Big Brother
Small Sisters and Free Speech
Reanalyzing some Threats to Personal Privacy

Anders R Olsson

© Stockholm Institute for Scandianvian Law 1957-2010

1 Introduction

From the viewpoint of privacy-protection, we live in a strange era. The way new technologies of communication are utilized today – and the term "ubiquitous computing" describing our situation tomorrow – effective data- and privacy protection seem to become a vanishing goal. Legislators as well as privacy-advocates, lacking alternatives, cling desperately to arguments originating from a main-frames-only world 30 years ago. Although these were quite reasonable given the kind of control over data that owners of isolated computers could claim in the 1970s, the arguments do not address the privacy-problems occurring in societies where everybody is on-line, everybody is using credit cards, communicated data is about virtually everything and networks are either open or poorly (because security is time-consuming and expensive) protected. Privacy-advocates then, have not been able to mobilize the kind of public support for their cause that could actually have an impact in the construction of future technical and administrative systems of communication. It seems they must think again.

This paper argues that privacy-protection needs reanalyzing at several levels: politically, technically, legally.

It's becoming obvious that in modern networks of communication ("cyberspace") personal data is no more effectively controllable. Information about people will flow through cyberspace in – but also out of – the context where it originated. In some electronic environments personal data will be passed around the same way it's passed around through gossip and small talk in the physical world. The fact that cameras are being connected to computer- and telephone-networks, relaying images of individuals (anywhere, at any time) is just another step in this direction. New technological environments will become normal and trivial to us, and societal efforts to control – with legal or technical means – information that cannot be controlled will surely prove counterproductive.

Although a society in which the flow of personal data is rich and largely uncontrolled might in some ways become unpleasant, there is not much support to the idea that we will see an Orwellian nightmare come true. Most likely, it will not be a society where the State (Big Brother) knows everything about everybody, nor a society where everybody (the gossiping little sisters) knows everything about everybody. At least three comforting factors must be considered:

1. The risks associated with techniques like "data mining" and "profiling" are generally exaggerated. There is no evidence that putting together a large number of trivial facts about an individual actually is a way of creating deeper knowledge of him/her. Police-organizations may believe that they, when using these techniques, can identify terrorists or other criminals before they strike – but let's not confuse this modern alchemy with gathering of knowledge. There's gold and there's clay, and so far no one has been able to transform the one into the other.

2. Citizens in general are more active and more capable than is usually acknowledged in protecting their privacy. There is no reason to believe that these skills will disappear in the Information Society. To a significant degree,

© Stockholm Institute for Scandianvian Law 1957-2010

citizens spontaneously thwart surveillance-efforts by providing personal information of bad quality to just about everybody, including data-collecting institutions – public as well as private ones. Only a small part of these "misinformation activities" can be labeled illegal, and even those can sometimes be justified from a moral standpoint.

3. Partly as a consequence of 1 and 2, people are likely to adjust and refine their attitudes to personal data available in cyberspace. Graffiti and sourceless gossip will not be viewed differently in the new environment than in the old. Young people in particular will adapt to greater volumes of personal data and get better at evaluating this information when it is "everywhere". Mans rapid adjustment to new technologies, the development of new skills in the handling of computer-mediated relations (as with SMS, as with chat-rooms) may be most obvious to parents of teenagers.

There is no reason to believe, I should add, that defamation will become accepted or legal as a result of personal data getting "uncontrolled". Libel and slander are defined differently throughout the world, but within all jurisdictions there are limits to what kind of information or statements about others one is allowed to make public.

2 A Wired World, Ubiquitous Computing – and Privacy?

As western societies gradually have become more dependent on computers and new technologies of communication, privacy protection, and data protection in particular, have turned into a political minefield. All societal actors – citizens, businesses, public sector institutions – are forced to make use of the technologies, but no one knows in which direction it is "good" or "safe" to move. The complexity of our communications systems is astounding. The amount of information on individuals that are created, communicated, stored and processed is overwhelming. New questions demanding political answers keep popping up, and politicians rarely know how to react. Responsibility is nowhere to be found.

From a traditional privacy-advocates point of view, we seem to be heading for disaster. As citizens get mobile with their phones and Internet-connections they get geographically traceable. The more they buy, search, read and discuss on the Net, the more information about them becomes accessible to others – and they have no way of knowing who these "others" are. It's obvious however, that the police and the national-security-institutions successfully pushes the kind of technological and legal solutions that will make us all available for scrutiny at any time. Big Brother IS here. Post-September-eleven, his presence is more perceptible than ever, and the terrorist attacks of Madrid in March of 2004 gave him another boost. (On March 25, the EU Council of Ministers made a "Declaration on Combating Terrorism" where it emphasized, among other things, retention of communication traffic data.)

Is it really that bad? In some ways, yes. In others, maybe not.

On the one hand, privacy protection as well as data protection seems to be a failure. Few modern efforts to control, safeguard or limit flows of personal data

© Stockholm Institute for Scandianvian Law 1957-2010

– using law, technical barriers or voluntary agreements on ethical standards – have been successful.

However, the weakening of privacy-protection that nowadays seem to follow "naturally" from the latest developments in information technologies have not caused the kind of public outrage that should be expected, considering the last 35 years of heated debate on the issues. This needs further analyzing. Had anyone described, in the 1970s, a society where citizens had become as dependant on communications networks as we are today – networks as badly protected from snooping and surveillance as ours – he/she would not have been taken seriously. Now the Internet and the mobile gadgets are here, and although people may dislike some qualities of the new technological environment, in practice most people seem quite prepared to live with it. Technical applications developed to protect the data and communicative acts of individuals are easily available – most of them based on encryption – but the vast majority of citizens on-line just won't use them.

One can only speculate on why:

a) Most people are badly informed about the way modern communications systems actually work.

b) The authorities and commercial interests eager to access personal data are politically and economically so strong that resistance to privacy invasions seem futile.

c) Sensationalist news media now exploit, more effectively than ever, violence and other threats to personal safety. This "sells" papers and news programs and simultaneously generates a growing sense of fear among readers/viewers. Huge parts of the population have obviously come to view safety as more important than privacy in most spheres of life. (The wide acceptance of – even support for – camera-surveillance in both public and private places is the most obvious sign.)

d) Most people actually don't agree with mainstream privacy advocate's claims about when their privacy is being invaded, about what is threatening and what is not.

No matter how much value (if any) one attaches to each explanation though – and I'm sure there are additional ones – it seems necessary to reassess some fundamental assumptions about privacy and the threats we have to deal with. This is not to argue that we should value privacy less than before, only that it is time to go back to the drawing board of data-protective structures and rethink some basic ideas about privacy protection.

The challenge is a big one. I would like to make three remarks. Although I think they are of importance, they are not the last word on each topic and are focused on the prerequisites for privacy-protection rather than on final solutions.

The fact that Europe and the US have somewhat different legal approaches – Europeans concentrating on "data protection" and Americans on the broader notion of "privacy protection" – probably works to the advantage of the latter. Focusing on the actual outcome (privacy invasion) rather then the method (data protection) legislators in the US should be in a better position to handle new technological environments. At the ideological level however, the problem is framed the same way on both sides of the Atlantic. I therefore criticize "data protection" and "privacy protection" as a single concept.

© Stockholm Institute for Scandianvian Law 1957-2010

I must also stress that there is precious little research in some of the areas crucial to my arguments. This means that I will refer more to common sense and personal experience than is usual in studies like these. I must stress then, that further research is necessary in key areas.

3 Databases, Filematching, Profiling – Making Gold out of Clay

> Henry Johnson, while still chief executive of Spiegel Company, could barely contain his glee as he described in Direct Marketing magazine how computers and the new concept of psychographic marketing – an automated means of divining the attitudes of consumers – had given his company the power to see the "inner selves" of individuals.
>
> "Through psychographics", he crowed, "we become the friend who knows them as well as – perhaps better than – they know themselves."[1]

One of the most common arguments from privacy-advocates, delivered in somewhat different theoretical frameworks since the 1960s, is that larger quantities of trivial personal information gathered in one place/file will constitute something harmful. (And "harm" here means something more substantial than just a feeling of unease.) There is very little empirical proof to support that claim. Over the years however, it has become so firmly established that it is rarely questioned: putting together a large number of trivial facts about X actually is a way of creating deeper knowledge of X. Nonsensitive information can, if provided in larger quantities, be refined into sensitive information – thus making X transparent.

This belief – supported in an unholy alliance by the marketing industry, companies selling "security" to both public and private institutions, technology-savvy parts of law enforcement agencies and privacy-advocates – is of fundamental importance within any regime of data protection. I realize that a thorough analysis of the issue would require extensive scientific research and the space of a book to present the results. To my knowledge, no such research has ever been carried out. In my view though, the exaggerations on this point have been so frequent and so gross that the gap between reality and the ideology of what could be labeled "the privacy community" is now evident.

The widespread conviction that one can make gold out of clay – that sensitive personal information can be extracted out of greater volumes of trivial data – can only be explained in terms of psychology and sociology.

(It falls outside the scope of this paper, but the idea was developed and nurtured within an emerging epistemic community in the 1960s and 70s. A number of academics, lawyers and civil servants in different countries, sharing basic values and a crusading spirit, became very influential. A study of how a certain notion of privacy was translated into data protection laws all over Europe would reveal that it was guided by a small "movement" dominated by people like Jan Freese from Sweden, Spiros Simitis from Germany, and Alan Westin

[1] Larsson, Erik, *The Naked Consumer. How Our Private Lives Become Public Commodities.* Penguin Books, New York 1992, p. 13.

© Stockholm Institute for Scandianvian Law 1957-2010

and Arthur Miller from the US. They served on parliamentary committees, held conferences, wrote books and often came to serve as experts to each other when called to witness before parliaments. This is not to suggest that there was a conspiracy or that this emerging international community was wrong in a more general sense. My criticism focus on the fact that true and false was established too early, and crusading rather than serious research was encouraged.)

Judging from the way a vast majority of citizens today use credit cards and modern communication technologies, they don't seriously believe that someone amassing trivial data about them is dangerous.

In this paper I will focus on only one aspect, although a crucial one: the personal information available to public sector institutions. Because authorities are given rights to interfere with our lives in many ways, they are often identified as Big Brother-institutions. In their more or less well-balanced efforts to fulfill this task or that, there is a strong incentive for authorities to collect and make use of huge amounts of personal information.

Many privacy-advocates have argued that the quantity of personal data available to public sector institutions is the most important privacy-issue of all. Renowned privacy-authority David H Flaherty in his book "Protecting Privacy in Surveillance Societies"[2] described the situation in Sweden, which he then (1989) called "the model surveillance society in the Western world":

> "In fact, the state administrative agencies know more about the lives of citizens than almost anyone except a compulsive diarist or record keeper, a condition rapidly being approached in other countries." (p 5)

Flaherty may have been right when he said that in Sweden, the public administration held more data on citizens than in any other country. (It may still be true, although to my knowledge no serious comparison of this kind has ever been made.) As Sweden is also committed to transparency as a core democratic value, granting citizens access to public documents and exempting from that right only personal data of a sensitive nature, this country is a perfect place to test the assumption that a mass of non-sensitive data about a person forms sensitive parts or a sensitive whole.

As noted above, this has never been seriously tested. Anyone supporting or dismissing the idea will have to rely on theory and circumstantial evidence – as do I in this article.

I have never tried to count them, but for the sake of argument, let's assume that 200 different facts about me are available to everyone in public documents in Sweden. On several occasions, I've dared audiences, among them two classes of journalism-students, to collect as much of this information as possible and thus reveal something sensitive about me. (Or, if they suspected me of being abnormal in the sense that I had nothing of an embarrassing nature to hide, do the trick on someone else.) So far, no one has succeeded.

Flaherty´s statement that Swedish authorities know more about the citizens than citizens do themselves is actually, if one looks more closely, quite

[2] Flaherty, David H., *Protecting Privacy in Surveillance Societies*. The University of North Carolina Press 1989, p. 5.

© Stockholm Institute for Scandianvian Law 1957-2010

ridiculous. I may not remember all the facts about me that have found a way into public administrative documents, but for every such fact that I've forgotten, I can provide thousands that no administrative agency – state or local – have ever been near.

The idea that privacy is a lost cause, that we will have to accept that anyone can learn anything about us, is today widely spread. (Of the people arguing along these lines, I would say that David Brin has written most interestingly. His book "The Transparent Society" was published in 1998.) This is to exaggerate, however, the effects of the communications-revolution. I agree with author Jonathan Franzen in his critique of novelist Richard Powers, who

> ...declared in a Times Op-Ed piece that privacy is a "vanishing" illusion and that the struggle over the encryption of digital communications is therefore as "great with consequence" as the Cold War. Powers define "the private" as "that part of life that goes unregistered", and he sees in the digital footprints we leave whenever we charge things the approach of "that moment when each person's every living day will become a Bloomsday, recorded in complete detail and reproducible with a few deft keystrokes." It is scary, of course, to think that the mystery of our identities might be reducible to finite data sequences. That Powers can seriously compare credit-card fraud and intercepted cell-phone calls to the threat of thermonuclear incineration, however, speaks mainly to the infectiousness of privacy panic. Where, after all, is it "registered" what Powers or anybody else is thinking, seeing, saying, wishing, planning, dreaming, or feeling ashamed of? A digital Ulysses consisting of nothing but a list of its hero's purchases and other recordable transactions might run, at most, to four pages: Was there really nothing more to Bloom´s day?[3]

Two remarks must obviously be added here. The first one is that large amounts of personal data *of the same type* – each piece of information trivial in itself – collected and processed can indeed reveal something sensitive. Not often, but sometimes. The typist may not worry about the boss knowing that at a certain moment in time, she pushed the button "g" on her keyboard – but if the boss can have information about every button she pushes every day, he can have it refined into detailed knowledge about her work performance. That, given the unequal nature of their relationship, can of course be sensitive.

The second remark is on profiling – using statistical methods to decide from huge amounts of non-sensitive facts about individuals who is most likely to belong to the group that purchase Levis jeans or hijack airplanes. This is a modern form of alchemy, and must not be confused with knowledge of individuals. Profiling activities based on trivial personal data may, however, cause serious trouble. If the fact that I drink a lot of green tea, grow a huge beard and have studied arabic means that I have things in common with dangerous people, I may be thoroughly searched before entering an airplane, harassed by policemen or even put under privacy-intrusive surveillance, but let's not blur the line between knowing and believing. The trivial facts used when creating my

[3] Franzen, Jonathan, *Imperial Bedroom*. In: Peacock, Molly (Ed) The Private I. Privacy in a Public World. Graywood Press, Saint Paul 2001, p. 149.

© Stockholm Institute for Scandianvian Law 1957-2010

profile have not revealed, to anyone, new “knowledge” about me in any reasonable sense of the word.

Witches didn’t exist in the 17:th century either, but this was little consolation to the women burned alive.

4 An Underestimated Factor: The Citizen

Now lets turn the perspective around and make it personal. Morally, I’d say I’m an average person. Of the things that I am ashamed of in my life, or want to keep private for other reasons, nothing appears in the papers of administrative agencies. There have been moments when I’ve acted cowardly, stupidly or insensitively, or when I’ve been disloyal or dishonest. And whatever people might think of my sexual escapades, I prefer to keep them to myself and (in each case) my partner. It’s possible of course that, my being a radical intellectual, the Swedish Secret Police have spied on me with enough smartness to uncover some secrets – but the idea that these could be found in accumulations of trivial data collected on different occasions for different purposes altogether lacks a substantive base.

There is of course a significant percentage of the population – although clearly a minority – that have criminal, social-security or medical records at public sector institutions containing sensitive information. Obviously some authorities knows things about some citizens that the latter would prefer to have erased or at least safely locked up. (And much of it is actually well protected both technically and legally.)

There is good reason to claim though, that what public sector institutions actually know about citizens is less than they think they know. Their data is often bad data, and this is important from a privacy-perspective. The limitations that poor data quality put on Big Brother-efforts are considerable. In this context it would be useful to examine, more closely, why authorities end up with so much inaccurate personal information – and how this effects their performance.

Reliable, empirical studies on the quality of personal data in public sector institutions are rare. They are expensive. Furthermore, there is little incentive for state or local agencies to show that their data is unreliable, as they could hardly claim to be performing good on the basis of bad information. Although I’ve kept my eyes open for books and articles on data quality in the public sector, I have found but one in english. In his book *The Rise of the Computer State*, David Burnham, famous for his investigative reporting, refers to a study conducted in the early 1980s by OTA, the Congress’s Office of Technology Assessment.[4]

This study, says Burnham, focused on the quality of the information in criminal-history-records

> “...passed on to law enforcement and other agencies from five official repositories maintained and operated by three separate states and the FBI. The information in the records from the repositories was then compared with the information in the original records in files of the county courthouses.

[4] Burnham, David, *The Rise of the Computer State*. Random House, New York 1983 p. 72-75.

© Stockholm Institute for Scandianvian Law 1957-2010

> (...)
>
> The findings are surprising. In North Carolina, only 12.2 percent of the summaries were found to be complete, accurate and unambiguous. In California, 18.9 percent were complete, accurate and unambiguous. In Minnesota, the researchers found that almost half the sample – 49.5 percent – met the same standards.
>
> The quality of the FBI files, which of course rests on the information submitted by the fifty states, was not noticeably better."

There are a few Swedish studies, although limited in scope and ambition, all concluding that data quality in public sector information on individuals is quite bad – and actually a serious problem. In the anthology "Data Quality In Longitudinal Research"[5] the contributing scientists focus mainly on theoretical aspects, but they do mention a few empirical studies. These all point in the same direction. Here's an example, provided by Gunnar Eklund, in discussing the reliability of census-data:

> "Can we really trust the occupation data to be adequate? A control study made in connection with the 1960 census revealed that classification errors comprised nearly 20% of the total number of occupations classified at the most detailed level and 13% of the total at the general occupational level..."[6]

A question about occupation could hardly be considered invasive or threatening – and in no way difficult to answer – and yet the Swedish Bureau of Statistics can not get it right. It's obvious, throughout this book, how the scientists wrestle with the problem of people refusing to tell the truth as soon as they are asked to provide information that is actually sensitive. Data, collected from interviews, on the consumption of medicines, alcohol or drugs is not to be trusted. Data on mental or physical health, and on criminal offenses, is also highly unreliable. There are a few other reports, in Swedish, indicating that data quality is a major problem in public sector institutions.[7]

Listing factors from which errors may originate – and under some conditions will not be corrected even when discovered – one gets something like this:

A. A mistake is made, explainable as carelessness or negligence by someone involved along the line of providing-transferring-receiving-storing-processing-retrieving data. Especially when the process involves manual transference of data from paper forms to a database, and the persons doing this tedious typing are less skilled and/or less motivated, the percentage of error tends to rise.

[5] Magnusson, David/Bergman, Lars R., (eds). *Data Quality In Longitudinal Research*. Cambridge University Press, New York 1990.

[6] Eklund, Gunnar. *Data in epidemiological longitudinal research*. From: Magnusson, David/Bergman, Lars R. (eds). Data Quality In Longitudinal Research. Cambridge University Press, New York 1990 p. 60.

[7] Justitieombudsmannen 1982:s 3. *JO om felaktiga skattekrav*. Dnr 3489-1982. Stockholm 1982. Riksrevisionsverket. *Rätt data?* Dnr 1989:393. Stockholm 1990. Riksrevisionsverket. *Fel data kostar!* Dnr 23-91-0550. Stockholm 1992.

© Stockholm Institute for Scandianvian Law 1957-2010

B. The information provider gives, on purpose, false information. He/she can have many reasons for this, and all can not be dismissed as morally unacceptable. (I expand on this below.)

C. The information provider do not care what's right or wrong. If finding out what's correct takes time or effort, and if there's no real incentive to get it right, he/she may prefer to guess.

D. The information provider can unintentionally give wrong answers to questions, often because the questions are badly phrased and difficult to understand. To the average citizen in western, heavily beaurocrotized societies with its myriad of forms, this point needs no further clarification.

E. The information receiver (responsible for transferring the data into files/records at public institutions) has an interest in getting it wrong. Not very common maybe, but it happens. In any fairly complex, rule based beaurocratic process, the civil servant may know that registering the correct data X will lead to extensive correspondence and investigatory work – unnecessary because the civil servant who can survey the information provider's whole situation is convinced that only one outcome is possible anyway – whereas registering the incorrect data Y will save time for public sector employees and thus taxpayers money. (That's what the beaurocrat will say if caught, but even if the actual reason was his/her own laziness it makes little or no difference within the context.)

F. The information receiver gets data that are incomplete or difficult to interpret, and has little or no incentive to do the extra work – to find out what is correct. ("If this sucker who can't provide readable text is not satisfied with what he gets, let him complain and we will sort it out on appeal.")

G. Whenever personal data is collected for one purpose and at a later stage used for another, they quite often turn out to be inaccurate (one way or the other) within the new context. Everyone who has paid serious attention to privacy-problems have seen examples of this. Jan Freese, longtime director-general of the Swedish Data Inspection Board, once told me that during a coffee-break (about 15 minutes) at DIB, his staff came up with 18 different ways in which Swedish public institutions used the term "income". Same term, 18 different meanings. The indistinctness of this term alone has caused numerous conflicts and misunderstandings in Swedish public administration.

H. Erasing incorrect pieces of information and replacing them with correct ones can, because the designers of the system have put so much emphasis on security, become time-consuming and therefore costly. As no one involved is prepared to pay, there is a strong incentive not to look for errors, and if errors nonetheless are found, dismiss them as "negligible". Dagens Nyheter, Sweden's biggest morning paper, reported (2002-06-05) that this is a major problem with case records at medical institutions.

I don't claim that this list is complete. It just covers the most obvious explanations to poor data quality that I have come across as a journalist and author working with privacy-issues.

The factor B is, I think, of special interest in reviewing the basic assumptions on privacy protection. I've met many privacy-advocates who apparently conceives of citizens, not as conscious, rationally acting individuals but as passive subjects, basically unable to counter any efforts by Big Brother or Big

© Stockholm Institute for Scandianvian Law 1957-2010

Business to uncover whatever there is to uncover in their private lives. It would be most useful, in understanding the strengths and vulnerabilities of citizens, to study, more in depth, the protective strategies that people employ in their daily encounters with data-collecting institutions.

5 Encountering Authorities

It would be illusory to think that individuals fit very often or very smooth into the categories used by societal institutions, categories created with a top-down-perspective. Let me illustrate this by telling the story of my own enrollment to military service.

The year was 1971. I was eighteen. Military training was mandatory for males, and I was called to be measured, tested in numerous ways and interviewed by a psychologist, all in order to ascertain the kind of military tasks I was suitable for.

The military people doing the enrollment thus had their agenda. But as an 18-year-old, although not to any extraordinary degree mature, bright or self-confident, I had an agenda of my own. I was basically loyal to the military institution and prepared to take part in the defense of my country, but not to the point of total submission.

At the time I was intent on becoming a middle-distance-runner of, if possible, world class. I wanted to train hard also while doing my military service. That could only be done if I was placed in what was called a “sports platoon”, where I would be allowed to spend 25 percent of the educational time training on my own. This was a special military arrangement designed for young athletes. The different national sports federations – in my case the Swedish Track & Field Federation – could pick a limited number of promising youngsters and recommend them for service at a sports platoon. Unless the military had good reason to place them elsewhere, the Federations had it their way. “Good reason” could relate to any of a number of military interests. A guy in excellent physical condition who also met a certain psychological demands would be picked for service at some elite unit, someone with a talent for learning languages could be assigned as an interpreter, etc.

I knew that I was good enough to be picked by the Swedish Track & Field Federation as suitable for the sports platoon. My agenda then, on the day of enrollment, had nothing to do with exposing the “real” Anders R Olsson. It was to strike a difficult balance. I must demonstrate a good physique, specifically stamina, otherwise they might question my suitability for the sports platoon, but not the kind of overall excellence that could qualify me for an elite unit. At the same time, I must not show too much talent intellectually or language-wise, because they might then find me a desk job suitable for some skill that I actually had. I couldn’t play outright stupid though, because I had decent grades and they would get suspicious.

To cut the story short, I succeeded and was eventually assigned to a sports platoon. In the struggle to end up there, I provided huge amounts of data about Anders R Olsson to the enrollment authority, of which very little was “true” or correctly mirrored the individual who was measured, tested and interviewed.

© Stockholm Institute for Scandianvian Law 1957-2010

I remember finding the interview particularly offending. A psychologist looked me in the eyes and promised that whatever I told him would get no further. He then asked me questions like “Are you straight or gay?” and “Have you had sex with a girl yet?”. This provoked me to give false answers to most questions, not because I thought it would better my odds to end up on the sports platoon, but because it was obviously none of his damned business. (I didn’t claim to be gay though, as I feared this could trigger some unforeseeable reactions within the military beaurocracy.) The data quality in my file, and probably in many others, was just awful: hardly anything was true.

The enrollment-situation may not be typical for the data exchange between citizens and public sector institutions. I am, like most people, more truthful when dealing with the taxation authorities. I would claim though, that there is some room for choices, for “maneuvering” with ones personal information in most data-providing-situations – and often quite a lot of room. I’m also convinced that the average citizen quite spontaneously makes use of this opportunity. When encountering a public institution, he/she realizes that his/her individual situation/need is unique, and that neither the regulatory system nor the employee of the institution is flexible enough.

This is not to advocate unlimited lying to – or cheating of – authorities. It is just to recognize the fact that we may accept the legitimacy of societal institutions and even sympathize with their ambitions, but we can’t and we don’t submit to them unconditionally. We have agendas too, legitimate interests that they are not capable of fully recognizing. We all become more or less “beaurocracy smart”, and although the consequence may be that beaurocracies sometimes get less effective, that is not all. In fact, the public sector probably functions more smoothly if we cooperate on our own terms than if authorities demand that we format ourselves – and our social realities – according to some infinitely complex legal framework. That simply wouldn’t work. Cooperating on our own terms also gives us opportunities to protect, to some degree, our privacy. In providing public institutions with data of varying – sometimes very bad – quality we simultaneously thwart, to a not insignificant degree, the kind of surveillance-efforts that so many of us have come to loath.

As there is so little serious research into this particular kind of data quality-issues, it is difficult to argue further. In the scientific study of modern privacy protection, this is another neglected field of inquiry.

6 A Maturing Citizenry?

As personal information gets increasingly available in cyberspace it will be necessary for all citizens, in order to function well socially, to sharpen their skills in sorting good information from bad, relevant from irrelevant, malicious speech from kind or neutral speech. This is of course what people always have done – in dealing with small talk and gossip in the physical world – but in a technologically-based communicative environment the prerequisites are different. So much information that used to be, for practical reasons, unrecordable now gets recorded.

The petty crime You committed, the stupid comment You made, Your failed attempts to do this or that – the facts may be out there forever, and more likely out of context than in context. We must learn to handle them maturely, to judge people on true, relevant and up-to-date information. (What is it actually worth to learn that Y, now 30, at the age of 15 was caught shoplifting? We may have to better internalize the realities of human socialization: lots of teenagers do worse things without getting caught and most of them grow up to be decent, law-abiding citizens.)

There are studies in the fields of psychology and sociology on our handling of personal information – our own and others. Scientists like Irwin Altman and Sandra Petronio have analyzed the complex interaction with others in which we develop our private lives. In her latest book, Petronio describes Communication Privacy Management (CPM), "a theoretical approach that gives us a rule-based system to examine the way people make decisions about balancing disclosure and privacy."[8] To put it briefly, she tries to capture a dialectical process of boundary regulation.

Although highly theoretical, complex and culturally-bound, such an approach seem to be the only reasonable starting point when searching for legal and technical solutions to the privacy problems of the future. Leysia Palen and Paul Dourish proposes, building on the works of Altman, "a conceptual framework that would allow more specific and detailed statements about privacy and technology to be made in HCI analyses."[9] (HCI = Human-Computer Interaction.) They argue that "privacy management is a dynamic response to circumstance rather than a static enforcement of rules."

"Fair Information Principles" in the handling of personal data were developed in the early 1970:ies and have since provided the guiding ideas behind all legislation on data protection.[10] The principles seemed sensible and functional in an era of nonconnected main-frames. Each person or institution dealing with personal information should adhere to rules like these, developed by the U.S. Dept. of Health, Education and Welfare in 1973:

> "1 Collection limitation. There must be no personal data record keeping systems whose very existence is secret.
> 2 Disclosure. There must be a way for an individual to find out what information about him is in a record and how it is used.
> 3 Secondary usage. There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.
> 4 Record correction. There must be a way for an individual to correct or amend a record of identifiable information about him.

[8] Petronio, Sandra. *Boundaries of Privacy*. State University of New York Press, New York 2002. p. 2.

[9] Palen, Leysia/Dourish, Paul, *Unpacking "Privacy" for a Networked World,* to appear in proceedings of CHI 2003 Conference on Human Factors in Computing Systems, Fort Lauderdale, FL, April 5-10, 2003

[10] Privacy Rights Clearinghouse: *A Review of the Fair Information Principles: The Foundation of Privacy Public Policy.* "http://www.privacyrights.org/ar/fairinfo.htm".

© Stockholm Institute for Scandianvian Law 1957-2010

5 Security. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data."[11]

Although there are still technical environments where these principles make sense – where a person or an institution can claim control over people's personal data and should be held responsible for what is done with it – they don't make sense when applied to the www or listservs. If someone puts information about me "out there" without my consent – and it's obviously impossible to enforce legislation making that illegal – there is no way for me to find out where that information goes, how it's used, whether it gets distorted etc.

When looking for future privacy protection measures we can no longer assume "maximum information control" as default. (As does, to name an important piece of legislation, the EU-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*".)

My suggestion is to develop new or better criteria for "harm", to identify and describe in a structured manner the ways in which individuals can get hurt by other peoples handling of information about them. In the legal context this would mean bridging the gap between privacy/data protection on the one hand and defamation on the other, a gap that has always seemed dubious. Considering how western societies value free speech and freedom of information – why punish people for "illegal" handling of personal data when no individual has come to harm?

7 Conclusion

I have argued that current data-protection-policies, aimed at giving individuals control over their personal data and authorizing law enforcement agencies to intervene in/stop A:s processing of data on B, is fundamentally unrealistic. In the technological era we are entering, new starting points and new policies are necessary, or growing parts of the population might start believing that privacy protection is a lost cause.

Efforts to legally constrain handling/processing of personal data as such should cease. The protective line must be drawn elsewhere. Such a reform would not be unproblematic, but neither would it mean that we realize the Orwellian nightmare of total surveillance.

The risks associated with a richer and freer flow of trivial personal information have been exaggerated. Furthermore, people do actually protect their privacy quite spontaneously by providing lots of false or misleading information about themselves, a behavior that normally is quite justified.

[11] From the website of Privacy Rights Clearinghouse, with reference to: *The Law of Privacy in a Nutshell* by Robert Ellis Smith, Privacy Journal, 1993, p. 50-51. "http://www.privacyrights.org/ar/fairinfo.htm".

© Stockholm Institute for Scandianvian Law 1957-2010

Policies for privacy protection – and I stress that policies not only suggests legislation but also political decisions about the standards and design of technical systems – should therefore focus on 1) adjusting the criteria for slander and libel to cyberspace, and 2) conducting further studies into what kind of measures a "wired" democratic society can take in enforcing laws on defamation.

This will obviously not be easy. (I personally advocate a right to speak anonymously which, if effectively realized, certainly would limit some possibilities of enforcement.)

Modern history shows however, that no measures of privacy-protection can be effectively implemented without the understanding and support of the people who is to be protected. My suggestions may be rejected – I'm quite aware that they are controversial – but as long as they provoke better research and new ideas progress has been made.

© Stockholm Institute for Scandianvian Law 1957-2010