation of privacy*. One important reason for why this is the case is that the amounts of information at hand and the rate at which new information is produced seem to ensure that it is costly to invade everyone's privacy. We could, for that reason alone, tentatively term this kind of society a *noise society*. Noise levels in general ensure that collective privacy is good, while individual privacy is almost obliterated. (see fig 4)

9 *See* Posner, R. (1981) *The Economics of Justice* (Cambridge, MA: Harvard University press).

Society matrix

	Collective expectation of privacy		
Individual expectation of privacy		*High*	*Low*
	High	**Privacy society**	**Ant hills, hive minds and "statistical societies"**
	Low	**Noise society**	**Surveillance society**

Fig 4: Society Matrix

What, then, is *noise*? According a simplified interpretation of the model launched by Claude Shannon we could say that noise is anything that distorts or destroys the communication process.[10]

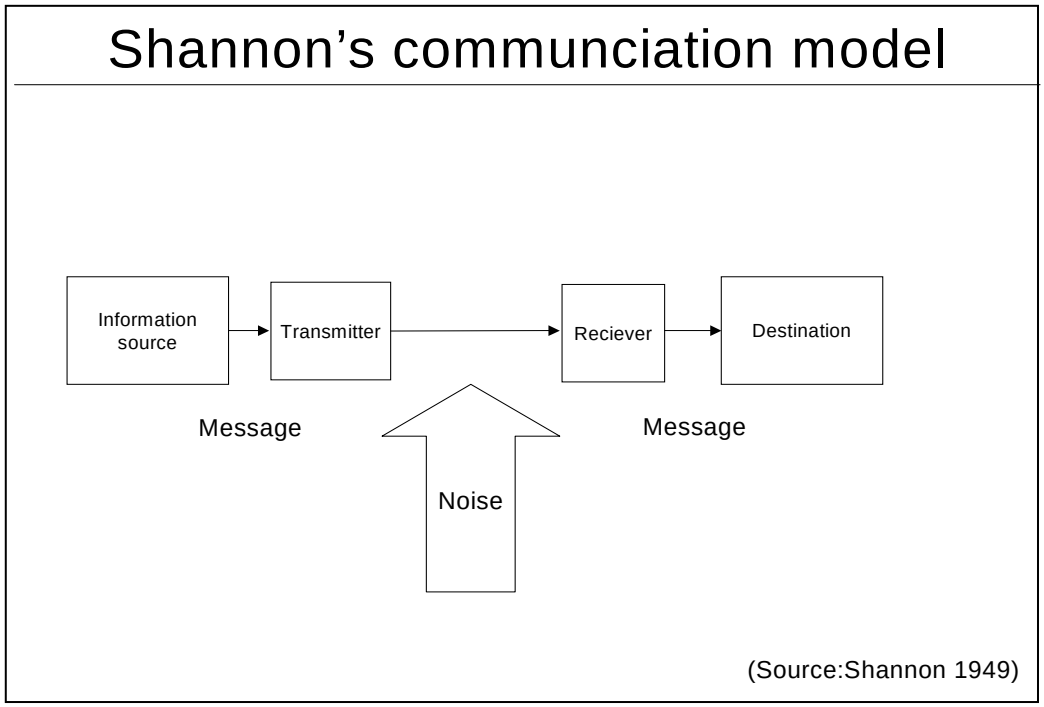

Fig 5: Simplified rendition of Shannon's model

10 *See* Shannon, C., *A Mathematical Theory of Communication*, The Bell System Technical Journal, Vol. 27, p. 379–423, 623–656, July, October, 1948.

It is in fact possible to claim that privacy invasion can be modelled as a form of communication process, where the receiver tries to extract as much information as possible from the sender, and the message contains personal data. Thus it becomes clear that anything that interferes with this process can be regarded as a kind of noise.

Noise does not necessarily need to be unstructured information, It can in fact be highly structured contradictory information that is inserted into the privacy invasion process, and thus must be evaluated to achieve the attempted privacy invasion. If someone gathers a lot of personal, but inaccurate data, structures them into information and interprets them, there has not been any invasion of privacy at all. If the false interpretations are disseminated this may constitute a form of libel, but this would not be privacy invasion in the sense that the concept is used in law.

If we apply the trichotomy we introduced above we see that we can discuss different kinds of noise that occurs at the different stages of a privacy invasion attempt.

1) *Data-related noise*. This kind of noise would occur when someone is attempting to collect personal data. The sheer amount of information may in some cases occasion noise effects, where it is not possible to collect all the available information.

2) *Information-related noise*. This kind of noise would occur when the data is being structured as information. Data sets may contain incoherencies or contradictions that make it impossible to structure the data received as information.

3) *Knowledge-related noise*. This last kind of noise is related to interpretation of the information structured from the data collected. It may be simple information overload, or contradictions with earlier knowledge held by the interpreting entity.

These different kinds of noise all arise from the wealth of data available electronically, and lowers the probability that any given privacy invasion will be successful as well as the probability that all would-be surveillance subjects can be controlled.

For the sake of completeness it is also possible to include a strange and unusual kind of society where the collective expectation of privacy is low, and the individual level of privacy is high. This could typically be oppressive states in which the individual holds no meaning, ant hills, science fiction hive minds such as the borg of popular television show *Star Trek* (all the individual borgs have excellent privacy, because they are not interesting as individuals, only as a collective) and other such anomalies. Other suggestive examples include youth cultures, saunas and different military groups, where the individual level of privacy is high, but the collective is expected to be transparent to a high degree.

It is hard to grasp how such a society would be structured however, where it is possible to map everyone, but not anyone. One possibility of course would be

that this refers to the kind of societies where there truly is no individuality, and thus not any *one* to control. (Clone societies would come to mind, where there is really only one individual.)

7 Consequences for Designing Privacy Strategies and Privacy Enhancing Technologies

What kind of changes does this imply for privacy strategies and the design of privacy enhancing technologies such as platform for privacy preferences (P3P)?[11] Today these technologies are varying and span over a wide range of different designs, but have some common qualities.[12]

The guiding principle in a noise society seems to be not to attract attention. Any individual that wants to protect his or her privacy must blend in with the crowd. Some examples of strategies that would probably be recommended are:

- *Avoid the use of encryption.* The use of encryption clearly signals that what you are doing is interesting. Encrypted traffic in and of itself is interesting in a society where the lack of encryption is the norm. (In situations where it is not, this does not apply – see for example the abundant use in e-commerce transactions of SSL) Traffic analysis singling out encrypted traffic as such may be quite common today. In a noise society the preferred method of protecting information is not encryption, but rather methods such as steganography. One of the most interesting examples of this is spammimic.com, allowing the user to hide secret messages in e-mail that looks like spam.[13] Forcing surveillance to sift through the massive noise generated by spammers is one good way of protecting secret information. Ironically this may mean that the fight for free encryption, although won, was of little use to enhance privacy.[14]

- *Avoid explicit resistance to the system.* When called upon to partake in a census or survey, it is best to do so but leave data that is of lower quality or simply false – but not in a signaling way! Do not give your wife's name as

---

11 For an overview of this standard *see* "http://www.w3.org/P3P/" [2004-05-27] or Cranor, L., *The Platform for Privacy Preferences*, Communications of the ACM, February 1999 vol. 42 no.2 p. 48-55. A critical view is provided in Clarke, R., *Platform for Privacy Preferences* in Privacy Law and Policy Reporter 5, 2 (July 1998 p. 35-39).

12 *See*, for an overview, Burkert, H., *Privacy Enhancing Technologies: Typology, Critique, Vision* in Technology and Privacy: The New Landscape (red Agre, Phil och Rotenberg, Marc) (MIT Press Cambridge, MA 1997) and Burkert, H., *Privacy Enhancing Technologies and Trust in the Information Society* International Conference on "The Information Society, the Protection of the Right to Privacy" (Observatory "Giordano dell Amore" on the Relations between Law and Economics) May 16 - 17, 1997, Stresa, Italia.

13 *See* SpamMimic, "http://www.spammimic.com" [2004-05-28].

14 *See*, for a discussion of this fight, Diffie, W. and Landau, Susan, *Privacy on the Line: The Politics of Wiretapping and Encryption* (Cambridge, MA: MIT Press 1999) and Levy, S., *Crypto: How the Code Rebels Beat the Government - Saving Privacy in the Digital Age* (2001 New York:Viking). The importance of cryptography would grow if more people used it. Today it only signals that you are doing something interesting.

> Aphrodite, the Love Goddess, but rather as Anna instead of Emma. (Clearly, being a privacy advocate is a dead giveaway signaling that you should be the focus of attention.)

In the design of new privacy enhancing technologies, the notion of a noise society offers important advice. The notion of blending with the crowd is not new in this context. Indeed there even exists a project which has taken "Crowds" as its name, the slogan of which is "anonymity loves a crowd".[15] However, these technologies are still obvious in that they are divorced from the regular networks. The notion of a noise society calls for a new subset of privacy enhancing technologies that can be called Jante-technologies after well-known Scandinavian author Aksel Sandemose who coined the phrase "The law of Jante". The law simply states that "You should not believe that you are somebody" and Jante-technologies would be privacy enhancing technologies that ensure that you never go from being nobody special to being somebody in particular.

Examples would be technologies to ensure that and individual user's e-mail traffic resembles statistical means, that the number and size of e-mail sent from the user's address does not deviate much from that of other users in the network, or technologies that create behavioral patterns in surfing based on average statistics, as to disable profiling in different ways. Another possible Jante-technology would be a noise generator, which takes as its input a typical page on a website, and then generates thousands of copies of that page with uniquely changed numbers, letters, words and information. Search engines have no way of knowing which web page is the original since information is heterarchical in most cases(if they are all named with some kind of random numbers for example), this would inject massive amounts of noise into the search engines, especially if the random pages are linked to each other to achieve a basic link density.

In summary, it seems obvious that designing technologies for privacy protection in a noise society would pose slightly different challenges than the same design would in any of the other societies. It also seems plausible that the design of noise generators and noise steganography methods would be a pattern that increased overall noise, thus raising the expected level of privacy for all.

8 Consequences for Designing Privacy Legislation

A noise society is not necessarily an ideal society for the individual. There are many weaknesses in a noise society, which need to be addressed. The perhaps most important such weakness is that a noise society fails badly: when someone really wants to invade another's privacy this is possible, and the results can often be tragic and horrible.

---

15 *See* for an introduction Reiter, Michael, Rubin, Aviel, *Anonymous Web Transactions with Crowds* Communications of the ACM, February 1999, Vol. 42, No. 2 p. 32-38.

In the case of Amy Boyer both of these adjectives apply.[16] Amy Boyer was the victim of stalker and weapons enthusiast Liam Youens, and decided to move to escape Youens attentions. He, however, acquired her personal data through an online information agency called *Docusearch*, an organization with the motto "as intrusive as you want us to be", and continued to seek her out. In the end he killed first her, and then himself, on the 15th of October 1999. This would perhaps only be a sad case proving the importance of privacy, if it were not for the fact that Youens had published a web page stating his intentions clearly. The following is only an excerpt, but it shows Youens' intentions:[17]

"I would just like to say that.. people are idiots and the world is full of bullshit. People who commit murder like this are never considered 'justified' nor will I, but who's going to stop me, you might as well murder me your-self. The people on Woodbury Drive are 'Protecting' Amy and say -> 'we make Amy safe from Liam..' ooo you put the cars off the street thats sooo scarey.., The NPD believed it could prevent me from getting guns HA! like that incident would make me change my mind, and they accually believe it. Some people thought that me working at 7-11 was hilarious, Idiots! the only reason I would get that job would be to spend every cent I earned on powerful assualt rifles to execute my vengence. As for Graeme's story I know exactly what he was saying to me, as if I didnt already view all perspectives. What a fool to think that I was That type of person, I have Always lusted for the death of Amy. Guess what Graeme I was depressed not for the love of Amy, but because I was unable to Kill her in school. How Pathetic Graeme and Bethanie are. Amy too, although she eventually realized I would kill her, she did not know that whatever she or anyone else did, it would not change my state of mind. Amy ruined her friendship with Bethanie for no reason."

A quick search on Youens would have shown the firm providing him with information on Amy Boyer what he intended to do with that information, and would have given the firm some idea about what kind of person Liam Youens was.

Boyer's parents opened a civil suit where they claimed that the information provider had to have some kind of responsibility for what happened. The New Hampshire supreme court answered, in a, that this indeed was the case. The court writes:[18]

"The threats posed by stalking and identity theft lead us to conclude that the risk of criminal misconduct is sufficiently foreseeable so that an investigator has a duty to exercise reasonable care in disclosing a third person's personal information to a client. And we so hold. This is especially true when, as in this case, the investigator does not know the client or the client's purpose in seeking the information. "

---

16 *See* for a short overview Lundblad, N., *Amy Boyers död blottlägger informationssamhällets brist* in Axess April 2003 p. 8-9.

17 From Amy Boyer's memorial website "http://www.amyboyer.org." [2004-05-27].

18 New Hampshire Supreme Courts Statement HELEN REMSBURG, ADMINISTRATRIX OF THE ESTATE OF AMY LYNN BOYER v. DOCUSEARCH, INC., d/b/a DOCUSEARCH. COM & a. Argued: November 14, 2002 Opinion Issued: February 18, 2003 "http://www. courts.state.nh.us/supreme/opinions/2003/remsb017.htm" [2003-04-04].

The case shows two things. The first is that a noise society, if indeed we live in such a society, in no way offers protection to individuals who are threatened by someone intent on finding information about them in particular. Noise, in itself, can only protect against parties that do not know for whom they are looking. The second thing the case implies is that privacy regulation in the noise society can be built on the notion of information liability or "abuse of information". This is also one of the main themes in an amicus brief submitted by the Electronic Privacy Information Center (EPIC). Epic argues:[19]

"Private investigators and information brokers have a legal duty to act with due care toward the subjects of their investigations. Because of their unique knowledge of the sensitive nature of the information they uncover and the intentions and background of the clients who request that information, these investigators are in a position to judge the possible harm that could result. In this case, the harm was eminently foreseeable based on the Defendants, own knowledge and the danger inherent in the information they sold. Further, without an effective tort remedy, private investigators and information brokers would rarely be held accountable for their contribution to the harm experienced by victims of stalkers and identity thieves."

In Sweden the post-personal data directive discussion centred on the notion of an *abuse model* rather than a *use model*, and the general idea was that it would be more logical to construct rule sets focusing on abuse of personal data, rather than rule sets that in detail laid out how personal data could be used.[20] It quickly turned out that this was difficult, since it is difficult to define abuse. The Boyer case seems to offer a principle, however, that could be used as a starting point for a renewed discussion on abuse models of privacy legislation.

If we view the issue of privacy as an issue of what is communicated with whom, and put a duty on the sender of information to ascertain as far as possible the use to which the information will be put, we have a proto-model of a regulatory alternative to regulating all handling of personal data. Obviously, this is no solve-it-all-solution, but it at least is a starting point for a discussion in general.

Another way of analysing the possible impact on regulatory solutions that the notion of a noise society would have is to examine the basic principles of privacy in the light of our new model. The Organization for Economic Cooperation and Development 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.

---

19 *See* Electronic Privacy Information Center Amicus Brief in the Amy Boyer Case, THE STATE OF NEW HAMPSHIRE SUPREME COURT 2002 TERM CASE NO. C-00-211-B ESTATE OF HELEN REMSBURG Plaintiff-Appellant v. DOCUSEARCH, INC., ET AL. Defendants-Appellees ON ORDER OF CERTIFICATION PURSUANT TO RULE 34 FROM THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEW HAMPSHIRE AMICUS BRIEF OF THE ELECTRONIC PRIVACY INFORMATION CENTER STATEMENT OF AMICUS CURIAE. "http://www.epic.org/privacy/boyer/brief.Html" [2005-05-24].

20 *See En missbruksmodell?: observatoriets överväganden om vissa frågor rörande PUL och om utformningen av en missbruksmodell*. (Det IT-rättsliga observatoriet, 1998– 8).

The OECD's principles are simple and the standing and position of these principles is undebated. 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:[21]

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."

This principle clearly is less important for an individual in a noise society. The mere collection of personal data is not the problem – since there is already an abundance of personal data in the noise of the net. The need for controlling the collection process is at least less than in a control society where all data can be assumed to be correct and usable to manipulate individuals.

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."

From the perspective of a noise society, this principle alone would eliminate much of the threat to an individual's privacy. If the party collecting data was obligated to control the accuracy of that data, the costs for collecting data would quickly become staggering. This principle should be kept and developed, perhaps even stricter applied in a noise society – offering protection through unreasonable costs for evaluating data collected.

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."

Again, this particular principle seems less important in a noise society. In a noise society citizens can allow information to be collected, and as a matter of fact would prefer that the collector did not have to communicate or examine the individual whose data was being collected in such a degree as to give a purpose or a use for the data. Remaining anonymous, and claiming no special rights, would in many cases be preferable.

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."

---

21 *See* OECD Privacy Guidelines "http://www.oecd.org" [2003-04-07].

Also this principle seems less important. Consent implies contact, which the subject of the data collection should avoid not to be noticed. If we assume that we live in a society where anyone, but not everyone, can be mapped the important lesson remains that we should not deviate from the general pattern. Any principle that requires contact or consent opens up possibilities for being observed by the data collector.

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."

This is a very general principle that is not necessarily affected by the notion of a noise society. It might be thought less important, since if the systems are not secure, the levels of noise will simply be higher.

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."

This may be a good principle, if we assume that we are going to build a regulatory model that imposes a duty of care on information dissemination practices. Knowing who the data controllers are is then important.

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

On the same reasons as above, this is not a beneficial principle in a noise society. Any individual that exercised these rights would deviate from the crowd in such a way as to lose what little anonymity he or she had left. Giving direct rights to data subjects is not necessarily a regulatory model that is compatible with the notion of a noise society.

Accountability Principle

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

Again a very general principle, that seems to be good in any of the societies discussed.

In summary then, the regulatory models in a noise society may well be different from those envisioned for the information society. Less stress might be put on the rights of an individual, since he or she will be loathe to exercise those rights and draw attention to him or herself. The general duties of care in disseminating information and demands on the quality of data can be tested by third parties in different ways, and thus need not expose individual citizens in a way that cost them their anonymity.

Not completely different regulatory ideas, but ideas with a different emphasis.

9 Objections

One objection to the idea of a noise society is that the technological development is so powerful that it efficiently obliterates the possible noise costs generated by information overflow. This objection is valid, and can draw empirical support from the current developments in information management and data mining. Translated into an economic argument, this objection seems to state that the costs for invading privacy will shrink and disappear in the wake of technological development.

This view, however, can be analysed further. As shown above, the process of privacy invasion consist of several different steps: collection, structuring, interpreting and disseminating privacy data, information and knowledge. Will we see the same cost reductions at all stages of the privacy invasion process?

I think that it is at least possible to argue that technological development will definitely lower the cost of collecting and disseminating data. Developments in data mining may well also lower the costs of structuring personal data into meaningful personal information. But will technological development really lower the costs of interpreting data? Perhaps. Developments in human-computer interaction and information visualisation may well reduce the costs for interpreting information into knowledge. But how much? It is reasonable to observe that the amount of time accessible to the interpreters is limited, and that the technological development today has done little to alleviate the information stress shared by many individuals. While the architecture of the information society might become more and more efficient at collecting and even structuring personal data, it is far from certain that the users of the information society will actually be able to use all the data collected to control each other – unless control is highly automated and mechanised.

This is a crucial question only if one, as I do, thinks that privacy is invaded only when another human being interprets personal information and thus gains access to personal knowledge about me. If we instead argue that the big brother state will be automated, and oppression and surveillance automatic, we find yet another interesting distinction to make in our studies of privacy: one between the

big brother society, where humans control humans (albeit with the help of computers), and the *big box society*, where computers control humans. This is an important dichotomy. For one thing the big box society assumes a development in artificial intelligence that we have yet to experience. The fear of big box is a different fear than the fear of big brother. It requires different legal means to be addressed as well.

A big brother society would have to be met with rules on handling personal data, information and knowledge, with the aim of regulating human users. A big box society would have to be met with rules on the construction of architectures, and the limitation of autonomy of computers in processing decisions based on personal information.

The objection that the technological development will eliminate all the noise costs is thus far from easy to prove, and turns out to lead to another question: against what kind of future society are we applying countermeasures?

A second objection can be made to the assertion that both control societies and privacy societies are economically unstable. It might be stated, with some force, that there is no empirical evidence to suggest this. The model I have sketched is just that, a sketch, and some readers may well think that both of these societies might be economically stable.

My only defense here is the fact that we nowhere have seen the rise of either privacy societies or control societies. In spite of the fact that we have lived through a period of intense technological development, we have not seen the rise of an Orwellian control state anywhere. This, in itself, may well be taken to mean at least something. I have offered one possible explanation for this fact – these societies are economically unviable. Those who argue that they are not should feel compelled to offer another, alternative explanation.

A third objection can be made from the fact that I seem to have adopted a very strict position on what would constitute a control society or a privacy society. These societies, it might be argued, are extreme models that we never expected to see in real life, and the issue at stake is not whether or not we will have complete Orwellian control societies or complete privacy protection societies. Rather, the issue is how we avoid ending up in a position that comes close to the Orwellian alternative.

This point can be reinforced by pointing out that I have not dealt with the problem of the little brothers – all the businesses collecting personal data. Indeed, it might be said that the problem addressed here – if we will end up in a control or a privacy society – is not a real problem at all. The problem is the gradual erosion of privacy by the multitude of actors in the personal data market, and the resulting insecurity felt be people as they enter into the information society transparent not just in their relationship with the state, but also in commercial, political and religious relationships with businesses, political actors and religious organisations.

Little are we comforted, such a critic may note, by the fact that an idealised, perfect Orwellian society cannot arise from economic reasons. What we need to know is how to stop the gradual erosion of trust and the disappearance of the personal sphere in general.

This is a valid point. I have tried to show why I believe that both Orwellian control societies and privacy societies will not arise, nor be stable should they

arise. The reason for this is that our society economically has organised itself in such a way that we live in what I have termed a noise society. Such a society has the peculiarity that it is possible to map anyone living in it, but not everyone. This fact I think can be helpful in trying to achieve the admirable goals set out by the fictional critic above. If the criticism or discussion of privacy simply strives to avoid the control society or build a privacy society we will miss many of the economic facts that govern the way identity is traded, constructed and disseminated in the information society today. We will also lose one of the really strong factors acting to our benefit – the information growth and the growth of costs of surveillance that follow with this growth.

A fourth objection could be that the noise society is a horrible place, and that it is scarcely better than living in a dictatorship.

This criticism, however, assumes that I am advocating the noise society as a solution much better than any other solution, which I am not. My observations on what kind of society we are living in are not recommendations on how we should organise society. They are simply observations and the sum of the observations have been collected to form a model that I think has some explanatory value.

A fifth objection may be that the driving factor behind the privacy erosion is in fact the economy of personal data, and the price discrimination made possible by the mapping of individuals. Andrew Odlyzko recently presented a paper to this effect.[22] The economics of eroding privacy are far greater than the costs of eliminating noise, one may argue, and thus try to show that the gains from price discrimination far outstrip the costs of filtering noise about individuals.

This objection can be met by stating that the noise society is entirely open to price discrimination. It may well be possible to show that low level privacy invasions that allow for some kind of price discrimination are compatible with the growing personal data sets we see today. What I have tried to show is not that privacy invasions become impossible, only that they become more costly and that it is unlikely that they can be used to build a control society or a big brother dictatorship.

10 Conclusions

The thesis of this paper has been that we live in a society where we have a high collective expectation of privacy, but a low individual expectation of privacy. This has a number of different consequences, of which we have listed but a few above.

Firstly, we see that the design of technologies and legislation will be slightly different in noise societies. Instead of focusing on the processing of personal data, or the use of said data, it would focus on abuse of that data. Secondly, we see that the design of what I have tentatively called Jante-technologies may be more important than the design of traditional privacy enhancing technologies.

---

22 *See* Odlyzko, A., *Privacy, Economics, and Price Discrimination on the Internet* ICEC2003: Fifth International Conference on Electronic Commerce, Sadeh, N. ed., ACM, 2003, p. 355-366.

Perhaps it would also be possible, with further research, to use this model of representing the privacy dilemma to throw light on the seemingly inconsistent beliefs that users hold about privacy. On the one hand they seem to think that privacy is important, on the other they are prepared to do very little about it.[23]

This behavior is, in a sense, consistent with a noise society interpretation. What users then say is that their individual privacy is important, but that they do not expect to be the focus of attention. That could be the reason they do not care to protect themselves. This is rational on an individual level in many ways. The individual computer user may perceive that he or she will a) likely not be the focus of attention in the noise on the net and b) if they should be the focus of such attention there are no simple means of protection that would suffice to protect them. Then, incurring the cost of a mediocre, general level of protection would not make sense at all.

There is also a positive note to this paper. It seems as if surveillance societies, such as the one suggested by Flaherty and others are unlikely to arise, due to the enormous costs associated with them.[24] It also seems unlikely that we will live in one-to-one economies such as the one suggested by Peppers and Rogers, with great detail about customers, due to the same costs reasons.[25]

Much remains to be done. The fact that we may live in a noise society also has implications for the copyright debate and other such legal informatics subjects, and the consequences are not clear. How do we balance freedom of speech, copyright and privacy in a noise society?[26]

In any case, the assumption of cost efficiency and the assumption about data quality have both been examined in detail, and arguably been shown to be lacking in important respects. If this holds true, we need not fear Orwellian dystopias, but we can not hope for privacy paradises, either. We must make do with, and adapt to this society, our noise society, for future regulation and technology design.

Acknowledgements

My thanks to the comments on a presentation of some of the thoughts in this paper that were received during the SAITS national workshop. I would also like to thank Mikael Pawlo for allowing me to test my ideas with him in another setting.

---

23 *See* for example on this lack of care Cranor, L, Reagle, J. and Ackerman, M., *Beyond Concern: Understanding Net Users' Attitudes about Online Privacy* in Vogelsang, I and Compaine, B The Internet Upheaval: Raising Questions, Seeking Answers in Communications Policy (MIT Press 2000) p. 47-70.

24 *See* Flaherty, D H., *Protecting privacy in surveillance society*, (The University of North Caroline Press, 1989).

25 *See* Peppers D., Rogers M., *The One to One Future : Building Relationships One Customer at A Time* (1997 Bantam Books).

26 *See* Seipel, Peter, *Upphovsrätten, informationstekniken och kunskapsbygget.* I: Vitterhets-akademiens årsbok 1998 "http://www.juridicum.su.se/iri/seip/text/upphov.htm" [2004-05-27].

The anonymous reviewers of an early version of this paper at WHOLES 2004 took time to supply me with some extremely useful comments as well and seriously contributed to the merits, but not the shortcomings, of this paper.

I have also received numerous interesting comments from colleagues and students that have contributed to this work.