Privacy and Surveillance with Technology

Margarita Georgieva, final assignment for "Ethics and Technology 2"

Introduction

In our electronic world, we give our personal information in exchange for different reductions in shops, for an employment, for a license, insurance, loan; for tax reductions, various privileges and subsidies etc. Even we give our personal data with readiness because we expect help by someone or by some organizations. Furthermore sometimes we don't even realize that some personal data about us is collected, stored and subsequently used. Does it mean that we can't keep any secret to ourselves anymore and that the "surveillance society" becomes inevitable? This paper will analyze different techniques used for electronic surveillance and their impact on privacy. We will argue that despite the "real and present" danger that contemporary surveillance poses for privacy, an open and democratic society can find ways to reconcile the two.

What is surveillance

Wikipedia describes surveillance as "process of monitoring of behavior of people, objects or processes for ensuring security or social control". Lyon defines surveillance as "systematic attention to person's life aimed at exerting influence over it".[1]
Benthams' idea for all-seeing man, as described in "Panopticon" is used as classic metaphor to characterize modern desire to observe and collect data, to control and impose order. The Panopticon is the most used metaphor about surveillance.
Although surveillance in everyday speech often means collecting information secretly about someone, this is not always the case. Surveillance can also be open or even prominent.

"Classic" surveillance

The nation-state with its bureaucratic apparatus and the capitalistic workplace with its hierarchical, detailed management provide many examples of routine type surveillance that is standard feature in modern society. This surveillance started to emerge at the dawn of modernity, during and after the industrial revolution. The purpose of surveillance done by state is to make sure that people live in line with the law, to prevent serious crimes and to protect national security and the dominant social order. Surveillance is also a way to enforce clearly defined hierarchical management within companies and to discipline employees to be efficient in their work. Although surveillance is possible by personal observation and reporting and it often has been done in this way, technology has played a role in surveillance for a long time. Telephone tapping for example was used not only by nation-state but also by employers[2]. Lists with phone calls were (and still are) used to make employees reimburse to the employer the costs of their personal phone calls. Photo and video cameras are also widely used for surveillance. But all these methods of surveillance require personal review of the collected data. This is relatively slow and expensive process, that's why before the rise of the ICT, surveillance was largely limited and centralized to the state (law and order enforcement) and to the working floor. This

[1] David Lyon - "Surveillance technology and Surveillance society"
[2] European Parliament - "Development of Surveillance Technology and Risk of Abuse of Economic Information (an appraisal of technologies of political control)."

doesn't mean, that surveillance was uncontroversial – to the contrary, there is a belief that surveillance is made by elite in order to influence and control behavior of people and to exercise power by knowledge. In this context the right to privacy is seen as a defense against the morally undesirable effects of surveillance.

"Contemporary" surveillance

The development of surveillance technology that relies on computers took off at the same time as the postmodern society was emerging. Post modernity comes with changes in society and in the technology. Technology is becoming more interconnected, faster, allowing for storage and exchange of huge amounts of information, and at the same time more affordable. Bureaucracy acquires means to process and analyze automatically vast information in existing systems and to collect more information at higher speed. Now it is often cheaper to preserve information than to discard it. Fast development of computer technology changes surveillance technology a lot.

Surveillance by using computer and communication technology is sometimes called **dataveillance**. According to Lyon, dataveillance is "systematic monitoring of people's actions or communications trough application of information technology" [Lyon2003]. This includes not only new, computer-based methods of collecting personal information, but also new, computer-based methods for processing, sharing and using data, even if it is collected by traditional methods – for example video and telephone tapping. Dataveillance is practiced in traditional areas like nation-state and working floor, but it also spreads to the consumer sector - for example shopping floor, insurance companies etc. - and even to personal and family spheres.

For example, recently so called "employee's assistance" programs are spreading [Lyon2003]. These programs are used by employers to "help employees to help themselves" or to manage their problems outside of work place – including financial problems, family problems, health problems, etc. Based on collected personal data, such systems categorize different employees' problems and allow employers to offer help. The systems are often well accepted by employees, because they expect help. But what lies behind these programs are risk management models which seek effectiveness at the working place, rather than to be really interested in the peoples' problems. The purpose is to identify psychological overstress and other risk factors at early stages. In practice, such programs also serve as a way for disciplining people. Other kind of programs, used by state authorities, generate "categories of characters likely to violate some rules" and match this categories with concrete persons [Lyon2003, quoting Gary Marx]. Yet another example comes from my personal experience. It is relevant for the welfare support department of a municipality to store data about someone's income and household composition, since this determines the right to welfare support. Fines for traffic offenses in Bulgaria are also handled by municipalities, by a separate department. Some municipalities are creating one integrated computer system for all this data, in order to serve citizens quickly and more conveniently ("one counter" concept). But then welfare and traffic departments get access to both types of data. Then some politicians proposed to link welfare support to traffic fines, since too many traffic offences mean that you are not "good citizen" so your welfare support should be reduced. Gary Marx describes cases where social services collect data for single mothers that receive financial help from them.

The data collected about mothers was "[in] areas of family, sexual behavior, income, and expenditures"[3] which was also used to find "risk patterns" and eventually to reduce the financial help. These are examples how linking and centralization of data can lead to more restrictive approach to public services. In other words, once data is collected and linked, someone will find a good reason to use it for rights restriction.

With connection of data from commercial and administrative sectors social services try to reduce fraud, to be sure that financial help goes on the right place and that citizens pay the taxes and fines they have to pay. Furthermore, interconnected data systems often enable institutions to provide better and more efficient services. On the other hand, it is questionable if all collected data is relevant for these purposes.

The examples also show how dataveillance enters people's personal life and consumer behavior. But it goes even further. Since human actions are considered more or less repeatable, studying the humans' habits by methods of dataveillance is used by advertising industry to predict their future needs and demands for new products. Other organizations that are interested in dataveillance are insurance companies and banks. By studying their clients' habits they evaluate what risk they take if they insure given client or what would be chances for banks to receive their loans back.

In general, the character of surveillance technology in the postmodern world is less coercive and less centralized but it is wider spread, because of interconnected computer technologies used in different sectors. As Lyon puts it, with so many interconnected databases there is no need for centralized surveillance system anymore [Lyon2003]. The goals of surveillance technology gradually shift from reactive (uncovering problems after they happened and taking corrective measures) to proactive - risk assessment and management (preventing problems from happening). But it does not mean that contemporary surveillance is less controversial. Because there is so much information, sometimes it is difficult to analyze all of it and to form a realistic picture of a person. It is possible that people's reputation and chances in life suffer not because of real wrongdoing they have done, but because a computer program has predicted that certain characters (persons) are likely to break the law, for example. This can happen because not entire information about someone is available in the dataveillance network, or because incorrect information is available, or because the information is used out of context. Finally, there is a possibility to misuse or distort the information for non-legitimate or non-ethical purposes. So using the right to privacy as defense from immoral use of surveillance is still actual, but the way of defense should probably change together with changes in surveillance. This leads us to our research question.

Research question

This paper will analyze how dataveillance may violate privacy and how these violations can be avoided? Thus, our goal is to analyze the ways in which the privacy can be violated *in a morally impermissible way* by intensive collection and flow of personal information between different information systems and organizations and to suggest some guidelines

[3] Gary Marx-"Seeing Hazily, But Not Darkly, Through the Lens: Some Recent Empirical Studies of Surveillance Technologies"

for solving or restricting these violations. The first step in our study will be to develop a framework for analyzing privacy from an ethical point of view. In the second part we will apply it to dataveillance in order to understand what privacy problems emerge. In the third part we will analyze what solutions to these problems are possible.

Privacy

Some, or maybe even most of surveillance examples described so far would intuitively be perceived as intrusion of our privacy. Although sometimes there are good reasons for such intrusions, most people would feel uncomfortable if such practices can be used uncontrollably by anyone. So what can we consider private in the context of surveillance with technology? Where is the border between private and non private? To answer these questions, we need to analyze the concept of privacy, and aspects of privacy.

What is Privacy?

There are various definitions for privacy. The definition in Wikipedia is "Privacy is the ability of an individual or group to stop information about themselves from becoming known to people other than those they choose to give the information to".

In her book "In Pursuit of Privacy " DeCew[4] mentions that there are two ways to ethically justify the right to privacy. One sees privacy as "primary good", a right by itself. The other notion is that right to privacy is derived from rights to liberty, autonomy, property rights and right to bodily security. But either primary or derived, there is a widespread consensus in ethics and political theory that privacy is a right of people. What differs between different authors and theories is the scope of privacy – what should be considered private – and the morally justified reasons to sometimes violate privacy.

Many definitions of privacy, like the one from Wikipedia above, relate privacy to seclusion and secrecy. Nissenbaum says that most public discussions about privacy are dominated by three main principles of privacy - "Protecting privacy of individuals against intrusive governmental agents, restricting access to sensitive, personal and private information and curtailing intrusions into places deemed private or personal"[5]. These principles, especially the second and third one, are clearly linked to secrecy and seclusion. Dubbeld concludes that in first half of 20th century privacy was mainly seen as the right to be alone, while in 1960's and later "rather than describing privacy as right to be alone [i.e. seclusion], scholars … referred to privacy in terms of control over the use and communication of personal information [i.e. secrecy]"[6].

DeCew proposes a broader definition of privacy and explains that privacy can't be considered simply as synonym of the secrecy, although most dictionaries give such definition. "Privacy is property of types of information and activity viewed by reasonable person in normal circumstances as beyond the legitimate concern of others" [DeCew

[4] Judith DeCew- "In Pursuit of Privacy"
[5] Helen Nissenbaum – "Privacy as Contextual Integrity", p.107
[6] Lynsey Dubbeld – "The regulation of the observing gaze: public implications of camera surveillance", p. 34.

97:60]. This definition is rather broad and relativistic because it does not give clear view who is a "reasonable person" and what are "normal circumstances". In her further analysis DeCew links privacy and liberty - if privacy secures some information from interference from others and since liberty is when we are free from external coercion and influence, then "protection of privacy can preserve some liberty" [DeCew97:58]. Protection of privacy is necessary but not enough to guarantee protection of the liberty. Different people have different understanding of what can count as private. The standardized concept of reasonable person does not serve well the interests of disadvantage groups like, for example, women, colored people etc. DeCew proposes solution for such cases. She claims that in concrete situation under the concept of reasonable person we have to have in mind not average person but reasonable person from the specific group. For example as reasonable women should be taken as reface point in the cases of rape. So despite its relativism, the definition of DeCew is important since it links privacy to the *context* of information or action.

The definition of DeCew allows violations of privacy to be legitimate in "circumstances when other moral values can prevail". Other authors agree. Loosing some of our privacy can diminish our freedom but "an individual must surrender a part of his or her personal information to society in order to receive the available services and benefits and a society must protect its members against the erroneous or irrelevant use of personal information in return"[7]. The definition of DeCew does not explain *when* it is legitimate to violate privacy. But since the concepts of privacy and liberty are tightly linked, one can expect that as there are principles for liberty restrictions, there are similar principles for privacy restrictions.

There are circumstances in which people are likely to surrender some of their liberty in exchange for safety for example. Beauchamp[8] describes four principles for liberty restrictions - no harm principle, legal moralism, no offense principle and paternalism. These principles are often combined in norms regarding liberty and autonomy[9] restrictions.

- No harm principle. A person's autonomy is justifiably restricted in order to prevent harm to others, caused by that person. But there are different definitions what "harm" means. Narrow definitions include direct physical or mental damage. Broader definitions include also property, reputation, and other "essential interests".
- Legal moralism is the philosophical principle which claims that it is morally justifiable to punish people for their immoral behavior even if there is no harm or offense to others and all parties have agreed with the action[10]. This principle can be seen in part as "anti-privacy", because of reasoning like "if you are moral person, you would have nothing to hide" and "society has the right to control

[7] Mun-Cho Kin -"Surveillance technology, Privacy and Social Control"
[8] Tom Beauchamp – "Philosophical Ethics: An Introduction to Moral Philosophy"
[9] Note: Autonomy is considered as ability for self-expression and self-determination.
[10] Note: The name of this principle in Beauchamp's book may be a bit confusing, but it comes from the idea that "what is immoral, is (or must be) illegal", that is the basis of the principle.

whether you are moral person even if you don't harm or offend anybody". With this type of reasoning practically no information can be justified as "private".

- No offence principle. A person's autonomy is justifiably restricted in order to prevent offence to others, caused by that person.
- Paternalism is a principle allowing restriction to a person's autonomy in order to prevent that person from harming himself. Beauchamp distinguishes weak and strong paternalism. Weak paternalism is about restricting someone's autonomy (i.e. taking decisions on his/her behalf) only when he or she is clearly unable to act autonomously – for example being unconscious, very sick, mentally handicapped, little child, etc. Strong paternalism accepts autonomy restrictions even if someone is able to act autonomously, but he is going to harm himself anyway.

Again according to Beauchamp, liberal democracies usually adopt the "non-harm" principle and often weak paternalism, but strong paternalism and "no offense" principles may be accepted only in limited cases and special circumstances. Legal moralism is in general not accepted and this in turn promotes the privacy.

In summary, we can say that privacy is context-dependent. Right to privacy can be justified in some contexts and can be legitimately violated in other context if there are very good (moral) reasons for this. We can define particular type of information as private, and spreading of such information in most contexts would be intrusion of privacy, but in specific contexts it could be perfectly justified.

Aspects of Privacy

Privacy violations can occur in various contexts. To analyze more precisely what is a privacy violation some authors define different aspects of privacy. Different norms about privacy protection can be determined for each aspect of privacy.

Dubbeld describes 3 aspects of privacy which can be taken as heuristic devices. Although it is difficult to include all privacy-related controversies in one framework, these heuristics can be used as point of references when analyzing privacy, points Dubbeld. The three aspects of privacy according to her are: *private sphere*, *bodily integrity* and *informational privacy*. Protection of *private sphere* includes protection against physical entry in the domestic sphere. Lately this sphere includes protection of the home also from non-physical intrusion, like protection from observation and recording. Other places, like (public or office) bathrooms and telephone booths, also have to be considered private. Privacy as *bodily integrity* includes protection against physical invasion into peoples' bodies. Lately this type of privacy started also to include individual control over "body intrusive actions, like medical treatments". Also bodily integrity recently deals with problems connected with publications of pictures revealing intimate parts. *Informational privacy* concerns right of individuals to protect their personal data. In era of well developed computer systems and networks it is necessary that national and international regulations are put in place to guarantee individual's right to control who has access to his/her personal information, to control if the information is used for the same purposes for which it was collected and also to guarantee good quality of the data [Dubbeld2004].

DeCew also proposes privacy framework with three aspects of privacy. These are *informational privacy*, *accessibility privacy* and *expressive privacy*. She explains that there is almost universal agreement that control over personal information is in the core of the privacy issue. *Informational privacy* protection shields individuals from intrusion or thread of intrusion and also allows individuals to control the spread and use of their personal information. *Accessibility privacy* allows individuals to control who has physical access to them, in term of bodily contact or observation, and to prevent contact that may be unwanted and may cause fear, vulnerability or distraction. *Expressive privacy* is about the right to express oneself without influence by others. In broader sense, it guards freedom of choice Mill's terms. This type of privacy promotes freedom to choose your personal style and behavior as far there is no serious harm to others' interests. Other authors argue that this is more a matter of freedom than a matter of privacy.

What is important for our purpose is that both authors agree that informational privacy is important aspect of privacy. Technologies for surveillance described above can create problems mainly with informational privacy[11]. So our focus in the rest of this paper will be on informational privacy.

Framework for Informational Privacy

As Lynsey Dubbeld has explained in her book [Dubbeld2004] we need framework for informational privacy in order to focus and structure our empirical exploration. Such framework should classify different aspects and norms of privacy and should have a normative basis in ethics if we want to do a moral evaluation of privacy related practices.

Nisselbaum describes two types of privacy norms related to information – norms related to appropriateness of information and norms related to flow and distribution of information. For example, there is a norm that it is appropriate in the context of love to share intimate information and to touch each other and there is also a norm that the intimate information should not be shared with others. In context of education it is accepted (in general) that teachers should share information about pupils with their parents, etc. Norms from one context, argues Nisselbaum, should not penetrate other contexts.

The concept of Nisselbaum for privacy "as contextual integrity" actually builds up on top of DeCew's approach, but it also adds to the framework of privacy a very important dimension – the dynamics. Nisselbaum accepts that norms about privacy change, in particular due to technological developments. Contexts also change. Nisselbaum proposes a way to evaluate these changes from a moral point of view and this way is based on certain moral values. According to her "values likely to impose restrictions on the flow and distribution of personal information include: prevention of information-based harm, informational inequality, autonomy, freedom, preservation of important human relationships, and democracy." On the other hand, "values that are regularly cited in support of free or unconstrained flows [of personal data] include: freedom of speech,

[11] Note: Video and audio surveillance may also violate the private sphere of people and the accessibility privacy.

pursuit of wealth, efficiency, and security. When these values clash with those that support restrictive treatment, we need to pursue tradeoffs and balance."

The importance of these moral values is culture-dependent. In order to come to a concrete and practically applicable framework of privacy, we will limit our investigation to Western liberal democracies[12], as also Nissenbaum does. Countries in this group not only have many cultural and political similarities, but also similar level of technological advancement and economic development, which will help us to narrow and focus our whole socio-technological research.

With this cultural restriction to Western democracies and with aspect restriction to information privacy, we now can describe a framework of privacy, taking Nissenbaum's work as a base.

Privacy is a moral value of its own, linked to liberty and safety. This means that we don't accept statements like "if you don't do anything wrong/immoral, you have nothing to hide" and "even if your private information is put on the street, there is no (moral) problem, if nothing wrong happens to you". Each violation of privacy is in principle immoral, unless there are reasons to justify it, based on other, overriding moral values. Informational privacy is the right of an individual to control who has access to his or her private data. Following Nisselbaum, we accept that what counts as "private data" depends on the social context. Each personal data can be deemed private unless it is generally accepted in the society that this data in a given context *has* to be shared in order to preserve other moral values. This approach emphasizes the importance of privacy as moral value, but it also shows that there might be other moral values that could in certain contexts be more important.

Information privacy is about controlling access to information. In this sense, there is no privacy violation if someone *voluntarily* shares private information with another person or institution. But this decision should be autonomous (i.e. made without coercion) and informed – i.e. the person should know what information he or she shares, with whom and for what purpose. The last point is very important because privacy is context-dependent. Data shared in one context without violation of privacy may be private in another context and using it in that context without consent of the person would be privacy violation. This means that in cases of surveillance people have to be informed what information is being collected about them, who will use it, in what context and for what purpose. The consent of the person whose data is collected is in general required. There are few exceptions, like surveillance (e.g. phone tapping) for solving a crime – in this case the "no harm principle" has priority and people might be under surveillance without being informed about this. But in this context there should be a trustful institution that ensures that only relevant data is collected and it is used only for crime-prevention or crime-solving purpose. Furthermore, the principle of proportionality has to be observed – the scale of privacy violation should be linked to the scale (danger) of the crime being investigated.

[12] Note: Thus, including EU and North American countries.

Dataveillance vs. Privacy

Dataveillance is used in different spheres and for different purposes, thus in different contexts. It is good idea to segment all contexts in which dataveillance is used. Based on the analysis in previous sections, we can distinguish three main contexts of dataveillance - *context of citizenship* (data collected by the state and related to prevention of crime and execution of citizenship rights), *context of work* (by the employer towards employees) and *consumer context* (e.g. for targeted advertising and risk assessment of commercial transactions). In all these contexts problems with informational privacy may arise.

In this paper we will focus on dataveillance in context of citizenship – in other words dataveillance used for law enforcement and just enforcement of rights and duties of the citizens. But we have to keep in mind that in contemporary society the boundary between citizenship and consumer sphere is obscure. Some rights provided by the state are administered by private or semi-private organizations (e.g. social security payments, pensions, etc.). Furthermore, even governmental institutions are under pressure to be economically efficient, so they may be tempted sometimes to choose efficiency over privacy, if the two come into conflict.

After we have limited our work already on informational privacy in the context citizenship we need to go one step further in the process of detailed analysis. We need to know in which processes problems with informational privacy may occur. Dubbeld describes 3 relevant processes – data collection, data flow (distribution) and data usage. In all these processes privacy violations may occur. We will analyze these processes according to our framework for privacy. It is important to remember, though, that these processes are interlinked especially because of contextuality of privacy – the context is the link between the processes since the crucial question is whether data collected in one context remains and is being used in this context and not in others.

Pieces of personal information, collected by different departments or organizations, are not so intrusive when they are separate. Before the era of computers there was a natural barrier against combining this information even when it was publicly available[13]. Merging and centralizing this information would have been a slow, expensive and space-consuming process. This situation changed with the help of ICT when various pieces of information are brought together. This way information becomes easily analyzable and also relevant and irrelevant information for specific context is mixed and more parties have access to it[14]. Although this in many cases improves the *efficiency* of public services and makes them more convenient for citizens, it also creates dangers for privacy. Furthermore, when

[13] Garry Marx- "Ethics for the new surveillance"

[14] Note: Let's consider an example here. It is relevant for the welfare support department of municipality to store data about someone's income and household composition, since this determines the right to welfare support. Fines for traffic offenses in Bulgaria are also handled by municipalities, by a separate department. Some municipalities are creating one integrated computer system for all this data, in order to improve *efficiency* of their services. But then both welfare and traffic departments get access to both types of data. It even may be relevant, some people proposed, since too many traffic offences mean that you are not "good citizen" so your welfare support may be reduced. This is an example how linking and centralization of data can lead to more restrictive approach to public services. In other words, once data is collected and linked, someone will find a good reason to use it for rights restriction.

data is collected by computers people can't be sure if only relevant information is collected.

Often people don't mind giving separate pieces of personal information, like age, nationality, education, etc. This is especially true when this information is necessary in order to justify rights and eligibility for certain public services – e.g. pension, voting rights, access to university, etc. Since informational privacy is about control over one's personal data, when personal data are collected they have to be collected with full awareness and *consent* of the subjects of the surveillance - i.e. people have to be aware that their personal data are collected and they have to agree their data to be subsequently processed. Certainly the consent should be informed and given *autonomously*, i.e. free of coercion. Furthermore, since privacy is contextual, people have to know for what reason (in what context) personal data are collected and by whom. If people know the real motives of institutions that collect their data, they can judge whether only relevant data for the specified purpose are collected and so people can make an informed consent. This information necessary for the consent should be equally available to all citizens so that *information inequalities* are avoided[15].

Special moral justification is necessary when an institution has the authority to do hidden surveillance, i.e. without subject's consent or even knowledge. Although this is always a privacy violation according to our framework, we have stated that sometimes violation of privacy is acceptable in order to prevent harm to others or to protect people who are not in state to protect them. So hidden surveillance in case of suspected criminals for example is acceptable, since its role is to prevent others form harm and attack. Of course it is again important to use the data only for the purpose of crime prevention and investigation; but it is also important to make sure that a well grounded suspicion is present and, as mentioned before, to observe the principle of proportionality is observed – i.e. the depth of privacy violation depends on the danger of the (suspected) crime. Dataveillance is easier to be hidden than "classic" surveillance (e.g. personal follow-up, house searches, etc.), but this doesn't make it less intrusive. Since digital personal data is so complete and revealing nowadays, information privacy is as important as bodily and home privacy. It is generally accepted in Western societies that there is reasonable protection of home and body privacy in criminal investigations. Our point is that the same rules and practices of privacy protection should apply to information privacy as well.

In summary, informational privacy is based on the following basic principles - personal data have to be given with *consent*, only *relevant information* have to be collected for given purpose, *data has to be used for that purpose only* and *only by the organization that has the consent.* Dataveillance creates opportunities for violation of all these principles. Since dataveillance is automated by ICT, it allows processing and linking of big amounts of data. ICT helps using data that have been collected for one purpose to be used in completely different context. ICT systems that contain personal data are often interlinked.

[15] Note: Another important aspect of information equality is that people who have access to others' personal data should not use this for any personal benefit. Yet another aspect of information inequality is the fact that often (much) more data is collected and stored about unprivileged social groups, like in the example of single mothers mentioned earlier.

Sometimes organizations that don't have explicit consent from citizens to use their personal data do have access to the data. This is a result of interlinking informational systems of several organizations. Furthermore, since dataveillance in general is less invasive, it becomes easier for personal data to be collected without informed consent.

Only because it is easier to collect, distribute and use personal information with ICT (thus it becomes easier to violate privacy) it does not mean that privacy violations will necessarily happen. But often dataveillance, in addition to creating conditions for privacy violations, also promotes values that, according to Nissenbaum, support free flow of personal data and thus often contradict to privacy - like efficiency and security. We will illustrate with examples how each of the basic privacy principles can be violated with dataveillance and will consider also the involved conflicting moral values in each case.

Variable kilometer tax- collection and storage of data

The Dutch government proposed a road pricing plan as part of its policy to improve accessibility of the roads[16]. The essence of this plan is that car owners pay depending on the use of car, the type of road they use and the time of usage.
What moral value requires kilometer tax? An opinion poll by Maurice de Hond (apparently well-known Dutch pollster) in July 2003 shows that 53%[17] of people are in favor of the tax because they think it is *just* (is terms of social justice) to pay according to road usage. This tax will make people to use roads more *consciously* and responsibly, considering also other available possible transportation options. Usage of road system only when it is really needed will reduce traffic jams and will make traveling time more predictable e.g. will increase *positive freedom*. Namely people will have opportunity to travel when they really need to, without wasting time waiting in traffic jams. Kilometer tax will increase *efficiency* of the road system and it will generate funds for improvements of road infrastructure. And last but not least it will have positive effect on the environment. Since traffic jams will be reduced, emissions of greenhouse gasses also will be reduced. All these moral values are in favor of variable kilometer tax but it also may create conditions for privacy violation by collecting personal information like the exact position of a car at a given moment, which is irrelevant for tax collection. The relevant data in this case is a summary that states how long a car has used specific type of roads.

The government has in mind different technical options for implementation of this plan. In any case there should be technology (using GPS, or sort of RFIDs) that makes possible to register the position of a car at certain moments. But collecting detailed information about position of a car on the road creates possibilities for privacy violations, because this information is irrelevant for collecting fees from drivers. When such data is collected, there is always a danger that it will be used for other purposes, either by people who legitimately have access to it, or by people who have obtained it illegitimately - for example, collected data can leak to criminals or criminal organizations or stalkers who

[16] Dutch Ministry of Transport, Mobility Policy Document (MPD), chapter 1 - http://213.156.8.79/pdf/nm4/pkb4-UK.pdf
[17] Maurice de Hond - https://n34.noties.nl/v/get.php?a=peil.nl&s=archive&f=svn33103-Kilometerheffing.html&PHPSESSID=a0f1c862c8a3d02d4e33defec43b525f&PHPSESSID=a0f1c862c8a3d02d4e33defec43b525f – visited on 25.02.07

may track people on their usual paths. This might be an extreme example, but it illustrates the possibility of *information-based harm* resulting from privacy violation. Also *preservation of human relationship* is at issue here. According to Nissenbaum, we need certain patterns of information sharing in order to establish friendship, intimacy and trust – in other words the sharing of personal information is an acknowledgement of friendship, intimacy and trust. If such information circulates without our control and consent, it is more difficult to develop trust, intimacy and friendship, so our relationships may suffer. Of course, there are rules and policies to prevent such dangers, since the state has a duty to prevent information-based harm even if it is done by third-parties. Nevertheless data leakages do occur[18]. Even if this does not happen often, a fear of such potential abuse is already a restriction to individual freedom and constitutes a violation of privacy. This is because people will take such tread in to account, as an external influence, when they plan their actions. So the criteria for collecting personal data should be very precise. But how people can be sure whether only relevant data are collected?

The best way to avoid privacy violation in this case is to avoid storing data about the exact location of the car. According to the New Rules Project[19], "Roel Pieper proposes a digital map of the Dutch motorway system divided into up to five colors, each one representing a price category. Charges will be summed up in the car, using a device issuing a bill at regular intervals. Because only the category and not the actual location of the road are recorded, supporters of the system claim that it will not infringe on drivers' privacy." In this way the responsibility to protect the privacy of the driver is delegated to the technical system. The device in the car will print a bill with calculated time that a car has spent on given road type and no other data will ever be given to a third party for further processing. This technical solution can bring *certainty* to drivers because the device is in the car and the data is not read by other technical devices and other institutions. Instead, the driver will see the printed bill and what data is included in it. Of course, there are some concerns about this option. The device in the car that keeps the data may be broken or manipulated by some drivers. But there are options to make this manipulation difficult, for example by plumbing the device so if this approach is technically feasible it would solve to a good degree the problem with the privacy.

This example shows how the task of privacy protection in dataveillance can be delegated back to technology in order to make abuse of personal data much more difficult, if not impossible. But this is a "lucky" example for several reasons – the data is collected for one purpose only, it will (presumably) be processed by one organization and in this case it is easy to determine which data is relevant and which is not. The situation is much more complex when same data can (legitimately) be used for several purposes and by different organizations. In such cases the data has to be shared between several parties and as the next example shows, privacy issues are then more complicated to deal with.

---

[18] Note: In 2005 "an employee of the [Dutch] intelligence service left computer disks in a lease car. The disks included information about the sex life of murdered politician Pim Fortuyn" – news report from Expatica - http://www.expatica.com/actual/article.asp?channel_id=1&story_id=27303

[19] New Rules Project – "Dutch Investigation of Kilometer Tax". http://www.newrules.org/environment/dutchkmhtax.html

Passengers' data sharing – flow of data

Development of technology not only makes surveillance less visible, but also makes it extremely powerful. The routine processing of personal data becomes automated and used for various purposes, like welfare, insurance or tax collection. Again with help of globalizing ICT, surveillance not only extends its spheres of application but it extends its application geographically. Surveillance becomes global. This is natural and necessary phenomenon in a world where social and commercial relations are stretched geographically, different national-wide infrastructures are connected and where constant international flows of goods, people and data are present. Often personal data is used not (only) by organizations that collected it, but (also) by other organizations. Cross-checking and matching of personal data collected in different governmental departments - sometimes on international level - become routine and possibly inevitable. These practices involve flow of data under routine conditions and increase probability of data leakages significantly. In US the terrorist attacks at September 11, 2001 stressed the need for data sharing between for example Central Intelligence Agency and Federal Bureau of Investigation. This event deepened surveillance in some spheres like airports, sport events, tall office buildings etc. The importance of security in our contemporary society and the ability of dataveillance to deliver data that can significantly improve security led to enacting more general legislation in Europe and United States that loosens privacy-related restrictions on collection and use of personal data – this is a clear example of conflict between moral values of *security* and privacy.

Globalization and deepening of surveillance requires political and social attention that should result in ensuring contextual usage of data, so that contextual integrity is respected. Ideally, as we said before, the data has to be used only for the purposes for which it has been collected and by the organization that collected it. But sometimes several organizations might legitimately (from moral point of view) need the same data so then sharing of data is acceptable if all organization obey sufficient privacy protection policies and rules. If all involved organizations are perceived as trustworthy in the society then data sharing is not a privacy violation, because these organizations will protect personal data and use them only in relevant context. But this trust should not be taken for granted, even in an open and democratic society. Let's look into the problems arising from global dataveillance in the case of data sharing between European airlines and US state department of Homeland Security. After the 9/11 attack US sought personal data of all passengers arriving in US by transatlantic flights. Initially, the American side requested that passenger data can be shared with any other US governmental agency, to be used for "any purpose" and to be retained for 50 years[20]. This position violated both the requirement of *consent* and *contextual integrity*. The US and EU reached agreement in 2004, agreeing to retain data for 3.5 years, to narrow the shared data to 34 pieces of information and to limit the purpose of data use to "combat terrorism and serious crime"; but US Department of Homeland Security requested and got direct access to the European airlines reservation systems, which brought uncertainty whether only agreed 34 details of personal data will be used or all existing information. Also data could be shared with third

[20] Privacy International (PI), a non-profit activist organization for privacy protection - http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-537923&als[theme]=Data%20Protection%20and%20Privacy%20Laws

party organizations like FBI, customs and Federal Food and Drugs administration. This agreement created difficulties for privacy protection since legislative framework for privacy protection is different in US than in EU. US attitude to privacy is more like to a commodity controlled through free market with special attention of protection of financial data and data linked with children. In EU countries privacy of individuals' is proclaimed a "fundamental right" and EU restricts data flow to countries that don't have the same privacy protections.[21] The 2004 agreement was eventually voided by EUs high court for technical reasons[22]. A new temporary agreement was reached in November 2006. With the new agreement the 34 pieces of information will be exported and send to US authorities instead of providing them direct access to the EU airline reservation systems. Since direct access to the reservation system seems the most *efficient* way to share data (it was implemented initially as temporary solution exactly because it was the fastest and cheapest way for data sharing), in this case the agreement compromises some efficiency in favor of privacy. Furthermore, conditions were described regarding sharing data with third parties so that "US authorities wanted to share automatically this data with number of different domestic agencies, but EU wanted to be sure that if the information did move between agencies then personal data would remain secure and protected"[23].

This whole controversy between US and EU may seem overdone and based on "purely theoretical dangers". After all, the mere data sharing doesn't violate any of the moral values that are usually linked to privacy – freedom, prevention of information-based harm, information inequality, preservation of important human relationships, etc. But as the next example shows, when privacy is disregarded, there is little defense left against violation of the other values too. This emphasizes the role of privacy not only as moral value of its own, but also as barrier against other moral violations.

Security profiling – use of data - hidden dataveillance and data mining

It became recently public, that a governmental data-mining project has been developed in US, called Automated Targeting System or ATS. This system has been used in the past four years for assessing all travelers crossing US borders, whether they are likely to be terrorists or criminals. "The travelers are not allowed to see or directly challenge these risk assessments, which the government intends to keep on file for 40 years."[24] The assessment is based on ATS' analysis of travel records and other information like how travelers have paid for the ticket, where they come from, history of the past one-way journeys, sitting and food preferences, their motor vehicle records, etc. "The government notice says some or all of the ATS data about an individual may be shared with state, local and foreign governments for use in hiring decisions and in granting licenses, security clearances, contracts or other benefits. In some cases, the data may be shared with courts, Congress and even private contractors" but not with the travelers. Travelers have no way

[21] Laurence Ashworth, Clinton Free – " Marketing Dataveillance and Digital Privacy: Using Theories of Justice to Understand Consumers' Online Privacy Concerns"
[22] In the press, USA Today - http://www.usatoday.com/travel/news/2006-10-06-eu-us-flier-data_x.htm, visited at 08.12.06
[23] In the press, BBC News - http://news.bbc.co.uk/2/hi/europe/5412092.stm - visited at 08.12.06
[24] In the press, Economic Times - http://economictimes.indiatimes.com/articleshow/677470.cms – visited at 12.12.06. All quotes about ATS are from this new report, unless stated otherwise.

to oppose or correct this assessment because they don't know they have been assessed. This case caused a public outcry and drew attention to moral controversies of data-mining.

High-technology data-mining systems are means for identifying and classifying people according to multiple criteria. They are used, amongst others, for minimizing criminal behavior [Lyon2003]. Nowadays surveillance is not only about discovering criminal behavior or wrongdoing in the past or at present but it is used also to predict such behavior in advance. The problem here is not so much in collecting of personal data but in using data-mining techniques for screening i.e. for picking up people that meet certain statistical criteria[25], derived from past wrongful activities of other people. As a result citizens who appear statistically similar but are not suspects for a crime can be targeted and "effectively blacklisted"[26]. When data mining techniques are used to assess how likely is for someone to be criminal or terrorist, technical problems are likely to happen, due to imperfections in classifying rules and/or in the collected data. As a result people who are not criminals can be picked up by the system and the other way around criminals could sometimes pass safely through the system. But except the technical problems there is something morally wrong in covertly categorizing people by a technical system. "It is unclear what are legal and moral grounds allowing dataveillance to be used for administrative determination about individuals or discrimination between individuals" [Clarke88]

Dataveillance and data mining can bring significant benefits. Physical *security* of people and property can be ensured. Financial errors and frauds can be avoided by dataveillance. Benefits can be foreseen both in governmental sector like welfare and taxes and private sector like insurance and financing. So data mining can contribute to *social justice* also. Even a new metaphor "Big Mother" has emerged to show the protecting role of dataveillance. Nevertheless dataveillance is threatening and intrusive by its very nature. In the ATS example some moral values connected to personal privacy are endangered. Wrongful identification of travelers by the data mining system might be result of low quality of data or acontextual use of it. Such faulty risk assessment by ATS "might cost jobs of innocent people, government contracts, licenses or other benefits". This system creates danger for citizens to be effectively blacklisted in variety of organizations since ATS is based on merged information form several institutions. Since travelers have no way to see and correct information gathered about them this faulty assessment will follow them whole life without way of redemption.

Clarke quotes Jayson P Ahern, an assistant commissioner of Customs and Border Protection, who says "the ATS ratings simply allow agents at the border to pick out people not previously identified by law enforcement as potential terrorists or criminals and send them for additional searches and interviews". This is fully arbitrary action since these citizens are no suspects. Such kind of system is extremely complex and if it gets into hands of inadequately trained, insufficiently professional, excessively enthusiastic or pressured people, data mining can be turned into modern tool for "witch-hunting" [Clarke 88]. Individuals are harmed not because they have made something wrong but it is harm based on guilt prediction, thus it violates basic principle of justice i.e. that citizens are

[25] L. Tuovinen and J. Röning - "Balance of power: the social-ethical aspect of data mining"
[26] Roger A. Clarke – "Information Technology and Dataveillance"

innocent until proven guilty. This is what Nissenbaum calls "*information-based harm*". In ATS case citizens are presumed guilty (or at least suspect) if they are picked up by AST computers and they have to proof they are innocent. This way the "onus of proof" is inverted [Clarke88]. Furthermore, in order to protect mechanisms and the sources of information, the individuals are not told that data mining techniques have been applied so these activities are done covertly and in absolutely *non-democratic* way. This means that government has deployed this system without knowledge and consent of citizens that their data will be used and there will be flow of personal data between organizations. The system has not been put to public debate as it is normal to be in democratic state. The existing *information inequality* and imbalance of power between organizations and individuals now with data mining are made even bigger, because individuals are refused capacity to defend themselves or to prosecute their innocence.

Dataveillance and especially global data exchange and data mining create dangers not only for individuals but also for the whole society. Additional investigations and monitoring like in the above case with data-mining are not result of reasonable suspicions but investigation is turned in routine action based on presumption of guilt. As a result of data mining suspicion can start to prevail in the society.

According to Clarke, uncontrolled dataveillance can cause citizens of advanced Western societies to start disbelieve in fairness with which they are governed (since decisions are taken in a non-transparent way) and this may lead to decreased respect of the law. In turn this may cause weakening of society's moral fiber and cohesion. Administrative apparatus that has enormous amount of data from variety of sources tends to take decisions on behalf of citizens. They start to believe that best and important decisions will be taken by the government so they do not need to bother. This reduces the self-reliance and self-determination of citizens. Furthermore dataveillance tend to diminish individualism and originality, to reduce meaningfulness of individual actions and to lead to primacy of the state. Not to mention eventual future invaders or totalitarian leaders can use the enormous amount of data collected by dataveillance for destructive purposes [Clarke88]. In this context we can say that right to privacy can be a defense against these social dangers and furthermore privacy would improve autonomy and responsibility of citizens.

Reconciling dataveillance and privacy

As we have seen, dataveillance has negative impact on privacy in two ways. First, it promotes moral values[27] that are contradictory to privacy – like security and efficiency – and second, with the help of the technology, dataveillance becomes powerful, easily concealed and easily affordable. So with dataveillance privacy is easy to be violated. Is there a way to minimize these privacy violations?

Dataveillance creates conflicts between moral values as security and efficiency on one hand and privacy on the other, together with privacy-related values as prevention of information-based harm, protection of important human relationships, information

[27] Note: "Promotes" here means that it creates conditions for easy achievement of these values in situations where earlier it was more difficult to achieve them.

equality, freedom and democracy. There is no easy solution of these conflicts, so it is not easy to determine when dataveillance violates privacy in a morally impermissible way. But a democratic society is able to find balance between these values in an open and democratic debate. This should be also an informed debate, thus citizens have to know how dataveillance is conducted in society and for what purposes.

Due to development of technology the dataveillance becomes more affordable, powerful, and unnoticeable since data can be collected easily with newest technologies. So even if a democratic society finds balance between those values that are in support of privacy and others that are in support of free flow of personal data, the society still has to make sure that data processing institutions will respect this balance and will not misuse personal data. This can be achieved in two main ways – by creating *certainty* and by building *trust*.

Creating *certainty* through technology we have shown with the example of kilometer tax. In that case certainty was created trough putting the data-collecting in the car. In this way the driver will see the extracted information from the device and will be sure that only relevant information is collected by the tax institutions. This way the task of privacy protection is delegated to technology and this guarantees that privacy violations will not occur.

Unfortunately in many cases a technical solution ensuring certainty is not feasible. In fact, in some cases such technical solution is clearly not possible. One such example is video surveillance. It is not possible to record only relevant information since it is practically impossible to technically divide relevant from irrelevant data (how to remove from the videotape or video-file a passer-by while a thief is breaking into a shop?!). Furthermore, sometimes it is not clear at the moment of collection what is relevant information - in case of criminal investigations seemingly irrelevant information often turns out to be very useful later.

When technical solution that creates certainty for users is not possible, then a social solution can be of help. In this situation it is necessary to build *trust* in institutions dealing with personal data. As for example such trust has been built in telephone system. In the nowadays computerized telephone system there is a technical possibility to register each call you make or receive. This is, of course, sensitive private information. But there is practically no abuse of phone records and few people worry about their privacy when they use the phone. Why is this so? Because there are legal, political and technical guarantees, that this information will not be abused. These guarantees work and most people trust them. And there is also an "escape" – you can use a pre-paid mobile phone to avoid being "tracked" by the system. This is expensive and not very convenient escape, but it exists.

How to build such trust in institutions that do surveillance? We will follow the approach described by Nissenboum in "Securing Trust Online"[28] and we'll apply it to dataveillance. According to Nissenbaum in order to establish relation of trust, the trustor should be ensured that those who they trust will not abuse their power or at least will not cause harm. In relation of trust trustors accept their vulnerability in respect to trustees, because

[28] Helen Nissenbaum - "Securing Trust Online"

they believe that trustees will act in good way, despite the capacity to do harm. In this kind of relation the trustor has no absolute guarantee that the trustee will not act wrongful, but because of past experience and other assurances the trustor believes in the good will and capacities of the trustee. When people are 100% protected from harm there is no trust but safety and certainty. But ensuring safety and certainty about privacy in reality is not always possible, especially when it comes to dataveillance. Usually security specialists are looking for good technical ways to protect data from leakage and unauthorized use – for example through access control, transparency of identity, encryption or surveillance. But even if we accept for a moment that our data is perfectly protected from outsiders (those who are not authorized to use the date), we can't be absolutely sure about our privacy since there is no guarantee it will not be violated by insiders, those who have authorized access to our personal data. No security measures can guarantee that insiders will not act wrongful. So privacy concerns can't be resolved based on certainty, they can be resolved only based on *trust*.

For trust to develop between individuals or between individual and an organization the trustor has to have possibility to test whether really s/he can trust the trustee. Trust flourishes neither in perfectly secure environment nor in a hostile one. At least the trustor has to perceive that he has a choice. He has to believe that to trust someone or some organization is not the only option but there are other possibilities. Furthermore, there should be safeguards that protect the interests of the trustor (in our case his/her privacy) to a good degree (without giving full certainty). And of course the trustee has really to act in good will and in such a way that it protects the interests of the trustor.

How such trust about privacy protection in context of dataveillance can be developed? First of all what is necessary is a properly enforced *legislative* framework. Legislation can play a role of a safeguard so that trustor can be sure that things can't go very wrong. Trustor has to know that s/he does not depend only on the good will of trustee, although it is needed for sure, but that there are special legislations that guard his interests. Also good legislation can serve to ensure good will of trustee. If trustee knows that he will sustain a loss when he uses personal data in improper way then there is more reliable guarantee that this will not happen. Besides the existence of good legislative framework for privacy it has to be enforced somehow. The enforcement is certainly done by the *state*, but this means that the state has to control itself. And there are people who don't believe in the state. So control by state alone is not enough. In open democratic societies *public (civil) control* also plays important role in legislation enforcement. Non-governmental organizations like Privacy International are examples of such kind of public control. Public control goes even further than serving as safeguard that enforces the legislation. It can influence the legislation itself so that it protects privacy better. Such organizations discover privacy violations and expose them in the society. They can provoke creation of a 'bad name' of an organization that violates privacy. Their role is multifunctional - as legislation safeguards, as factors that can influence legislation because they reflect citizens' opinion and as educator, that gives information to the people about privacy and protection of their personal data. Finally, *individual control* is necessary for successful trust building. Everyone should be able to do individual control over his personal data. This possibility helps people to test whether they can trust organizations that collect and use personal information.

The importance of legislative framework, public and individual control we will illustrate with three examples.

Legislation example - Dutch Personal Data Protection Act

Good example for proper legislation according to our framework is Dutch Personal Data Protection Act[29]. According to this law personal data *have to be processed in proper and careful way and in accordance with the law*. This means not only to comply with this specific law but also to take in to account other related legislations that contains rules for data processing. *Personal data can be processed only for specific purpose and based on specific ground.* Purposes have to be specified before an organization starts to collect personal data. The purposes have to be legitimate and explicit. Organizations that collect personal data have to ascertain that collected data are really necessary for the specified purpose and that the data will be used for that purpose only. So the law acknowledges that privacy is context-dependent.

The law specifies six legitimate grounds for collection and procession of personal data:

1. When data subject has given his unambiguous consent that his data can be used. According to our framework this is legitimate ground because when there is consent there is no privacy violation.
2. When processing of personal data is necessary for performance of a legitimate contract. If an organization is unable to fulfill a legitimate contract without processing of personal data then it has legitimate ground to process this data. This ground is also legitimate according to our framework because if someone has a legitimate contract with an organization and the organization obviously needs some personal data to perform the contract, then by signing the contract the person gives (implicit) consent to use this personal data. For example if you hire a painting firm to paint your house and they ask you for your address to send you invoice, this is not violation of privacy.
3. When processing is necessary for compliance with a legal obligation to which the controller (the one that processes data) is subject. If a law exists that obliges specific organization to process some personal data and if we accept that the law reflects moral values of people and society, then we can say that people agree to surrender private information in favor for other moral values, that are the base of the law. This also doesn't contradict our privacy framework which agrees that sometimes privacy can be surrendered in exchange for other more important values (for example safety) in a specific context.
4. When processing of personal data is necessary in order to protect the vital interests of the data subject. This ground can be used only in case of emergency when the data subject is not capable to take autonomous decision. This is "weak paternalism" as described in analysis for privacy (see "what is privacy" section) and, as mentioned there, it is in general acceptable as reason to violate privacy.
5. The processing of data is necessary for the proper performance of a public law duty. From moral point of view this is the same as ground 3.
6. The processing of personal data is necessary for the purposes of a legitimate interest. Legitimate interest includes business and managerial interests also. The law seems too open at this point, since it doesn't specify which business interests can overrule

[29] Dutch Personal Data Protection Act - http://english.justitie.nl/images/handleidingwbpuk_tcm75-28677_tcm35-15485.pdf?refer=true

privacy and how much. But it stated that a balance business interests and fundamental right and freedom of data subject have to be observed. Maybe there are other relevant documents that contain normative rules about this balance. Furthermore, some sensitive private data like race, political and sexual orientation, etc. is explicitly banned for being collected and used on this ground.

Finally, the law also states that in principle every data subject has the right to see what personal data is stored about her or him and may require corrections if incorrect or incomplete data is stored. This way the law creates a base for individual control of people's personal data and privacy.

Individual control example – Dutch Credit Registration Institute (BKR)

As we have mentioned, possibility for individual control over one's personal data is essential for building trust in data processing institutions. This control should be not only possible but also it should be made possible in an easy way for citizens. It shouldn't be too much time consuming. Citizens should be informed how they can check collected personal data for them. Existence of easy understandable information about control possibilities is also very important. Good example of an organization that gives information about collected personal information is Dutch Buro Krediet Registration (BKR). This organization collects personal data of all citizens that have taken credit from a Dutch bank. Personal information like what kind of credit you have taken, when you have taken it and when you have to return it and also information whether you have always paid on time your monthly payments is collected by this organization. So every bank can check at the institute for existence of bad credit history before it gives a credit to someone. BKR collects also information about personal unpaid mobile telephone bills. On the internet site of BKR it is clearly stated what kind of information is collected, with whom the information is shared and for what purposes. There is clear description how every one can ask for the information that is collected for him. This is possible by sending to BKR a hard copy request for obtaining personal information and paying 4.50euro in the nearest bank. After that the information is sent to the citizen by post.
This procedure for requesting and collecting this information is a bit complicated and time consuming. Making this process of obtaining personal information even easier could be our recommendation. This can be done for example via internet, and then it will be quicker and more convenient for citizens. This would then be an example that shows how technological solutions can promote individual control.

Public control example – Privacy International

Privacy International is a non governmental organization and it works towards establishment of effective privacy protection. According to their web site "Privacy International (PI) is a human rights group formed in 1990 as a watchdog on surveillance and privacy invasions by governments and corporations. PI has conducted campaigns and research throughout the World on issues ranging from wiretapping and national security, to ID cards, video surveillance, data matching, medical privacy, and freedom of information and expression."[30]

[30] Privacy International (PI) Home Page - http://www.privacyinternational.org/

Privacy International monitors activities of governments and international organizations, like European Union, European Council and UN agencies and focus citizen's attention on national and international policy making about privacy. They inform the public about development of surveillance systems that sometimes bridge the law. Privacy International and other groups devoted at civil rights protection play in such a way a role of *safeguards that enforce the legislation*. Such organizations for example alarmed the public about the 'Automated Targeting System', as it was mentioned above. That system is a violation of the US law and also a violation of US – EU agreement for transferring passengers' data. It violates the agreement with EU because "it uses the data for profiling or risk assessments when it was agreed the data would only be used for verifying whether someone is on a terror watch-list, in accordance with U.S. law" [31]

Privacy International and many other organizations like it provide exert opinion and commentary, write reports on policy and technology issues and provoke discussions in society. They do this work in order to *influence policy development and decision making process.* Such is the case with biometric ID cards. In some countries it is possible to influence the policy development process because laws concerning such cards are still in development. In Thailand and the Philippines, for example, Privacy International worked with local human rights bodies to develop national campaigns against the establishment of government identity card systems. After many debates the identity card plan has been rejected by the Supreme Court in Philippines[32]. In Britain[33] the identity cards plan was approved, but only after the House of Lords rejected it five times. Although this plan has been approved and it is going to be implemented, some important compromises have been achieved - biometric identity cards are not compulsory until 2010 and there will be public debate on this issue[34]. This delay of two years is very important because if Conservatives win next elections, they claim they will repeal the law for creating ID cards. Labour party says that by then the process will be unstoppable. So the question about ID cards becomes an election issue and will be discussed in society for long time ahead and there are chances that public opinion will influence the legislation process - which is exactly the intention of Privacy International.

Privacy International also plays a role of an educator raising public awareness about processes in the society connected to people's privacy. They write reports about hidden privacy threats connected with important technological and political developments. In this way they help citizens to participate in public debates and take informed decisions. On the site of PI there is a section 'Stupid Security Contest' where people can tell and nominate different situations that they find as intrusive for their privacy. There people tell their stories, like the one that in Denmark commuters from the island of Bornholm (which is part of Denmark) are required fingerprint scans to board the boat to mainland Denmark.

---

[31] PI - "PI and ACLU call for repeal of EU-US agreement on data transfers"- http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-548477&als[theme]=Policy%20Laundering%20Home%20Page

[32] PI - Philippines Supreme Court rejects ID system - http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-224701

[33] Note: During the WWII the ID card was seen as a way of protecting the nation from Nazi spies. But in 1952, Winston Churchill's government scrapped the cards.

[34] In the press, BBC News - http://news.bbc.co.uk/2/hi/uk_news/politics/3127696.stm , visited at 7.3.07

This is in fact the first occasion in Denmark when biometric data is used – otherwise Danish use ID cards with photos[35]. By existence of such section PI intends to raise the awareness of the people about their privacy rights and to stimulate active citizen participation in privacy protection.

These examples illustrate the role of non-governmental organizations as safeguards for privacy. Such organizations are essential component of the public control over privacy protection in civil societies.

Conclusions

Dataveillance poses specific characteristics. First of all, it is more transparent that classical surveillance, so it is easier to hide and can be perceived as less intrusive in general. It is also decentralized, used in a network environment and people often don't worry about privacy when they give bits and pieces of personal data at different moments and to different organizations. This may lead to the belief that it is more acceptable from moral point of view than classical surveillance. Furthermore, by automating data collection, data transfer and data usage, dataveillance can significantly improve efficiency of public services and it contributes to public safety.

But consequences from improper use of data collected by dataveillance are not less harmful than from other forms of surveillance. The dangers get even bigger when we take into account that data subjects often can't control what data is collected about them and especially with whom it is shared. This, together with the fact that dataveillance is becoming more affordable and the border between public and commercial sphere is diffusing can lead to a "total surveillance" society without people even noticing it. Dataveillance without safeguards poses serious risks both for the individual and for the society as a whole. Blacklisting, reducing of self-determination, suppression of originality and in extreme cases blackmailing can occur towards individual people. At the level of whole society unprivileged social groups can have their access to public services even further limited and they can have difficulties to exercise their citizenship rights. Bureaucracy gets additional means of control over citizens that can be abused and even undermine the democracy. Finally, an overall climate of suspicion can prevail that undermines the moral fiber of society and endangers relationships based on intimacy, friendship and trust.

Right to privacy remains nowadays a protection against such undesirable effects and the moral importance of privacy has not diminished, but to the contrary, it increases together with increase of surveillance. Informational privacy is becoming an essential aspect of privacy in general. Informational privacy is about control of individual people over who, when and why gets and uses their personal data. In general, since privacy is contextual, the best way to avoid privacy violation is to collect data only after informed and autonomous consent of people. This consent has to be based on information about the context in which the data will be used and the data has to be used only in this context and

[35] PI, "Stupid Security Contest 2003" - http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-63273&als[theme]=Stupid%20Security%20Awards

only by the party (or parties) to whom the consent is given. Such parties have furthermore moral obligation to protect the personal data from leakage to others. But privacy can be violated in certain cases, when other moral values become more important. In practice that means mainly protection and solving of crime and other harm, as well as, in limited circumstances, protection of interest of people that are not in state to protect themselves. Safety, efficiency of public services and care are then the moral values that have to be balanced with privacy. Due to dataveillance these moral values come more often to conflict with privacy. Finding the right balance between them is a matter for informed, open debates in democratic societies. These debates should be ongoing, since new social and technological developments may unsettle the established balance.

A general agreement in society about borders of privacy protection is not sufficient to avoid privacy violations. In order people to feel their privacy respected, they have to trust the institutions that collect and use personal data and the institutions have to act in such a way that they earn such trust. For trust to be built there should be safeguards ensuring that privacy of people can't easily be violated. These safeguards include legislation, public control over the institutions via civil society, individual control by citizens and development of affordable and understandable technical solutions for data protection. It is very important that these safeguards are constantly reviewed and updated in order to match the new developments in the area of ICT and new methods and means for dataveillance.

References

Albrechtslund, A. - "The Postmodern Panopticon: Surveillance and Privacy in the Age of Ubiquitous Computing", presented at CEPE 2005 CONFERENCE, Twente University, The Netherlands, available at http://www.albrechtslund.net/texts/postmodernpanopticon.pdf

Ashworth L., Free, C. – "Marketing Dataveillance and Digital Privacy: Using Theories of Justice to Understand Consumers' Online Privacy Concerns", in Journal of Business Ethics (2006) 67:107–123 _ Springer 2006, DOI 10.1007/s10551-006-9007-7

Australian Parliament, Scrutiny of Acts and Regulations Committee, May 2005 - http://www.parliament.vic.gov.au/sarc/E-Democracy/Final_Report/Glossary.htm

Beauchamp, T – "Philosophical Ethics: An Introduction to Moral Philosophy", McGraw-Hill Professional Publishing, 2001, ISBN: 978-0072840827

Clarke, R. – "Information Technology and Dataveillance" in Communications of the ACM, Volume 31, Number 5, May 1988

DeCew, J. W. - "In Pursuit of Privacy – Law, Ethics and the Rise of Technology", Cornell University Press, 1997, ISBN: 0-8014-8411-1

Dubbeld, L. – "The regulation of the observing gaze: public implications of camera surveillance", p. 34; Ipskamp Printpartners, Enschede, The Netherlands, 2004. ISBN: 90-365-2085-1

Dutch Ministry of Transport - Mobility Policy Document (MPD), chapter 1 - http://213.156.8.79/pdf/nm4/pkb4-UK.pdf

Dutch Personal Data Protection Act - http://english.justitie.nl/images/handleidingwbpuk_tcm75-28677_tcm35-15485.pdf?refer=true

European Parliament - "Development of Surveillance Technology and Risk of Abuse of Economic Information (an appraisal of technologies of political control)." Available at http://cryptome.org/dst-1.htm, visited 10.01.07

In the press, BBC News - http://news.bbc.co.uk/2/hi/europe/5412092.stm, v. 8.12.06

In the press, BBC News - http://news.bbc.co.uk/2/hi/uk_news/politics/3127696.stm, visited at 7.3.07

In the press, Economic Times - http://economictimes.indiatimes.com/articleshow/677470.cms, visited at 12.12.06

In the press, USA Today - http://www.usatoday.com/travel/news/2006-10-06-eu-us-flier-data_x.htm, visited at 8.12.06

Kin, M.-Ch. -"Surveillance technology, Privacy and Social Control"- Korea University; International Sociology, June 2004, Vol 19(2): 193–213, SAGE

Kinsella, J - "Is Spyware Legal", Windows IT Pro electronic magazine, March 2005 - http://www.windowsitpro.com/Windows/Article/ArticleID/45324/45324.html

Lutterbeck, B., Heiß, H.-U. -"Public Surveillance: The Technology and Its Privacy Aspects"

Lyon, D. - "Surveillance technology and Surveillance society", in "Modernity and Technology", edited by T.Misa, Ph. Brey, A. Feenberg, Massachusetts Institute of Technology (MIT Press), 2003, ISBN: 0-262-13421-7

Marx, G. - "Ethics for the new surveillance", The Information Society, 14:171-185, 1998, Taylor & Francis, ISSN: 0197-2243

Marx, G. - "Seeing Hazily, But Not Darkly, Through the Lens: Some Recent Empirical Studies of Surveillance Technologies", Forthcoming in Law and Social Inquiry, Blackwell Publishing, available at http://web.mit.edu/gtmarx/www/hazily.html, visited at 22.10.06

Maurice de Hond - https://n34.noties.nl/v/get.php?a=peil.nl&s=archive&f=svn33103-Kilometerheffing.html&PHPSESSID=a0f1c862c8a3d02d4e33defec43b525f&PHPSESSID=a0f1c862c8a3d02d4e33defec43b525f - visited on 25.02.07

New Rules Project – "Dutch Investigation of Kilometer Tax". http://www.newrules.org/environment/dutchkmhtax.html, visited 2.11.06

Nissenbaum, H. - "Securing Trust Online – Wisdom or Oxymoron", available at http://www.nyu.edu/projects/nissenbaum/papers/securingtrust.pdf, visited 20.10.06

Nissenbaum, H. – "Privacy as Contextual Integrity", p.107, Washington Law Review, Vol. 79, No. 1, 2004, available at SSRN: http://ssrn.com/abstract=534622, v. 15.10.06

Phillips, D. -"Texas 9-1-1: Emergency telecommunications and the genesis of surveillance infrastructure", Telecommunications Policy, Volume 29, Issue 11, December 2005, Pages 843-856

Privacy International, a non-profit activist organization for privacy protection – home page - http://www.privacyinternational.org/ Various sub-pages are quoted in the paper, see footnotes.

Tuovinen, L. and Röning, J. - " Balance of power: the social-ethical aspect of data mining", Intelligent Systems Group, Department of Electrical and Information Engineering P.O. BOX 4500, FIN-90014 University of Oulu, Finland