History of Privacy[1]

Jan Holvast

Holvast & Partner, Privacy Consultants, NL - Landsmeer,
The Netherlands
henp.holvast@wxs.nl

Abstract. Discussion on privacy issues is as old as mankind. Starting with the protection of one's body and home, it soon evolved in the direction of controlling one's personal information. In 1891, the American lawyers Samuel Warren and Louis Brandeis described the right to privacy in a famous article: it is the right to be let alone. In 1967 a new milestone was reached with the publication of Alan Westin's Privacy and Freedom when he defined privacy in terms of self determination: privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.

History of privacy makes clear that there is a strong relationship between privacy and the development of technology. The modern discussion started with the use of cameras and went on to include the development and use of computers in an information society in which personal data on every individual is collected and stored. Not only is it a great concern that privacy is eroding but also that we are entering a surveillance society. This loss of privacy seems to be even more the case since the protection of privacy is strongly dependant upon the political will to protect it. Since 9/11, however, this political will world-wide is oriented more toward the effective and efficient use of technology in the battle against criminality and terrorism than it is toward protecting privacy. Therefore it is time to re-evaluate the use of technology and the protection of privacy. It is not only privacy that is at stake but above all democracy.

Keywords: data protection, information, information technology, information society, privacy, self regulation, surveillance society, vulnerability

1 Introduction

"The good news about privacy is that eighty-four percent of us are concerned about privacy. The bad news is that we do not know what we mean." The figures Anne Branscomb [1] mentions are still true for most countries in the Western hemisphere, and the reason for not knowing what we are talking about is primarily because many authors on privacy issues are writing about different aspects of privacy. Some are referring to the need for privacy; whereas, others are referring to the right to privacy,

[1] This contribution is an elaboration of a more lengthy article in Karl de Leeuw and Jan Bergstra (Eds), The History of Information Security: A Comprehensive Handbook. Elsevier: 2007.

the invasion of privacy, the functions of privacy, or even the (legal) protection of privacy. In this paper, we start with the need for privacy and attempt to unravel the confusion within that issue. Thereafter, we will give an overview of the concept of privacy, an interpretation of that discussion, and a way of looking at privacy. In addition we will examine the function of privacy in order to clarify the importance of privacy (protection).

The third chapter is devoted to the attacks on privacy starting with the first publicly discussed cases in 1361 and then focusing on the development during the 20th century until the present day. This chapter makes clear how strong the relationship is between privacy discussion and technology, in particular information technology as it is called now. It shows the double face of technology, which can help people to master problems and simultaneously can influence people and their conduct in a negative way. An example of these technologies is the Radio Frequency Identity (RFID). As a pacemaker, the RFID is helpful but as a chip under the skin it can become a tool for tracing all movement of an individual. Another example is ambient technologies which will be present in almost all households in the Western hemisphere.

For some time, there have been ways to protect privacy. In many countries, this protection is included in a country's constitution, and in some cases privacy protection is deliberately translated into privacy and data protection laws. The legal systems are, however, not always the same. In this work, we will make a distinction between comprehensive legislation (omnibus laws) and sectoral laws which are intended to protect a particular part of society or areas such as communication technology. In addition to legal measures, self-regulation is used, in particular by industry in the form of codes of conduct or codes of practice. More and more technology itself is used as a means of protection. Security measures are examples but also the often discussed but less implemented Privacy-Enhancing Technologies (PETs) are examples of using technology itself in the protection of privacy. In addition, publicity after privacy has been invaded in an unacceptable way is an important tool of protection, although in an indirect way. We will give some famous examples.

Returning to the issue of privacy, we will explain how privacy is often invaded. Information has two important characteristics: it is power and it is money. These two reasons drive the collecting, storing, and using of information in the current way that it does. It is also the explanation for the omnipresence of information technology. Everywhere humans walk, sleep, and talk, technology is present. And as humans are increasingly adept at data producing, more and more traces of our daily life will be gathered and known by others, both in government and in industry. Countermeasures will be politically defined, and their power relations given in order to see that not all privacy will be able to be protected. Consequently, we must conclude that we are increasingly going to live in a surveillance society in which almost everything about our lives will be known. The consequences of this new society are until now unknown while sociologists seem to have no interest in this new society.

2 Privacy

2.1 The need for privacy

Humans have always had a need for privacy. The privacy issue can already be seen in the writings of Socrates and other Greek philosophers [2], when a distinction is made between the 'outer' and the 'inner', between public and private, between society and solitude. Although private life sometimes was seen as an antisocial behaviour, periods of retirement normally were accepted. There always has been a kind of conflict between "the subjective desire for solitude and seclusion and the objective need to depend on others" [3, p. 5].

An important change took place with the colonization of America. It appears that issues of privacy were brought along from Europe. The ownership or possession of land in the New World furnished a secure base for the privilege of privacy. Because of the distance between homesteads, in the view of David Flaherty [4], physical privacy became a characteristic of everyday life, and the home itself became the primary place of privacy. The home is still seen in that way since the home is a personal castle, which emphasizes the idea that privacy is related to wealth. Historically, poverty and the home meant less privacy, particularly where families share common dwellings with almost no physical separation.

Nowadays it is generally accepted that everybody has a need for privacy, although the way it is appreciated differs from culture to culture and from person to person. At the same time it is clear that a need for privacy can never be absolute and must be balanced against other needs, for example the need for fighting terrorism, criminality, and fraud. As we will then see, the discussion on privacy primarily is a political discussion about the way the distinct individual and societal interests can be balanced.

2.2 The concept of privacy

In the most fundamental form, privacy is related to the most intimate aspects of being human. Throughout history privacy is related to the house, to family life, and to (personal) correspondence. This relation can be seen as a way of controlling a situation. Since the 14th through the 18th century, people went to court for eavesdropping or for opening and reading personal letters. Since the end of the 19th century, the emphasis shifted more toward personal information with the same intention that is, to control one's own information.

The general discussion on privacy started shortly after the Second World War in the United States. Numerous publications were devoted to the issue of privacy. In these publications attention primarily is paid to a description of the concept of privacy and to the developments of techniques invading privacy, in particular the computer which is seen as primarily responsible for privacy invasion. These publications culminated in the founding in 1962 of the Project *The Impact of Science and Technology on Privacy*. The project was developed between 1962 and 1966 by the Special Committee on Science and Law of the Association of the Bar of the City of

New York. Director of Research was Alan Westin who published extensive details of the results in the Columbia Law Review and in his book *Privacy and Freedom* and laid a profound base for the later discussion [5], [6], [7].

In almost all publications from that period, three words are used in relation to privacy: freedom, control, and self-determination [8], [9], [10], [11], [12], [13], [14] [15]. The concept of privacy is defined in almost the same way as it was in 1891 by Warren and Brandeis. Privacy is described as a right to be let alone and a right of each individual to determine, under ordinary circumstances, what his or her thoughts, sentiments, and emotions shall be when in communication with others. Because of the advancement in technology, privacy becomes an ever growing concern. These characteristics of privacy are repeated and elaborated by numerous authors in the beginning of the 1960s.

In his *Privacy and Freedom*, Alan Westin summarizes the discussion and defines privacy based on all of these points. "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy or, when among larger groups, in a condition of anonymity or reserve" [7, p. 7]. Since 1967, there has almost not been a publication on this subject in which this definition is not presented.

As can be seen from the literature on the subject, two dimensions of privacy can be distinguished: a relational one and an informational one. The first deals with the relation one has to other people, for example controlling who may enter the domestic environment or who is allowed to touch one's body. These aspects sometimes are described as territorial privacy and bodily privacy [14]. The informational dimension is related to the collection, storing and processing of (personal) data.

Common to both dimensions of privacy is the need to maintain control over personal space, the body, and information about oneself; however, it is clear that in certain situations, loss of control is even more important, for example when people lose their consciousness due to an accident. Control can, then, be described in the form of two aspects of freedom: being free to … and being free from…. The first is the more active part. Within certain borders, humans prefer being free to do what they wish and not be hindered by others or experiences from the past. The second is being free from being watched or eavesdropped on. In both situations the central idea is the concept of self-determination. Although these two freedoms sound rather absolute, it is clear that 'within certain borders' does mean that in all these situations we are depending on others, our neighbours, our co-citizens, and other people. Living in a community means by definition involved with others. But it means at the same time that we must have some free space or sense of freedom since otherwise we would be prisoners of society.

In the writer's view, privacy can be described as the individual's right to self-determination, within certain borders, to his home, body, and information. Although the word 'right' suggests otherwise, the concept of privacy is much more politically determined than legally. This position is more clearly demonstrated by the changing climate of opinions since 9/11. Personal data, such as Passengers Name Records is now made available for governmental use without much debate. A comparable

situation shows the discussion on the retention of communication traffic data for at least half a year in order to trace back potential terrorist who have used electronic means of communications. It shows how due to a sudden event the balance between a need for privacy and the need for information can change fundamentally. It is not the right itself that is being discussed but rather the amount of privacy that is remained after the government satisfies its need for information. As we will increasingly see, the technical means for collecting and storing information are increasing in an enormous way.

2.3 The functions of privacy

It is almost impossible to describe the various ways in which the functions of privacy were seen in the past. Alan Westin has given a comprehensive description of these earlier functions in his study 'Privacy and Freedom' [7], p. 330-338]. He distinguishes among the four functions of privacy which are still important in modern life.

The first is a need for personal autonomy, which is vital to the development of individuality and the consciousness of individual choice in anyone's life. Privacy is equally important as it supports normal psychological functioning, stable interpersonal relationship, and personal development. Privacy is the basis for the development of individuality.

In the second place we need privacy as a form of emotional release. Life generates such strong tensions for the individual that both physical and psychological health demand periods of privacy. It supports healthy functioning by providing needed opportunities to relax, to be one's self, to escape from the stresses of daily life, and to express anger, frustration, grief, or other strong emotion without fear of repercussion or ridicule. The consequence of denying opportunities for such privacy can be severe, ranging from increased tension and improvident expression to suicide and mental collapse.

A third function is that of self-evaluation and decision making. Each individual needs to integrate his experiences into a meaningful pattern and to exert his individuality on events. Solitude and the opportunity for reflection are essential for creativity. Individuals need space and time in which to process the information which is coming to them in an enormous amount. Privacy allows the individual the opportunity to consider alternatives and consequences to act as consistently and appropriate as possible.

A fourth function is the need for a limited and protected communication, which is particularly vital in urban life with crowded environments and continuous physical and psychological confrontations. The value of privacy recognizes that individuals require opportunities to share confidences with their family, friends and close associates. In short privacy is creating opportunities for humans to be themselves and to stay stable as a person.

Unfortunately since Westin's 1968 study, little attention has been paid to these four functions, and it is still unclear how a significant threat to one's privacy affects psychological growth. Scientists know too little about how people respond under constant surveillance. A concern, however, is that people may become more conformist as they suppress their individuality [15]. On matters related to employees,

more information is available. Barbara Garson in *The Electronic Sweatshop* states that there is some empirical prove that for clerical workers whose keystrokes are counted by the minute or airline clerks whose figures are posted daily, electronic monitoring has been linked to pain, stress, and serious disease. Medical reasons then have been some help in limiting the monitoring of employees [16].

3. Privacy under attack

Literature and court cases show that for a very long time, in one way or another, privacy has always been perceived as attacked. At first the attack on privacy was done by persons with whom individuals have a close contact, such as neighbours and people living in the same village or colony. Later attacks were also accomplished by governmental agencies, industry, or the press. In this chapter we will make a distinction between past situation which lasted until the 1980s and the present situation which covers from the 1980s until 2008 as well as the future situation of which we already now have clear indications of new methods of privacy surveillance.

Although these three periods are distinctive from each other, it is not to say that they can be separated one from the other. An important characteristic of the use of information and information technology is that it is a cumulative process. The beginning of one period does not at all mean that the previous period has concluded. The contrary is the case as, for example, photography and computer uses for privacy invasion show. Many of the earlier techniques are combined with new, even more powerful techniques.

In this overview of (technical) attacks, this contribution will strongly rely on past literature and court cases from the United States since most publications dealing with these discussions and incidents of privacy are published in that country. For the present and future situation, we will use international references, including web-pages. These sources will show that attack on privacy is becoming not only an international but a global problem.

3.1 Use of information in the past

Almost all authors on privacy start the discussion with the famous article *The Right to Privacy* of Samuel Warren and Louis Brandeis in the *Harvard Law Review* of December 15, 1890 [17]. Although the effects of this article can not be underestimated this starting point does not mean that there have been no discussions on the invasions of privacy before 1890. As Westin shows in his publications, in the fifteenth century the word ‘privacy’ was already used in England and historical research shows that colonists in New England were respecting privacy in relation to an individual’s home, family, and even written communication. Hixson [3] shows that there was opposition against the first U.S. census as early as 1790, although the government required little more than enumeration of persons, both slave and free. This opposition resulted in instructions to census takers in 1840 that individual returns be treated as confidential. It was feared that the citizen was not adequately protected

from the danger that private affairs or the secrets of family would be disclosed to the neighbours.

3.1.1 Trespass

As we have seen, the home and its related physical privacy were, from the beginning, the form of privacy that most vehemently was protected. It is not astonishing that the first cases brought to court had to deal with intrusions of the home, in particular by eavesdropping. Electronic Privacy Information Center (EPIC) cites James Michael who shows that in 1361 the Justices of Peace Act in England provided for the arrest of peeping toms and eavesdroppers. In 1765, British Lord Camden, striking down a warrant to enter a house and seize papers wrote "We can safely say there is no law in this country to justify the defendants in what they have done; if there was, it would destroy all the comforts of society, for papers are often the dearest property any man can have" [14, p. 5]. The law of trespass and the constitutional protection of unreasonable search and seizure in the United States as formulated in the Fourth Amendment were interpreted as protections against official and unofficial intrusions.

3.1.2 Correspondence

In addition to the home, personal mail was seen as a part of private life in need of special protection. Long before this protection was generally accepted, in particular by the use of the telegraph, the first incidents about invasion of reading personal mails are known. One story is from 1624 [3]. Plymouth Plantation was the scene for what Hixson mentions as the first recorded invasion of privacy. Governor William Bradford learned of a plot against the leadership of the small colony. He had intercepted several incriminating letters written by two newcomers and sent to friends in England. When the two men denied any conspiracy the governor produced the letters and asked them to read the content aloud. The men expressed outrage that their private correspondence had been intercepted but did not comply further since they had no legality on which to stand.

3.1.3 The Press

Curiosity has always been an enemy of privacy and is a foible that has stimulated privacy invasion and on which newspapers have exploited individual privacy on a commercial basis. Already in 1873 the first complaints were uttered against the way journalists were using interview techniques. President Cleveland expressed dislike of the way the press treated him on occasion, especially when some journalists followed him and his bride on their honeymoon trip in 1886. Also E.L. Godkin wrote at the end of the 19th century that the chief enemy of privacy in modern life is the curiosity shown by some people about the affairs of other people [3, p. 29].

Although it is not known how far Warren and Brandeis were influenced by Godkin, generally the discussion on the attack on privacy starts with the famous article of these two lawyers, published in 1890 in the *Harvard Law Review* under the title *The Right to Privacy* [17]. The reason for publication grew out of a specific situation. The *Saturday Evening Gazette,* which specialized in 'blue blood items' reported activities of Warren and his wife in lurid details. Warren, together with Louis D. Brandeis, was the first to start a fundamental discussion on his rights not to have

his thoughts, statements, or emotions made public without his consent. Since the publication of this famous article, no contribution of the issue of privacy fails to mention it.

3.1.4 Instantaneous photography

In their article Warren and Brandeis not only blame the press but also recent inventions and business methods like instantaneous photographs. In combination with the newspaper business, these business methods and new technologies invaded sacred personal and domestic precincts. As predicted in the famous Warren and Brandeis article, these numerous mechanical devices would be the source for 'what is whispered in the closet shall be proclaimed from the housetops' [17, p. 134].

Since 1890, however, the relationship to the use of technical means is apparent. Already mentioned in the article of Warren and Brandeis, the use of instantaneous photographs makes possible publication for various purposes without the consent of an individual. A classic type of invasion of privacy is the use without consent of a person's picture to promote a product. The initial test was *Roberson v. Rochester Folding Box Co.,* which startled the New York legal world [18]. A local milling company decided to use a photo of Abigail Rochester, a charming and attractive girl at the time, to promote their product. For that reason the brilliant slogan *The Flour of the Family* was used and, together with the photo, placed in numerous stores, warehouses, and saloons. Abigail claimed a 'right of privacy' and brought suit for the sum of $15,000. The New York Court denied the suit, by a 4-3 decision, saying that her claim held no right on grounds that it was yet unknown to common law what had been infringed.

This decision excited much amazement and strongly influenced later court cases, in particular three years later *Pavesich v. New England Life Insurance Co.* In that court case, Paolo Pavesich's picture was used, also without his consent, by a life insurance company for an advertisement. The photograph showed a healthy man (Pavesich) who did buy a life insurance policy, in contrast to a sick man who did not and presumably could not make such an 'invaluable' purchase for his future security. In the picture of Pevasich there was a legend underneath: "In my healthy and productive period of life I bought insurance in the New England Life Insurance Co. of Boston Massachusetts, and today my family life is protected." Pavesich had, in fact, never purchased such a life insurance, nor made any such statement as quoted. He found the advertisement distasteful and brought suit for $25,000 damages. In this case the right of privacy was unanimously accepted. The Court found the insurance company subject to damages for invading the privacy of Pavesich [18, p. 99]. It was a strong precedent for precisely one aspect of personal privacy: the unauthorized use of an individual's picture.

3.1.5 Wiretapping

An extremely important and much cited case has been *Olmstead v. United States* in 1928 [19]. In this case wiretapping equipment was used by the police as a way of obtaining evidence. However, the complaint was not accepted by five of the nine justices because there had been no actual entry into the houses and nothing tangible had been taken. So the search and seizure amendment did no apply. Even more

important than the decision, however, was the dissent of Justice Brandeis, the co-author of the article *The Right to Privacy* in Harvard Law Review. In his view, this case indicated that the privacy of the man had been invaded, that is "the right to be let alone – the most comprehensive of rights and the right most valued by civilized men."

Brandeis' reasoning was adopted only forty years later in the *Katz v. United States* case. Federal authorities used electronic listening devices attached to the outside of a telephone booth used by one Charles Katz, whom the authorities suspected of violating gambling laws. Even though the property was not invaded the court found that this method of collecting evidence infringed on the Fourth Amendment's rights of Katz. In the view of the court, the constitution protects whatever seeks to be preserved as private. What is most remarkable about this case is the interpretation of what is private within the meaning of the Fourth Amendment. In the view of Justice Harlan private can be defined by the individual's actual, subjective expectation of privacy and the extent to which that expectation was one that society is prepared to recognize as 'reasonable'. This interpretation has since been used in many cases related to homes, business, sealed luggage, and packages. At the same time it is also often criticized and seen to be of limited value since it is restricted to government invasion of privacy and does not apply to objects controlled by third parties such as bank records. Above all, this case is dependent upon what society's expectation of what invasion of privacy is, which is a serious disadvantage since whatever the public views as reasonable tends to evolve more slowly than does information technology [20].

3.1.6 Psychological testing and lie detectors

Around the 1960s, it was not the single collection of data by means of photography and technical devices that worried people but the mass collection of data with the help of psychological testing, lie detectors, and attitude scales used by social scientists. Not only are these techniques criticized but in particular the philosophy behind the use of them. In his *The Organization Man* William H. Whyte [21] expects that social sciences will become more and more a type of social engineering, the goal of which is to adapt a society to one in which all problems will be solved. In a cynical moment, Whyte promoted a kind of Universal Card with an individuals' fingerprint, IQ, and several other personal characteristics attached. To his astonishment the proposal was not criticized but strongly endorsed.

Another criticism came from Vance Packard [22]. In his *The Hidden Persuaders* he shows the strong relationship between techniques that detect hidden personal emotions and feelings and the way this data is used for advertisement.

As a criticism not only of the techniques as discussed but the social sciences in general, Oscar Ruebhausen and Orville Brim [23] are the first to make clear that the development of social research proves that ethical and legal rules are necessary and most especially regulations that allow for the expressed consent of the individual who is willing to cooperate. Nowadays the use of these techniques, in particular that of the lie detector and questionnaires are still criticised.

3.1.7 Computer as a black box

At this same point in discussion of privacy rights, a new development was added, that is how the computer could be used as a primary data storage device. Large scale storage of data as well as the processing and exchange of data between organizations are now possible. The computer as a data giant has been seen as frightening by several authors. Numerous publications have appeared with thrilling titles that warn of gigantic invasions of personal privacy, for example *The Assault on privacy: Computers, Data Banks and Dossiers* [24], and *The Data bank Society* [25]. The emphasis is in this issue is on computers and databases, that is huge collections of data processed by electronic means.

At the end of the 1970s, a new dimension—telecommunication—was added to the discussion. Telecommunication in combination with informatics was referred to as telematics. It is not only the processing of data which is frightening but above all the distribution of the data to unknown recipients. The combination of computer and telecommunications led, in turn, to a 'tele'-hype of what the future might bring about in society, such as tele-education, tele-work, tele-medication and tele-papers. The future is the human home in which individuals communicate with the outside world exclusively by way of the television. It is a brave new world in which privacy will be strengthened since the home will become even more than ever a castle but at the same time privacy can be attacked by all traces that remain from that type of communication.

3.2 Present use of information technology

3.2.1 Video Surveillance

Surveillance video cameras are increasingly being used throughout the public arena [26]. In almost all cities of the western world walking around means being recorded and it is expected that this surveillance will be expanded in the next years by improved technology, by centralizing the surveillance, and by the unexamined assumptions that cameras are providing security.

Cameras in some countries are being integrated into the urban environment in ways similar to the integration of the electricity and water supply at the beginning of the last century [27]. The CCTV market in an increasing way integrated into technologies, such as the internet, face recognition software, and law enforcement databases is enjoying an uninterrupted growth. CCTV's power is substantially increasing, and it has features that include night vision, computer assisted operations, and motion detection facilities.

3.2.2 Biometric identification

Biometrics[2] is the science and technology of measuring and statistically analyzing biological data. In information technology, biometrics refers to technologies for measuring and analysing human body characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements, especially for

[2] http://whatis/techtarget.com/definition7

authentication and identification. Biometrics involves comparing a previously captured, unique characteristic of a person to a new sample provided by the person. The biometric information is used to identification or verification of a persons to find out whether they are who they claim to be. This process can mean an attack on one's privacy when the collection takes place without consent or permission and without transparency about the purpose for which this data is used.

3.2.3 Genetic data

There is an increase in DNA-analysis for medical testing research and for investigative purposes which are incorporated into routine health [26, p.5] testing. Unlike other medical information, genetic data is a unique combination difficult to be kept confidential and extremely revealing about us. Above all it is easy to acquire since people constantly slough off hair, saliva, skin cells, and other trails containing our DNA. No matter how hard we strive to keep our genetic codes private, we are always vulnerable to the use of it. The data collected tells about our genetic diseases, risk factors, and other characteristics. For the financial services companies, it would be useful to be able to assess risks on the basis of genes patterns that can indicate an individual's future potential susceptibility to illness and diseases. A specific problem with genetic data is that an individual who discloses his or her genetic information also discloses the genetic data of his or her relatives.

3.2.4 Identity theft

Identity theft is one of the fastest growing types of fraud. Identity theft is the use of another person's financial identity through the use of the victim's identity information. This information includes a person's name, address, date of birth, social security number, credit card numbers, and checking account information. Elbirt [28] makes a distinction is sometimes made between identity theft and identity fraud. Identity theft occurs when someone is using one's personal information to impersonate him or her to apply for new credit accounts in his or her name. Identity fraud involves an unauthorized person using one's credit card number from an existing account to make purchases. Seen from the consequences for the individual, theft normally refers to both.

One of the increasing forms is phishing by which thieves on the internet pose as legitimate account managers for credit card companies and financial institutions and ask for personal information under the guise of account verification or maintenance [29]. An even more aggressive form is pharming, a word play on farming and phishing. Pharming is an attack aiming to redirect a website's traffic to another (bogus) website. This website duplicates the look and feel of a bank or other sensitive website. Via this bogus website criminals try to steal, for example, account information.[3]

3.2.5 Data warehousing and data mining

Datawarehousing is the collation of (personal) data into huge, queriable repositories in such a way that they allow analysis of all data related to a particular person. This

[3] http://en.wikipedia.org/wiki/pharming

data is collected in order to make data mining possible, which is a statistical technique enabling analysis of the data in order to find patterns and relations which are nor expected nor predictable. In this way new patterns can be discovered or can confirm already suspected relationships. A famous example is the data mining that marketers show that fathers who buy diapers often pick up beer at the same time. The link prompted some stores to stock the seemingly unrelated items at the same aisle so even more fathers would reach for beer. The underlying expectation is forming profiles of groups of people that make behaviour predictable, for example potential terrorists or criminals.

3.2.6 Chip or Smart Cards

A chip or smart card is a credit card size device with an embedded microprocessor(s), capable of storing, retrieving, and processing a tremendous amount of information related to one person. This person is obliged to wear and use this card in all contacts he or she has with the distributor or distributors of the cards, since combinations of applications are likely. Examples of these cards are the modern driver license, passport, medical cards, and loyalty cards. The content of the card can be read by making contact with a reader or in a contactless way as is used on public transport.

3.2.7 Global Positioning System (GPS)

With the rapid growth of wireless communications, such as mobile phones, the use of the Global Positioning System and the related Location Based Services (LBS) is increasing. The GPS is a system of 24 well-placed satellites that orbit the Earth and make it possible for people with ground receivers to pinpoint their geographic location. The location accuracy is anywhere from one hundred to ten meters for most equipment. A well-known application is the use of GPS in automobiles to order to pinpoint precisely a driver's location with regards to traffic and weather information. By using mobile telephones it is rather simple to detect the place where the mobile is by using network based technology and/or handset bases technology. By using the cell of origins method the telephone, once connected, is communicating his position regularly. In this way the user of the telephone can always be traced, as in the case of International Mobile Subscription Identity (IMSI), which collects the signals of mobile telephones and can identify the content of the communication. Another use also based on tracing is electronic monitoring as an alternative for imprisonment in certain cases.

3.2.8 Internet

Internet is the most fruitful area for data collection in modern times. It is quite possible to collect tremendous amounts of data on almost all users of the internet without their knowledge. Using search engines like Google makes clear how elusive the internet is becoming. Although it is at the same time a mighty instrument in the hands of the consumer or citizen for improving his or her knowledge, it is also an instrument for contacting these individuals. The combination of cookies and spam shows in which ways the internet can be used for advertising purposes. A cookie is a piece of information unique to a user that the user's browser saves and sends back to a web server when the user revisits a website. Cookies form a specific part of the more

general area called spyware which extracts information from an individual without the user's knowledge or consent. The purpose of spyware is to gain access to information, to store information, or to trace the activities of the user. Cookies allow the server to link information entered by users on different web pages and keep a consistent state of the user's session. The registration information is stored on the server and if it's part of a cookie it contains a limited subset of this.

This information in the form of an email address can be used for advertising purposes in the form of spam, which is hundreds of unsolicited junk emails that contain advertising or promotional messages and sent to a large number of people or even to one person at the same time [30]. Spam, therefore, can be described as the electronic distribution of large amounts of unsolicited emails to individuals' email accounts. Spam email is definitely distinctive from the traditional direct mailings in that the costs for such massive mailings fell to the sender. The cost of sending mail through conventional means is very real, including postage costs all paid by the sender. On the other hand, costs of sending bulk emails are very small. It is the fact that emails can be sent at low costs and in great quantities that attracts direct marketers and other companies to use spam emails for advertisements.

3.2.9 Key Logger

A key logger application records the key strokes an individual enters on a computer keyboard [14, p. 39]. Key stroke loggers can be employed to capture every key pressed on a computer keyboard, including information that is typed and deleted. Such devices can be manually placed by law enforcement agents on a suspect's computer or installed remotely by placing a virus on the suspect's computer that will disclose private encryption keys. The question of legitimacy of these methods arose in the case of *United States v Scarfo* where a key logger was placed in order to capture an individual's PGP encrypted password. The existence was confirmed by the FBI. The key logger did not need physical access to the computer in order to accomplish the desired task of capturing private information.

3.2.10 Radio Frequency Identification (RFID)

Use of the RFID is advancing rapidly and, in a sense, is the successor of the chip card. In a similar way, RFID tracks and traces objects and subjects easily. One of the most well known applications is a yellow tag tracing cows in countries of Western Europe. RFIDs are smart tags which make it possible to follow exact movements of the objects wearing it. It is in a type of successor of the barcode with the most important difference being that a barcode is identifying a type of product whereas the RFID is identifying each distinct product. An RFID label consists of two parts: a microchip and an antenna. The chip contains data about the product and a unique code by which the product can be identified. The antenna makes it possible for that data to be sent to a receiver; therefore, one of the most important differences from past applications is that the tag can be read from a distance without the wearer of the tag being knowledgeable of the tracing.

This tag can be attached to a product (cow) but can also be implanted under the skin. In the summer of 2004, the RFID application became well known in bars of Barcelona, Spain and Rotterdam, The Netherlands where visitors had the possibility

to have an RFID-chip implanted under their skin. This chip recognized people as they entered a bar, knew their preferences for drinks, and knew the bank accounts to be charged for paying the drink bills. This RFID-chip was used during the football World Championship in Germany so that on every entrance billet, an RFID-chip was attached thus each visitor could be identified and, in case of incidents, be arrested. In Japan the RFID is sometimes part of a whole system of sensors and communication techniques forming an Ubiquitous Network Soceity.

3.2.11 Wireless networking

Wireless networking has already been in use for several years in the form of Wi-Fi that is, Wireless Fidelity. Wi-Fi was intended to be used for mobile computing devices, such as laptops; however, it is now used increasingly for other applications, including Internet Access, gaming, and basic connectivity of consumer electronics such as television and DVD-players.

A new development in the field of wireless networking is Bluetooth. Bluetooth is an industrial specification for wireless personal area networks (PANs)[4]. It provides a way to connect and exchange information between devices like personal digital assistants (PDAs), mobile phones, laptops, PCs, printers, and digital cameras by way of a secure, low cost, globally available short range frequency. The range of Bluetooth depends upon its power class which covers one to one hundred meters; it also includes a low-cost microchip in each device.

This flexibility is making Bluetooth vulnerable to interceptions, and the most serious flaws of Bluetooth security may be the disclosure of personal data. Research from the University of Tel Aviv in Israel has detected that Bluetooth can be cracked, and these findings have been published in the *New Scientist*. The researchers have shown both active and passive methods for obtaining the PIN for a Bluetooth Link. The passive attack would allow a suitably equipped attacker to eavesdrop on communication. The active method makes use of a specially constructed message that must be inserted at a specific point in the protocol to repeat the pairing process. After that the first method may be used to crack the PIN.

3.3 Technical use in the future

3.3.1 Ambient technology

In a sense, the RFID-chip is a significant part of a development process called ambient technology or, as it is sometimes referred to, as pervasive or ubiquitous computing. Ambient intelligence is an intelligence system that operates in a surrounding environment, a trend brought about by a convergence of advanced electronic, and particularly wireless, technologies and the internet [31]. These ambient devices are not personal computers, but very tiny devices, either mobile or embedded, in many objects, including cars, tools appliances, clothing, and consumer goods in such a way that they become an everyday part of life and reacting to our behavior as

[4] http://en.wikipedia.org/wiki/Bluetooth

well as participating our human needs.[5] Used in refrigerators they can remind us to use the oldest products and once the item is used automatically adding it to our shopping list. The vacuum cleaner can also be started without human intervention once dust density becomes too high. Utilities are able to monitor the performance of home appliances, sending repairmen or replacements before they break down. Local supermarkets can check the content of customers' refrigerators and make out a shopping list for customers. From desktop computers, office workers can check up on children at home [32].

3.3.2 Neurolinguistics

Neurolinguistics is based on the fact that different people are processing information differently [33]. So, for example, there is a difference between male and female brains with the female brains taking more notice of more cues within a piece of communication and using colors, imagery, and graphics much more to interpret meaning compared to male brains. Combined with other technologies a NBIC convergence takes place: combination of nanotechnology, biotechnology, information technology and cognitive science.

Neurolinguistics uses knowledge on how information processing styles differ in order to target consumers. It can be used to detect different responses to car designs and to evaluate television commercials. This type of use is called neuromarketing: seeing how different people respond to advertising and other brand-related messages by seeing brain responses.

3.3.3 Memetics

The science of memetics has recently attracted significant attention [33]. A meme is an idea that is passed from one human generation to another. It is the cultural and sociological equivalent of a gene, the basic element of biological inheritance. In contrast to genetics, a meme acts not vertically through the generations but horizontally. They work as a viral contagion. A good example of the principle is how it is difficult not to start yawning if others are yawning or not applaud when others start to applaud. It is speculated that human beings have an adaptive mechanism that other species don't have. Humans can pass their ideas from one generation to the next, allowing them to surmount challenges more flexibly and more quickly than through the longer process of genetic adaptation and selection. Examples of memes include the idea of God and other forms of belief.[6]

It is believed that changing memes means a change in personality, for example when anti-depressants are used. Therefore it is a concern that others can use memes to influence human behaviour and influence humans both in commercial areas and in political campaigns. The influence might be an unconscious one that might be most enduring if installed at an early stage. In relation to memes it is feared that marketers can use it to infect consumers with a mind virus that is not recognised consciously but which suddenly results in joining a fad or fashion.

---

[5] http://searchnetworking.techtarget.com/sDefinition

[6] http://whatis.techtarget.com/definition

3.3.4 Grid technology

A new way of living will evolve as the internet morphs into 'the grid'. Wireless tags will be embedded in nearly every object, and even people, linking humans and machines together as 'nodes' on a single global network. By tying all computers together into a single grid, this system will allow any one computer to tap the power of all computers. It is a sort of fourth wave bringing together the power of mainframes, PCs, and the Internet. This grid system will be able to link companies, consumers, and governments together. Biochips might be able to send real-time heart readings to cardiologists by way of the grid. "A smart chip in your convertible could allow the manufacturer to track both the car and your driving habit. A digital double of your car might even be parked on the grid, where your mechanic could watch it for engine trouble or the police could monitor your speeding" [34, p. 67]. The endless streams of data are too voluminous for human engineers to track. The grid therefore will have to be self-managing, self-diagnosing, and self-healing, telling people when things go wrong and instructing us on how to fix them. At the moment there seems to be only one problem: software to make the grid secure does not yet exist. It is said that in a highly networked world the 'castle' model of security with firewalls will not work.

4 The protection of privacy

4.1 Introduction

As we have already noted, the first protections of privacy came from the citizen himself or from relatives. During the Middle Ages this picture stayed almost the same. However with the rising intrusion of governments into private lives, assistance against privacy intrusion required the help of others, legal legislation, and the addition of self-regulation. Later technical instruments like security measures and PET were added.

EPIC distinguishes four models of privacy protection [14, p. 3]:

- Comprehensive laws: a general law that governs the collection, use, and dissemination of personal information by both the public and the private sector. An oversight body then ensures compliance.
- Sectoral laws: rules in favour of specific laws, governing specific technical applications, or specific regions, such as financial privacy.
- Self-regulation, in which companies and industry establish codes of conduct or practice and engage in self-policing.
- Technologies of privacy: with the development of available technology-based systems it becomes possible for individuals to protect their privacy and security.

Although there will always be distinctions between countries and cultures in how these four measures will be emphasized, it seems clear that the countries which will protect the data most efficiently will probably use all four of the models simultaneously to ensure data protection.

As can be seen from the formulation in this model, emphasis will be on data protection. Nonetheless it is necessary to make the distinction between privacy protection and data protection. The first is a general protection historically oriented towards the home, family life, and correspondence while the latter will emphasis the informational dimension.

4.2 Comprehensive laws and regulatory agents

The legal interpretation of privacy depends on the way the concept is used. As we have seen, two dimensions can be distinguished: a relational and an informational one. With respect to the relational privacy there has been a long tradition in Europe and in the United States. In terms of protecting data, the regulation is nascent. In 1971 the first privacy act, The Data Protection Act, took effect in the State of Hesse (Germany); shortly thereafter, Sweden and the United States passed privacy legislation. Subsequently, privacy protection has become a part of many constitutions, with the exception of the United States where the protection must be derived from amendments. This paper will start with a short overview of the situation in the United States followed by a more extensive treatment of the situation in Europe.

4.2.1 Privacy protection

Although the United States is the country where most of the earliest discussions have taken place, privacy protection has never had a base in the U.S. constitution. An important characteristic of the American constitution, which went into effect in 1789, is that in general it has a negative formulation. The U.S. constitution does not oblige the government to protect but rather to refrain from taking actions. In that sense and in an indirect way, people are protected against government actions. Although more or less all constitutional freedoms are related to privacy, this type of privacy right is not explicitly mentioned in the Constitution. In particular it must be derived from three amendments: the First, Fourth, and Fourteenth.

The First Amendment protects the freedom of expression, religion, and assembly. The freedom of expression assures the unfettered interchange of ideas for the bringing about of political and social change by the public [19].

The Fourth is centered on the prohibition of unreasonable search and seizure. As can be understood from the history in the United States, it has two deeply rooted concerns: that its citizens' property is protected from seizure by the government and that its citizens' home and person be protected from warrantless and arbitrary searches. This very amendment is the much used, but still unclear, concept of 'reasonable expectation of privacy' which was introduced by Justice Henson in the famous court case *Olmstead vs. US*.

The Fourteenth Amendment guarantees due process and nondisclosure of personal information. As this language is more in line with the informational dimension of the computer age, we will treat this amendment in relation to data protection.

Although there has been some form of legal privacy protection for some time now based on case law, international recognition of privacy as a human right can be traced back to the period immediately following the Second World War. Recognition of this particular right emerged as a response to some of the abuses perpetrated by fascist regimes before and during the war. The Universal Declaration of Human Rights was adopted on 10 December 1948 by the United Nations general Assembly. In article 12 the territorial and communications privacy is protected. It states: "No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interference or attacks." It was the first international instrument to deal with this right to privacy. As it was in the form of a resolution of the General Assembly it was not legally binding.

In 1950 the European Convention for the Protection of Human Rights and Fundamental Freedoms was drafted. Article 8 of the Convention is still one of the most important international agreements on the protection of privacy: "Everyone has the right to respect for his private and family life, his home and his correspondence." At the same time the second paragraph of the article makes clear that this right to privacy is not absolute. Interference by a public authority is allowed when such is necessary in accordance with the law and is necessary in a democratic society in the interest of national security, public safety, and the economic well-being of the country, for the prevention of disorder or crime, for the protection of health and morals or for the protection of the rights and freedoms of others. With this formulation three zones of privacy are defined, that is private and family life, home, and correspondence, although correspondence is very narrowly related to the secrecy of letters.

This Convention has a legal mechanism for its enforcement through the European Commission. It is legally binding on each state that ratifies it and must be put into effect in its domestic laws. This Convention has inspired many countries to create and formulate national laws and constitutions for the protection of privacy that went further than the requirements of this Convention as was already the case in the United States in the First, Fourth, and Fourteenth Amendments. In particularly the notion of correspondence has been deepened.

4.2.2 Data Protection

Although the protection of personal data is dealt with in the Fourteenth Amendment this turned out to be increasingly insufficient in an age in which information became an important force. Therefore in 1974 the Privacy Act was enacted which enforces agencies to process data fairly and limits the disclosure of individual records. The Privacy Act protects in full American tradition primarily against governmental processing of data. In the private sector the emphasis is on self-regulation combined with specific sectoral laws. A few examples out of numerous ones are the Children's Online Privacy Protection Act (COPPA) of 1998, the Fair Health Information Practice Act of 1997, and the Fair Credit Reporting Act of 1997.

As we have seen since the 1960s, the relationship between privacy and the use of data has become closer as has the awareness that this form of privacy should be protected. In addition to the domestic laws on data protection, in 1981 a special Convention was devoted to the use of personal data: the Convention for the Protection

of Individuals with Regard to Automatic Processing of Personal Data [35]. In this convention some general guidelines were formulated with regard to data processing and were elaborated in approximately twenty recommendations for specific fields, such as police, medical data, and statistical data.

These guidelines are in large part are based on the principles of data protection formulated by the Organisation for Economic Co-operation and Development (OECD) which outlines protection is equated to privacy protection [36]. Curiously, the OECD is endorsing the protection of privacy on the one hand, yet they are promoting these principles because there is a danger that disparities in national legislation could hamper the free flow of personal data across the frontiers. Restrictions of these flows could cause serious disruption in important sectors of the economy, such as banking and insurance. For that reason these principles can be seen as guidelines that enhance fair and good practices more than they enhance privacy protection. Nevertheless they have had a big influence on all data protection legislation in Europe and elsewhere.

These principles are:

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

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

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

Use Limitation Principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the specified purpose except: (1) with the consent of the data subject or (2) by the authority of law.

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

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

Individual Participation Principle: An individual should have the right: (1) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (2) to have communicated to him, data relating to him (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; and (iv) in a form that is readily intelligible to him; (3) to be given reasons if a request made under subparagraphs (1) and (2) are denied, and to be able to challenge such denial and (4) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

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

These principles, however, have not been implemented in legislation in all member states of the European Union in the same way. Therefore the fear of hampering the free flow of information remained. In the beginning of 1990 an effect was made to harmonize legislation within the EU. It resulted in a European Directive on Data Protection [37].

This directive enshrines two of the oldest ambitions of the European integration project: the achievement of an Internal Market (the free movement of personal information) and the protection of fundamental rights and freedoms of individuals. It is stated that both objectives are equally important. The status of such a directive is that it binds member states to the objectives to be achieved, while leaving to national authorities the power to choose the form and the means to be used to implement these objectives.

The directive applies to the public and private sector and covers the processing of personal data by both automated and manual means. Processing includes any operation or set of operations which is performed on personal data, which mean all information relating to an identified or identifiable natural person. This directive elaborates in a way the general OECD principles operationally. These principles are formulated relating to data quality and criteria are given for making data processing legitimate. Special attention is paid to special categories of processing of data of what formerly was called sensitive data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. Processing of data relating to offences, criminal convictions or security means may be carried out only under the control of official authorities, with suitable specific safeguards, or as provided under national law. The controller, that is to say the one who determines the purpose and means of processing is obliged to inform the data subject about the purpose of the processing, except where he already has the information. As already is written into the principles, the data subject has the right of access to his own data as well as the right to rectify, erase or block the processing of data in case the data are not correct or not up to date.

All member states are obliged to comply with the directive and to implement the principles in national laws. With the implementation the member states shall provide

that one or more public authorities are responsible for monitoring the application with its territory of the provision. Regarding the transfer of data to third countries (countries outside the European Union) there is the strict rule that this transfer may take place only if the third country in question ensures an adequate level of protection, judged as such by the European Commission. If this level is missing, additional measures have to be taken either in conformity with the directive or in the form of contractual clauses. One of them is the so-called Safe Harbour Principles formulated by the Federal Trade Commission (FTC) in the United Sates.

4.2.3 Regulatory agents

An essential aspect of any data or privacy protection is oversight. In most countries with a comprehensive law or an omnibus data protection, there is a data commissioner, sometimes in the person of an ombudsman. Under the Directive 95/46/EC, it is an obligation to have such a data commissioner.

Under article 21 of this directive, all European Union countries, including the new ones, must have an independent enforcement body. These agencies are given considerable power: governments must consult the body when they draw up legislation relating to the processing of personal data; the bodies also have the power to conduct investigations and have a right of access information relevant to these investigations; they may impose remedies such as ordering the destruction of information or ban processing and start legal proceedings, hear complaints, and issue reports. The official is also generally responsible for public education and international liaison in data protection and data transfers. They have to maintain a register of data controllers and databases. They also are represented in an important body at the European Union level through article 29 Working Group which issues reports and comments on technical and political developments.

4.3 Sectoral laws

As we have seen, the recommendations based on the Strasbourg Convention form a kind of sectoral legislation in addition to a more comprehensive legislation. In 1997 a special European directive was adopted which is specifically related to the protection of privacy in the telecommunication sector [38]. The development of more advanced digital technologies, such as the Integrated Services Digital Networks (ISDN) gave rise to specific requirements concerning the protection of personal data. Meanwhile this directive is repealed and replaced by a directive on privacy and electronic communications [39]. In addition to Directive 95/46/EC which formulates general principles of data protection, this directive is oriented towards the use of new advanced digital technologies in public communications net works, in particular the internet.

The new Directive is a response to two developments that addresses the idea that the private sphere must be protected in a more advanced way. The first is the development of so-called spyware, web bugs, hidden identifiers, and other similar devices that can enter the user's terminal unawares. Such devices, for instances cookies, should be allowed only for legitimate purposes and with the knowledge of the user concerned. These cookies may, for example, only be used for analyzing the

effectiveness of website designs and advertising and in verifying the identity of users engaged in on-line transactions. Users should therefore have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment.

The second development is unsolicited communications. In the EC directive, safeguards are provided against the use of unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, e-mail, and SMS messages. For these forms of communications the prior explicit consent of the recipient must be obtained before such communications are addressed to them; in short the user must opt in for these communiqués to be legitimate. The only exception is the use of electronic contact details for the offering of similar products or services by the company that has obtained these contact details. The customer should be informed about this use and be given the opportunity to refuse such usage or to opt out.

This directive, then, is meant not only to protect the privacy of the consumer, it allows also for the retention of traffic and location data of all people using mobile telephones, SMS, landline telephones, faxes, e-mails, chatrooms, internet, and any other electronic communication devices. The traffic data include all data generated by the conveyance of communications on an electronic communications network, and location data is the data indicating the geographic position of a mobile telephone user, like the GPS. The contents of communications are not covered by these measures.

4.4 Protection by technical means

Related to technological instruments, Charles Raab [40] makes a distinction among the following:

- *Systemic instruments* which are produced by engineers who design the network, the equipment, the computer code, or the technical standards and protocols;
- *Collective instruments,* which result from government policies, such as policy applications in which government and business builds privacy protection into a technical systems for goods and services, such as the development of a public key encryption infrastructure;
- *Instruments of individual empowerment,* required for explicit choices by individuals, such as encryption instruments, devices for anonymity, filtering instruments, and the Platform for Privacy Preferences (P3P)

4.4.1 Systemic instruments

The systemic approach regulates to the technical rules embedded within the network architecture. The technical standards and protocols as well as the default settings chosen by system developers set threshold information privacy rules. They define the capabilities of networks to invade or protect privacy. As an example anonymous internet use may be built into the network structure just as surveillance tracking may be built into the network. Cookie management options are developed to allow users greater control over such tracking. Joel Reidenberg [41] calls this kind of regulations the *Lex Informatica.*

4.4.2 Collective instruments

One example of these instruments is a measure which becomes well known under the name Privacy Enhancing Technologies (PET's). The basic idea behind PET was developed by David Chaum, who published an article in *Communications of the ACM* on security without identification [42]. Although this article and other publications of Chaum got a lot of publicity, the real breakthrough came when the data protection authorities of The Netherlands and Canada published two reports on Privacy-enhancing Technologies [43].

PET's are a coherent system of ICT[7] measures that protect privacy by eliminating or reducing personal data or by preventing the unnecessary or undesirable processing of personal data without losing the functionality of the information system. Eliminating personal data means that adequate measures are taken to prevent identification of a person. Direct and indirect identifiers are removed in such a way that a person can no longer be identified. Reducing personal data means that although identification is possible it is made more difficult and is only allowed in a controlled context, for example by using a Trusted Third Party (TTP). In both situations the starting point is that personal data are not always needed and that the necessity of the personal data must be proved. If that is not possible, either the data is made anonymous or a so-called Identity Protector is used, which converts the actual name to a pseudo-identity.

A very old application of this kind of technology is data security. Data or information security means that a coherent package of measures is taken and maintained for securing the collection and processing of information. These measures are related to availability (information must always be available for the legitimate user), exclusiveness (information may only be used by authorized persons), and integrity (information must be in accordance with reality and be reliable, correct, and up to date). To be accurate as to which types of measures are needed, a risk analysis is necessary in which the importance of information is measured as well as the consequences in case the information gets lost. These measures enclose all people and all means that are necessary for data processing. A concrete plan is made including all technical and organizational measures that should be taken, regarding the costs, the state of the technique, and the risks of the processing. Well known security measures are firewalls, which protect against unauthorised access, the use of passwords, and the authorization for the users of information.

4.4.3 Instruments of individual empowerment

One peculiar application of PET is offering the individual the means and measures for empowering his own control over the processing of his personal data. It deals with instruments that can be chosen by the individual to enhance his control over the processing and distribution of his data. Sometimes these instruments are called add-ons and well known examples are the cookie killers, the proxy servers, anonymous remailers, and the Platform for Privacy Preferences.[8] A good example of such an instrument in relation to the internet is the system MUTE, developed by Jason Rohrer [44], in which random access strings are used. Each time a computer (node) is

---

[7] Information and Communication Technology

[8] See f.e. www.anonymizer.com; www.zeroknowledge.com; www.privada.com.

connected with a P2P network that uses software to facilitate the sharing of music, a new IP-address is generated, making it extremely difficult to track the user.

Another example of this type of protection is the research done after PISA: Privacy Incorporated Software Agent. PISA is a specific application of the Intelligent Software Agent Technologies (ISATs). PISA enables the user to control the quality of input of the consumer or the citizen in e-commerce or e-government transactions and communications for protection against loss of control over personal information. A much discussed disadvantage for the protection of privacy is that agents need to maintain a perfect profile of their users in order to know one's likes and dislikes, habits and personal preferences, contact information about friends and colleagues, or the history of websites visited, and many other electronic transactions performed.

4.5 Protection through bad publicity

During the last years a strong form of protection has come from the media which publish regularly on all types of misuse of data. In some cases, the public outcry has demonstrated the significant role of the media in informing consumers and facilitating a popular response. The media then highlights not only the effectiveness of protests but also the potential for the technologies such as e-mail and general internet usage in order for disclosure of information to be used to protect privacy.

In Stockholm a discussion started on February 10, 1986 when the newspaper *Dagens Nyheter* intensified its coverage of the Metropolit study [45]. Metropolit Projects in Copenhagen, Oslo, and Stockholm were initiated based on the same concept. All males born in these three cities were registered from birth certificates by way of regular medical investigation. Age tests, as well as psychological tests, home surveys on military service, and family particulars were carried out. The different files were all identified with a personal identification number which made linkage possible. Discussion of one specific research project rapidly escalated into a general outcry against micro data research methods. The strongest criticism was leveled at the fact that many variables were merged into databases from other sources as well as from paper documents. A subsequent judicial examination proved that no illegal activities had taken place, and that neither data laws nor any other instruction or legal provision had been contravened. Despite the fact that Statistics Sweden had not been in any way involved in the project, the affair had a strong negative influence on the public attitude towards social research in general and Statistics Sweden in particular.

In 1991 Lotus Development Corporation and Equifax abandoned plans to sell Households a CD-ROM database containing names, addresses, and marketing information on 120 million consumers, after they received 30.000 calls and letters from individuals asking to be removed from the database. More recently, Lexis-Nexis, has changed plans for P-tracks, a service that provides personal information about virtually every individual in America to "anyone willing to pay a search fee of eighty-five to hundred dollars" [20, p. 104/105]. The database includes current and previous addresses, birth dates, home telephone numbers, maiden names, and aliases. Lexis was also providing social security numbers but stopped in response to a storm of protest and is honouring the requests of anyone who wishes to be deleted from the database.

So found the Vons chain of supermarkets in Los Angeles [46] itself the recipient of unwelcome front page publicity when it allegedly used data contained in its store-card database to undermine a damages claim from a shopper. The shopper claimed that he slipped on spilt yogurt in the store, shattering his kneecap, but said that when he filed a suit for damages, he was advised by the store's mediator that his club card records showed him to be a frequent buyer of alcohol.

5 Analysis

Analysis of the use of personal data shows how important information is becoming and shows the omnipresence of technique, probably resulting in a surveillance society.

5.1 Importance of Information

Information is becoming more and more important since it has two characteristics: information is *money* and information is *power*. Although these two characteristics partly are in parallel with the distinction between the private and public sector, a cross fertilization appears quite often. The private sector is not only interested in money but very often in an influence, as can be seen in the power that insurance companies wield. In addition, the public sector is also interested in influencing people and in money. These two characteristics, then, make it clear that in contrary to general opinion, privacy is not a true juridical issue, but in fact a political one. Making money and having power are not wrong; however, the way such influence is used, and perhaps over-reach, can create problems.

Several tools are used for collecting and analyzing personal information: database marketing, relationship marketing, permission marketing, and loyalty programs which all help marketers to find the information they crave. When these collection techniques combine with data warehousing and data mining tools, individual information security can be at risk. Database marketing is also known as one-to-one marketing, whereas permission marketing acknowledges the need of permission from customers before approaching them with advertising messages, which can stand as one solution to the problem. The philosophy behind this approach is that customers are willing to release personal information if they can profit by doing so, as seen with loyalty cards. The consequence is that direct marketers fill mailboxes; relationship marketers ask for more and more information; telemarketers call home at dinner time; and spam is a highly used tool for advertisement.

Getting and using power is again a question of balancing several interests and balancing the means and the political choices. Political choices mean that choices are made in which the privacy is protected as much as is possible. The impetus for information as a means to knowledge and power became visible after the dramatic attacks of terrorists on September 11, 2001. These policy changes were not limited to the United States but also involved most other countries with increasing surveillance powers and minimizing oversight and due process requirements. The use of new technologies were incorporated and included which in turn permitted governments to

use these powers and formalize its roving powers. In general, the result was a weakening of data protection regimes, an increase in data sharing, and an increase in profiling and identification [14, p. 25-27] of individuals.

As we have seen, information is power and since the terrorist attacks in New York, Madrid, and London this type of power over citizens is becoming more and more a reality. Information is seen as one of the most important weapons in the battle against terrorism and crime. Measures like the introduction of Passengers Name Records (PNR) and the long retention of traffic communication data make clear that politics in one way or another will win. Data commissioners talk about balancing the interests of privacy protection and the protection of security, but it is clear that one can not speak of a real balance. Laws are used to accept means and measures of data collection which were never accepted without the current political agendas. The introduction of CCTV, the use of internet data, and the exchange of data among all western countries are clear examples of this untoward development.

Long before the attack of 9/11 intelligence agencies from America, Britain, Canada, Australia, and New Zealand jointly monitored all international satellites telecommunications traffic by a system called 'Echelon', which can pick specific words or phrases from hundreds of thousands of messages. In 2000 it was publicly revealed that the America's FBI had developed and was using an internet monitoring system called 'Carnivore'. The system places a personal computer at an internet service provider's office and can monitor all traffic data about a user, including e-mail, and browsing. It gives governments, at least theoretically, the ability to eavesdrop on all customers' digital communications.

5.2 The Omnipresence of Technique

Compared with approximately one hundred years ago, the situation has changed dramatically. From an incidental intrusion by humans into each other's lives and, rarely, having the technical means to find out too much, society now has the technical means and capacity of collecting individual data to a serious level. Since technique is omnipresent and, as an old sociological wisdom says, humans are a data producing animal, all tracks and traces left behind by human beings can be and are collected. As we have seen, since information is money and power government and industry are using almost all means at their disposal for this data collection regime.

It is, however, not only the omnipresence of technique which is frightening but also the sheer lack of awareness of its usage. One of the most impressive examples is the way data can be collected from the internet. Cookies and more general spyware are used to collect data without our knowledge. And this lack of transparency increases once data are used. Although in many case we know the purpose of the use, we do not always know for sure whether the actual use is as indicated. Responsible for this lack of transparency in data mining is making clear the distinction between data and information. Data is a collection of details or facts which, as such, are meaningless; however, when those details or facts are placed in a context which makes data usable, serious information can be gleaned. Depending upon the placement-context, the same data can be transformed into different information.

The classical example is the speed of a car. Saying that a car is driving at a speed of forty miles does not mean anything. Depending upon the context, for example in a city or on a highway, the information can be interpreted quite differently: in a city, forty miles per hour can be too fast, especially in a school zone during school in-take hours but on a highway, forty miles per hour may be too slow and seriously jeopardize the flow of traffic.

Another example is the supermarket which introduces loyalty cards and asks patrons to fill in a form in which the sex of the owner of the card and the sex of his of her partner must be filled in. Although it was said that the provided data would only be used for contacting the owner or his or her partner, it is clear that the data can also be used for detecting homosexual relations. Numerous other examples make clear the importance of the distinction between data and information. Knowing for what purpose *data* are used does not mean that for the same purpose the *information* would be used.

5.3 Surveillance

The omnipresence of technique and the acceptability of politics and the law to collect, store, and use almost all personal data is making the information society a surveillance society. Simultaneously the number of techniques is increasing so intrusion of privacy is inevitable. Distinct authors [47], [48], [26], agree that surveillance might create conformist actions. People will keep their records clean and will avoid controversial or deviant behaviour, whatever their private views and intentions might really be.

But it is not only surveillance that matters, it is the fact that we are on the way to a *riskless* society in which more and more the policy is oriented toward avoiding risks and errors produced by human beings. Personal data is used for determining the amount of risk a person forms in the eyes of government and industry. In government these figures are used for political reasons, in industry for discriminating between the good and bad consumer. It is this use which makes a consumer into a glass-consumer, in a manner of speaking, for whom there is a deep concern for unfair exclusion, unfair targeting, and unfair discrimination [49].

6 Lessons learned of?

Starting with the more general discussion on privacy in 1891 with the publication of Warren and Brandeis *The Right to Privacy* we will pose the question if we have learned from the developments and incidents. The answer must be: yes and no. For making this clear three periods must be distinguished.

The first is the period between 1891 end the beginning of the 70's of last century. This period can be described as the period of growing awareness of the importance of privacy and privacy protection. Many articles and books on privacy are published in which this importance is stressed cumulating in Alan Westin's *Privacy and Freedom.*

The second period –from the beginning of the 70's till the beginning of the 21th century- can be described as the period of taking measures ending in the

implementation of the European Directive on Data Protection, not only in the European countries but in almost all technological advanced countries. Together with the establishing of data protection authorities a kind of legal protection is suggested. Unfortunately this legal protection is overemphasised, in particular by the data protection authorities, and seen as the only best solution for a political problem.

This becomes obvious in the third period which starts at the beginning of this century. In this period the incident of 9/11 is of overriding importance. It makes clear how information can be used in the battle against fraud, criminality and terrorism. It at the same time shows the weakness of legal regulation as these regulation can simple be overruled by legislation in favour of order and law. It shows again how the protection of privacy is a political issue that can not be solved by only legal means. In that sense it is stimulating that the young generation, as for example present at the Summerschool in Brno, was not so much looking at the legal solution as well on technical solutions, like security and anonymity. It was even more stimulating that they went back to the basis, the articles of David Chaum published in the beginning of the 90's of the last century. He in my view is the real Godfather of the philosophy that in a period in which the stress is on the use of information for almost all purposes the path to anonymity is an important solution. In that sense legal people have learned less form the past, the technical people seemingly the more.

7 Conclusions

The legal measures, and the way political decisions are taken, make clear that data protection is passive. The consumer or citizen plays almost no significant role in the process. It is the government (laws) and industry (laws and self-regulation) who define the way and amount of protection. A more active role can be played when the consumer or citizen is allowed to use technical means, but also in this case it is politics and government who determines when and how these techniques may be used.

It is the government that wants to control the use of information and refuses to strengthen the position of the individual. For that reason, almost all emphasis is on reactive control of privacy predicaments. If some form of participatory control is given, it is always given under the restriction that in the end it is the government who has the ultimate control. Only in relation to industry does the role of the consumer become legally empowered regarding the use of cookies and spam. At the same time industry is used as a source of information. Traffic and location data must be stored longer then is necessary and must be given to a government in case of suspicion of terrorist actions.

Not only are these techniques empowering governments but they also become legal as has been seen in the case of the Patriot's Act in the United States and the Regulation of Investigatory Powers Act in the United Kingdom. The same development can be seen at the Directive on Privacy and Electronic Communications, which opens the possibility to enact from domestic laws the retention of traffic and location data. Most especially, these developments strongly suggest vigilance. Information as a means of power and legislation as legitimizing power are dangerous

instruments in the hands of unethical politicians who are missing the necessary checks of balances of a democracy. In that case not only is privacy at stake but above all so is democracy. It is time to revisit the use of technology, the law, and the role consumers have in this serious issue. A positive sign comes from the British National Consumer Council in its publication *The Glass Consumer, Life in a Surveillance Society* [50]. Although the title sounds pessimistic, the book ends optimistically with the NCC's agenda and recommendations for the future.

References

1. A.W. Branscomb, Who Owns Information? From Privacy to Public Access. New York: Basic Books (1994).
2. Barrington Moore Jr., Studies in Social and Cultural History. Armonk, New York: M.E. Sharpe, Inc. (1984).
3. Richard F. Hixson, Privacy in a Public Society. Human Rights in Conflict. New York, Oxford: Oxford University Press (1987).
4. David H. Flaherty, Privacy in Colonial New England. Charlottesville: University Press of Virginia (1972).
5. Alan F. Westin, 'Science, Privacy and Freedom: Issues and Proposals for the 1970's. Part I; The Current Impact of Surveillance on Privacy, Disclosure, and Surveillance', in Columbia Law Review, 66, (1966), 1003-1050.
6. Alan F. Westin, 'Science, Privacy and Freedom: Issues and Proposals for the 1970's. Part II, Balancing the Conflicting demands of Privacy, Disclosure, and Surveillance', in Columbia Law Review, 66, (1966), 1205-1253.
7. Alan F. Westin, Privacy & Freedom. London, Sydney, Toronto: The Bodley Head (1967).
8. Alan Bates, 'Privacy – A Useful Concept?', in Social Forces, 42, (1964), 429-435.
9. Myron Brenton, The Privacy Invaders. New York: Coward-McCann, Inc. (1964).
10. Annette Harisson, The Problem of Privacy in the Computer Age, an annotated bibliography. Santa Monica: The Rand Corporation (1967).
11. Sidney M. Jourard, 'Some Psychological Aspects of privacy', in Law and Contemporary Problems, 31 (1966), 307-319.
12. Harry Kalven Jr., 'The Problem of Privacy in the Year 2000', in Daedalus, 93 (1967), 876-882.
13. Milton R. Konvitz, 'Privacy and the Law: a Philosophical Prelude', in Law and Contemporary Problems, 31, (1966), 272-281.
14. EPIC, Privacy & Human Rights, An international Survey of Privacy Laws and Developments. Washington: Electronic Privacy and Information Centre and Privacy International (2002).
15. The Economist, Move over, Big Brother, 'The Economist Technology Quarterly, 2 December (2004), 26.
16. Barbara Garson, The Electronic Sweatshop, How Computers Are Transforming the Office of the Future Into the Factory of the Past. New York: Penguin Books (1988).
17. Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy', in Adam Carlyle Breckenridge, The Right to Privacy. Lincoln: University of Nebraska Press (1970), 133-153.
18. Miichael F. Mayer, Right of Privacy. New York: Law Arts Publishers, inc (1972).
19. William Zelermyer, Invasion of Privacy. Syracuse University Press (1959).
20. Fred H. Cate, Privacy in the Information Age. Washington D.C., Brooking Institution Press (1997).

21. William H. Whyte, The Organization Man. Middlesex: Penguin Books (1956).
22. Vance Packard, The Hidden Persuaders. Midddlesex: Penguin Books (1964).
23. Oscar M. Ruebhausen and Orville G. Brim Jr., 'Privacy and Behavioral Research', in Columbia Law review, 65 (1965), 1184-1211.
24. Malcolm Warner and Michael Stone, The Data Bank Society. Organizations, Computers and Social Freedom. London: George Allen and Unwin LTD (1970).
25. Arthur Miller, The Assault on Privacy: Computers, Dossiers and Data Banks. Ann Arbor: The University of Michigan Press (1971).
26. Jay Stanley and Barry Steinhardt, Bigger Monster, Weaker Chains, The Growth of an American Surveillance Society. New York: American Civil Liberties Union (2003).
27. Simon Davies, 'Big Brother at the Box Office, Electronic Visual Surveillance and the Bog Screen', in Proceedings of the 21th International Conference on Privacy and Personal Data Protection. Hong Kong (1999), 151-160.
28. A.J. Elbirt, 'Who are You? How to Protect Against Identity Theft', in IEEE Technology and Society Magazin, (2005), 5-8 .
29. Ann Cavoukian, Identity Theft Revisited: Security is Not Enough. Ontario: Information and Privacy Commissioner (2005).
30. Michael Erbschloe and John Vacca, Net Privacy, A Guide to developing and implementing an ironclad ebusiness plan. New York: McGraw-Hill (2001).
31. Penny Duquenoy, and Vijay Masurkar, 'Surrounded by intelligence …' in Penny Duquennoy, Simone Fisher-Hübner, Jan Holvast and Albin Zuccato, Risks and Challenges of the Network Society. Karlstad: Karlstad University Studies (2004), 121-134.
32. The Economist, 'The surveillance society', May 1st (1999).
33. Martin Evans, 'The data-informed marketing model and its social responsibility', in Susanne Lace [Ed.], The Glass Consumer, Life in a surveillance society. National Consumer Council (2005), 99-132.
34. Rana Foroohar, 'Life in the grid', in Newsweek, September 16-23 (2002), 64-67.
35. Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, European Treaty Series No. 108, Strasbourg (1982).
36. OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris (1981).
37. Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data, Official Journal of the European Communities (1995), 281/31-50.
38. Directive 97/66/EC of the European Parliament and the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, Official Journal of the European Communities (1998), 24/1-8.
39. Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communication, Official Journal of the European Communities (2002), 201/37-47.
40. Charles Raab, 'Regulatory provisions for privacy protection', in Susanne Lace [Ed.], The Glass Consumer, Life in a surveillance society. National Consumer Council (2005), 45-67.
41. Joel Reidenberg, 'Technologies for Privacy Protection'. Paper presented at the 23rd Internation Conference of Data Protection Commissioners, Paris (2001).
42. D. Chaum, 'Security without identification: Transaction Systems to make big brother obsolete', in Communications of the ACM, 28 (1985), 1020-1044.
43. Henk van Rossem, Huib Gardeniers and John Borking, Anne Cavoukian, John Brans, Noel Muttupulle and Nick Magistrale, Privacy-enhancing Technologies, The path to anonymity. Volume I and II. Registratiekamer, The Netherlands & Information and Privacy Commissioner, Ontario, Canada (1995).

44. Frances S. Grodzinsky and Herman T. Tavani, 'Verizon vs the RIAA: Implications for Privacy and Democracy'. Paper presented at ISTAS '04, International Symposium on Technology and Society, Globalizing Technological Education (2004).
45. Lennart Brantgärde, 'Swedish trends in Data Protection and Data Access', in Paul de Guchteneire and Ekkehard Mochmann [Eds.], Data protection and data access. Amsterdam: North-Holland (1990), 105-122.
46. Computer Business Review, June 2001.
47. David Burnham, The Rise of the Computer State. The threat to our Freedoms, our Ethics and our democratic Process. New York: Random House (1983).
48. David Flaherty, 'The Emergence of Surveillance Societies in the Western World: Toward the Year 2000', in Government Information Quarterly, 4 (1988), 377-387.
49. Harriet Hall, 'Data use in credit and insurance: controlling unfair outcomes', in Susanne Lace [Ed.], The Glass Consumer, Life in a surveillance society. National Consumer Council (2005), 157-186.
50. Susanne Lace [Ed.], The Glass Consumer, Life in a surveillance society. National Consumer Council, 2005.