Privacy in a Noise Society

Nicklas Lundblad
St Anna Institute
C/O Stockholms Handelskammare
Box 160 50, 103 21 Stockholm
+46 70 638 60 60

nicklas@skriver.nu

ABSTRACT

In this paper, an economic study of different levels of expected privacy, both individual and collective, is used to demonstrate that we live neither in a dystopian control society nor in a utopian privacy enhanced society, but rather in a *noise society* characterized by high collective expectations of privacy and low individual expectations of privacy. This has profound consequences for the design of privacy law, privacy enhancing technologies and the sociology of privacy.

General Terms

Economics, Human Factors, Legal Aspects,.

Keywords

Noise, Privacy, Cost of surveillance.

1. INTRODUCTION

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 effect for privacy by raising the costs for surveillance. This effect, tentatively termed the noise effect will however not protect individuals and raise their *individual expectation* of privacy directly. Instead it will raise the *collective expectation* of privacy. Here the consequences for 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.

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 world privacy can no longer be only the right to be let alone. [24].

1.1 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 [1]. Most writers today seem to gravitate towards the dystopian view of the future [13,22,25]

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, 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) [8].

Both of these scenarios lack in realism, for the same reason. Both can be described as *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.

1.2 The cost of control societies

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

- *Collection of data*. Data has to be collected. This is generally a linear cost that rises linearly with the number of subjects that are under surveillance
- *Classification and structuring of data*. Data has to be structured to be searchable and of use to a surveillance society or even a "little brother"-society. This is a non-linear cost that grows quicker, the larger the number of subjects under surveillance.
- *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 1970:s 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 Jeremy Benthams panopticon quickly would become economically stagnant.

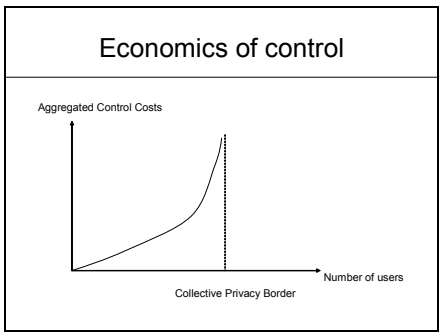

Fig 1 Economics of Control

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. Orwells 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 destabilize even more quickly – leading to both transaction costs and surveillance

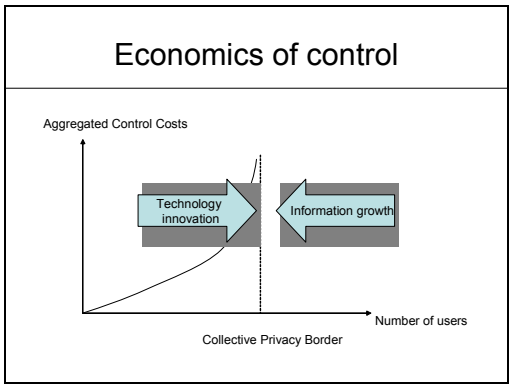

Fig 2 Factors affecting the Privacy border

costs in excess. It is less costly to gather incorrect information (one could apply less exacting standards to information collection), but instead it becomes more costly to rely on and act on such information (assuming that X is trustworthy from incorrect information can lead to direct costs, for example).

A corollary to this 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.

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. 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.

Law has to handle this complex interaction, and we will return to a discussion of how this can be done. [21]

1.3 The costs of privacy societies

Also privacy societies are 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 in adapting systems, developing interpretations of what is a generally worded law and handling request for personal information from customers.
- *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 ones is the expected growth of crime and fraud rates in a society which goes to extremes in protecting personal data. As Posner has pointed out privacy is oftentimes used to conceal less appetizing data about subjects in different ways [18]. 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 is higher than perhaps 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.

2. 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 ensure that it is costly to invade everyones 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 table 1)

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 would 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.

3. 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 P3P? These technologies are varying and span over a wide range of different designs, but have some common qualities[2,3]. For examples see [4,6,10,23 with an interesting criticism of P3P in 5].

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 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 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. (Link) Forcing surveillance to sift through the massive noise generated by spammers is one good way of protecting secret information.
- *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 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 also offers important advice. The notion of blending with the crowd is not new in this context, indeed there exists a project which has taken "Crowds" as its name, and the slogan of which is "Anonymity loves a crowd" [23]. 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 belive that you are somebody" and Jante-technologies would be privacy enhancing technologies that ensure that you never go from being anybody to somebody.

Examples would be technologies to ensure that 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 behavioural patterns in surfing based on average statistics, as to disable profiling in different ways. Another possible Jante-technology would be a noise generator, that takes as it's input a typical page on a website, and then generates thousands of copies of that page with uniquely changed numbers, letters, words and information. Since 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 same search engines.

In summary, then, 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 less likely that privacy will be built into the architectures of society, since there is no need for such architecture regulation. [14].

4. Consequences for designing privacy legislation

A noise society is not necessarily ideal. 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 van often be tragic and horrible.

In the case of Amy Boyer both of these adjectives apply [15]. 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:[1]

Table 1: Different expectations of privacy

	COLLECTIVE EXPECTATION OF PRIVACY		
INDIVIDUAL EXPECTATION OF PRIVACY		*High*	*Low*
	2.1.1 High	**Privacy society**	**Ant hills, hive minds and "statistical societies"**
	Low	**Noise society**	**Surveillance society**

[1] From Amy Boyer's memorial website http://www.amyboyer.org.

“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 shown 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 [16]:

“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. ”

The case shows two things. The first is that the noise society in no way offers protection to individuals who are threatened by someone intent on finding information about that person. Noise, in itself, can only protect against parties that do not know for whom they are looking. The second thing the case imply 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 that[9]:

“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 (ref), 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 would be used. It quickly turned out that this was difficult, since it is difficult to define abuse. The Boyer’s 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.

5. 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.

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 on hand they seem to think that privacy is important, on the other they are prepared to do very little about it. [7,11]

This behaviour 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 would require substantial psychological research to establish however.

There is also a positive note to this paper. It seems as if surveillance societies, such as the one suggested by Flaherty [12] are unlikely to arise, due to the enormous costs associated with them. 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.[17]

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? [21]

6. FURTHER RESEARCH

This is only the start of further research, aiming to collect empirical data about costs of privacy in different ways. The results here are tentative and await empirical corroboration. The model, however, has sufficient explanatory value to be a good starting point.

7. ACKNOWLEDGMENTS

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.

The anonymous reviewers of this paper took time to supply me with some extremely useful comments as well, and seriously contributed to this paper.

8. REFERENCES

[1] Brin, D., The Transparent Society: Will Technology Force Us to Choose between Privacy and Freedom? (Perseus 1998)

[2] Burkert, H., "Privacy Enhancing Technologies: Typology, Critique, Vision" i Technology and Privacy: The New Landscape (red Agre, Phil och Rotenberg, Marc) (MIT Press Cambridge, MA 1997)

[3] 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

[4] Chaum, D., "Achieving Electronic Privacy" in Scientific American, August 1992, pp. 96-101

[5] Clarke, R., "Platform for Privacy Preferences" in Privacy Law and Policy Reporter 5, 2 (July 1998 pp 35-39)

[6] Cranor, L., "The Platform for Privacy Preferences", Communications of the ACM, February 1999 vol. 42 no.2 pp 48-55.

[7] 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) pp 47-70

[8] 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.

[9] 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)

[10] Eran Gabber Phillip B. Gibbons David M. Kristol Yossi Matias Alain Mayer "Consistent yet Anonymous Web Access with LPWA" (1999) Communications of the ACM

[11] Etzioni, A., The Limits of Privacy (Basic Books 1999)

[12] Flaherty, D H., Protecting privacy in surveillance society, (The University of North Caroline Press, 1989)

[13] Garfinkel, S., Database Nation: The Death of Privacy in the 21st Century (O'Reilly 2000)

[14] Lessig, L., Code and Other Laws of Cyberspace (Basic Books 1999)

[15] Lundblad, N, "Amy Boyers död blottlägger informationssamhällets brist" in Axess April 2003 pp 8-9

[16] 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])

[17] Peppers D., Rogers M., The One to One Future : Building Relationships One Customer at A Time (1997 Bantam Books)

[18] Posner, R. The Economics of Justice (Cambridge, MA: Harvard University press 1981)

[19] Reiter, Michael, Rubin, Aviel,"Anonymous Web Transactions with Crowds" Communications of the ACM, February 1999, Vol. 42, No. 2 pp 32-38

[20] Seipel, P "Law and ICT. A Whole and it's parts"., in Seipel, P (ed) Law and Information Technology: Swedish Views, An anthology produced by the IT Law Observatory of the Swedish ICT Commission (Swedish Government Offical Reports SOU 2002:12)

[21] Seipel, P., Upphovsrätten, informationstekniken och kunskapsbygget. I: Vitterhetsakademiens årsbok 1998 [http://www.juridicum.su.se/iri/seip/text/upphov.htm]

[22] Sykes, C., The End of Privacy (St Martins Press 1999)

[23] W3C P3P http://www.w3.org/p3p/ [2003-04-07]

[24] Warren, S and Brandeis, L "The Right to Privacy" 4 Harvard Law Journal (1890)

[25] Whitaker, R., The End of Privacy: How Total Surveillance is Becoming a Reality, (The New Press, 1999)