

Surveillance technology and law: the social impact*

Dr. Pieter Kleve, Prof. Richard De Mulder and Dr. Kees van Noortwijk
Erasmus University Rotterdam.

Abstract

In this article, attention will first be paid briefly to surveillance technology as such. An attempt will be made to sketch out the extent and the limitations of the techniques. A question then addressed is why the use of this technology is growing. Given the increasing interest in surveillance technology, an examination is made of the permissibility of the use of this technology taking certain constitutional and legal rights into account. What is the role of supervisory technology within the context of wider social developments? The article reaches the conclusion that with the increasing significance of surveillance technology and the increasing use of it the importance of 'monitoring the surveillers' will increase as well.

1. Introduction

There had been serious rioting after a football match on the 17th April 2005 in Rotterdam, the Netherlands. On Tuesday, 30th of August 2005, approximately 17,000 mobile phone users who, according to the transmitter data of the telephone provider, had been in the vicinity of the football stadium in Rotterdam on the day of the riots received an SMS. The SMS was from the Rotterdam police force and urged all those with any knowledge of the riots to come forward and help the police with their inquiries. This is one of the many recent examples of technology being used as an instrument of surveillance. Such use has not been without criticism, in particular with respect to infringing the right to personal privacy and creating a 'big brother' atmosphere.¹

Technology for surveillance and monitoring has, in today's society, become commonplace. In the Netherlands, for example, because of the risk to public health caused by air pollution, in the Rotterdam area certain so-called 'sniffing poles' have been installed. They measure the level of air pollution and when a certain limit is reached a warnings system is activated. As a consequence of the disastrous tsunami in December 2004, a tsunami warning system has been installed in the Indian Ocean. And, in general, in various industrial sectors, many processes are monitored with the help of technology; hospitals use technology to monitor the state of the human body and our financial obligations are monitored by computers that send us reminders and final demands if the payment has not been made on time.

Surveillance and monitoring technology has become commonplace throughout the world. It is used to supervise both social and physical processes, and to monitor individual behaviour. This technology is constantly being refined. For example, speeding, as an offence that forms a risk to public health, has for some time been dealt with by technology. The standard approach has been to have a camera that takes a

* In: Proceedings of The First International Conference on Legal, Privacy and Security Issues in Information Technology, Sylvia Mercado Kierkegaard (ed.), Hamburg April 30 - May 2, p. 473-492. ISSN: 0806-1912

¹ C.f. D.J. Solove, 'Privacy and Power: Computer Databases and Metaphors for Information Privacy', *Stanford Law Review*, 2001 Vol. 53, <http://docs.law.gwu.edu/facweb/dsolove/Privacy-Power.pdf>.

photograph of the car once a certain maximum speed has been exceeded. Having established the level of the speeding, a fine is then sent to the car owner. However, in this set up the camera can only register the offence if it takes place where the camera is located; speeding either before or after the location of the camera cannot be registered. To remedy that deficiency, a new form of surveillance has made its appearance: it is now possible to follow the car along a section of the road. A camera located at one place on the road registers the speed of the car at that point and a camera placed a number of miles farther down the road registers the speed there. A computer then calculates the average speed of the car along that stretch of road between the two cameras. If the average speed is too high, a fine will be sent. For the road user, this development means that it is pointless just to slow down at the location of the first camera; speed must be kept down for the whole stretch of road between the two cameras.²

In the above example, there are legitimate legal grounds for the use of surveillance technology; the law has already laid down what constitutes the maximum speed and the carrying out of the procedure is the responsibility of the state. This surveillance technology has led to a certain conditioning of driving behaviour. However, even though we have become familiar with the use of road cameras, that does not mean that their existence is accepted by all road users. It could be that we consider that driving above the speed limit on that particular road, or section of the road, is not dangerous, or that we have a good excuse for speeding. When the check-points were manned by police officers, a sympathetic officer might have been prepared to accept a good story; a camera is not.

Road cameras have stimulated some drivers to find means of evasion. One such technique is the radar detection device, which warns of the vicinity of radar controlled speed measurement equipment. That has led some authorities to demand that such detection devices be made illegal (and consequently some manufacturers have developed detection devices that do not fall within the category of 'illegal radar detection devices'). What this shows is that a rule of law does not, of itself, produce compliancy. Individuals will act in their own self-interest, as they see it.³ This action/reaction phenomenon draws attention to the relationship between a rule of law and the enforcement of that rule of law. The enforcement of a rule of law is of great importance. The use of technology may promote compliance with the law, although that is not always necessarily the case.

Surveillance by camera is, of course, not confined to traffic situations. The use of camera surveillance is common in shopping centres, petrol stations and industrial areas, to name just a few examples. Moreover, camera surveillance is on the increase. If you wish to visit a company, instead of signing in using the traditional guest register, visitors may have to be prepared to undergo a video registration by complying with the friendly request to look in the camera and give their name.

Although camera surveillance is an obvious example of making people feel that they are 'being watched', it is by no means the only form of surveillance. It is already the

² It should perhaps be pointed out that this technology will not catch the driver who only speeds for a very short time on that section of road.

³ C.f. M.C. Jensen & W.H. Meckling, 'The Nature of Man', *Journal of Applied Corporate Finance* 1994-2, p. 4-19.

case that foreigners who wish to enter the USA must provide fingerprints of both index fingers and a passport photograph. Other personal data is provided by the charter company. Nor is Internet as anonymous as its users have long presumed. Surfing on the net leaves countless tracks, which can be picked up by businesses that chart users' Internet behaviour. Given the state's monopoly on coercion, it is not difficult for the state to obtain access to these 'tracks'. There was considerable consternation when the press revealed the existence of the Echelon program of the American National Security Agency (NSA). This controversial program could monitor (or tap) data exchange on the Internet, and thus in effect worldwide. However, the question must also be raised as to whether the consternation would have been greater if it had appeared that the NSA did not carry out such monitoring.⁴

2. Surveillance with the help of technological means

From the above examples, it is clear that technology plays an important, and in some cases even an essential, role in surveillance. For that reason, attention will now be paid to a number of possibilities for surveillance that can be realized by using technology. Surveillance is not exclusively aimed at conformity with certain legal requirements. Surveillance by the authorities is often the starting point of a process that leads to tracking down offenders and prosecution. IT (information technology) has become a major means for implementing all the stages in that process.

2.1 Camera surveillance in public and non-public places.

The use of audio-visual equipment (cameras) is closely connected to surveillance. Cameras allow real time surveillance as well as retroactive surveillance. It has been argued recently that it is the real time surveillance that makes cameras in public places particularly effective, as action can be taken directly once a situation appears on camera.

With respect to surveillance in real time, the role of IT in the process may not be immediately apparent: in principle what is involved here is a screen that must be monitored by a human supervisor. However, these days the video signal is often not recorded and broadcast in an analogue form but directly in a digital form. That opens up various new possibilities. These video images can be relayed more easily to differing locations. That is particularly the case if the camera has a network connection and can communicate via the Internet protocol. These images could then, in principle, be accessed via any computer connected to the Internet.

The traditional way of looking at the images allows the supervisor to call upon the signals from various cameras or to project the images from those cameras next to each other on a screen. Digital image processing, however, is now also a possibility, allowing the computer to analysis and process the material at various levels. The following examples illustrate this technique (ranked, more or less, according to the complexity of the operations).

- Motion detection or similar techniques that make sure that only the recordings in which something has happened are shown or stored (for example, where there has been movement or sound).

⁴ C.f. O.S. Kerr, 'Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't', *Northwestern University Law Review*, Vol. 97, 2003, <http://ssrn.com/abstract=317501>.

- Increasing the sharpness and contrast of a recording, so that it is possible to zoom in on details (such as a number plate or a person's face).
- Facial recognition: identifying a person by recording that person's face. Great steps forward have now been made in the application and processing of this form of biometric information (this is dealt with in more detail below). The Dutch Committee on Criminality and Technology considered this application to be one of the 'most promising' techniques dealt with in its report. With this technique, it is already possible to identify someone in a crowd (although the person's face must, at a certain moment, be visible). The technique has not encountered much resistance, probably because recording someone's face is seen as less threatening and less intrusive than, for example, an iris scan. Experiments are already underway to use this technology for controlling entrances to offices, hospitals and even swimming pools (sometimes in combination with other techniques such as fingerprint scanning).
- Where cameras are positioned at more than one location, it becomes possible to track and trace people for a certain distance and over a certain period of time on the basis of facial recognition. This technology means it is possible to make a detailed analysis of where a given person is at any given time in the area covered by the cameras.
- Object pattern analysis: this system makes it possible to look at images where something out of the ordinary is considered to be taking place. This system makes it possible to track deviant behaviour, for example, where someone remains motionless at a particular location for a much longer period than average. The technique also makes it possible to isolate deviant patterns, for example cars or lorries that exhibit an unusual route pattern.
- The use of images from special satellites which have advanced cameras and sensory equipment making it possible to localize, identify and follow people or goods.

It is clear from the above examples that the 'traditional' form of camera surveillance, whereby analogue imaging is relayed via specific, separate infrastructure to a location where the pictures can be seen or recorded, has been overtaken by new forms of technology. In particular, the fact that digital cameras, based on Internet technology, do not need separate infrastructure or cables is a great advantage. It is, therefore, expected that this technique will supersede the analogue version in the years to come.

2.2 Surveillance of telecommunication

As well as extensive camera surveillance, the monitoring of all forms of telecommunication has also become large-scale. That monitoring applies not just to telephone and fax messages, but also, and increasingly, to data traffic on the Internet.

From a technical viewpoint, in most cases it no longer matters what sort of communication is involved; even speech can often be directly digitalized and then transmitted. This is, for example, the case with respect to mobile telecommunication via GSM, the omnipresent 'Global System for Mobile communication' used by almost all mobile phones. Another technique for directly digitalizing speech is VOIP, 'Voice Over IP'. In this case, the audio signal is converted into data packages, structured in such a way that they can be sent over the Internet. VOIP can be used between two computers connected to the Internet (both having audio hardware). Today, there is also specific equipment (in the form of conversion units and VOIP

telephones) that makes it possible to use this technique even without a computer. It is possible that this form of telecommunication will replace the traditional phone within a few years.

This makes it clear that there is little point in monitoring or tapping data on the basis of which type of communication is going to be the subject of the surveillance. It is usually not possible to distinguish these types before the data has been received and decoded. The decoding establishes, inter alia, what type of data is involved (digitalized speech or computer data etc). However, it is also quite likely that the sender of the data has sent them in an encrypted form. This is, in principle, very easy where digital data are involved. Trying to decrypt without the right key can be extremely difficult and time consuming, in particular when a so-called strong form of encryption has been used. Even the use of technology does not mean this problem can be easily solved. This is why authorities have considered placing encryption under legal regulation. In the Netherlands, an attempt was made to make the users of encryption provide the data for decryption where a criminal investigation was concerned. This provision never became law. Nor did the rule that encryption keys had to be deposited with 'Trusted Third Parties' (TTPs).

A specific form of surveillance, entailing the surveillance of people rather than of telephone or data traffic, allows people to be located, based on their mobile phone data. This information can be derived from one or more transmitters for mobile phones. It makes it possible to determine who was where (in the vicinity of one of these transmitters) at a certain time, at least if the mobile phone was on. This technique is now used regularly to follow a suspect. However, the use made of this data by the Rotterdam police to send sms messages to all those who had been in the vicinity of the football stadium at a certain time, was new, at least for the Netherlands. Of interest here is that the data of bystanders was used for the purposes of a criminal investigation, not just the data of those suspected of a criminal offence. In itself, this may not seem so spectacular, its effect was arguably no different from the traditional door to door police inquiry, but the scale of the application and the infringement of the privacy of those bystanders led to a heated discussion in the Netherlands.

For this sort of location data, as well as data traffic itself, it is obvious that the registration and storage of such data can be of great importance for retrospective monitoring. European law has already been introduced to make this possible. Nonetheless, its introduction has met resistance from providers and Internet user organisations, such as 'Bits of Freedom'.

2.3 Entry control; determining the identification of persons and goods

The time that entry would be granted to a person based on no more than an identification card, specifying the carrier's name and photograph, is drawing to an end. The traditional identification papers are simply too easy to copy. It is, therefore, not surprising that measures have been taken to make passports, driving licences and similar forms of identification more difficult to forge. The newest weapon against forgery is the use of digitalized biometric information as a means of identification.

Biometrics (literally 'measuring life') has quite a long history. The use of the finger and handprint for identification was known in China in the 14th century. In Europe, fingerprints have been used as a means of identification since the end of the 19th

century, based on a system developed by Richard Edward Henry of Scotland Yard.⁵ Fingers are not the only parts of the body, however, that can be used for identification purposes: hands, eyes (the iris and retina), the face, the voice and the DNA itself can be used. However, they all require specific technology. The certainty of identification they provide may vary. DNA is generally regarded as being the most accurate and reliable biometrical method. The disadvantage of using DNA for identification is that the process requires considerable time and cost, whereas an iris scan, a face scan or a fingerprint can be carried out quickly and cheaply. It is for these reasons, that the latter techniques are the ones used at entry points.

IT plays an important role in the use of biometric techniques. For example, the characteristics of a fingerprint are normally stored in the form of a so-called template. The accuracy with which that process takes place determines the dimensions of the template and also its reliability. The template can be stored in a memory chip which, for example, can be used in an identity card.

Not only persons, but also goods can be identified and traced. One traditional form is the traditional metal detector, for example a screening doorway at airports, which makes use of a magnetic field. Other techniques that are increasingly being used include MRI scans, microwave radar registration and microwave dielectrometrics, each of which are capable of detecting specific types of objects, for example in baggage. Explosives can be detected by, inter alia, 'Explosives Trace Detection' (ETD), a relatively cheap system in which traces of explosive materials are traced by way of samples, and by 'Explosive Detection Systems', which uses expensive automated scanners with x-ray capacity in order to analyse the content of packages and suitcases. Similar techniques are available to detect biological weapons.

All these techniques have in common that they make use of the existing characteristics of persons or goods. It is, however, possible to track a person or goods by means of a tagging system. With respect to goods, a good example of this form of tagging is the security barcode label that is now found on many products, which triggers an alarm once the exit has been passed. A similar application can be found in cars and scooters, enabling stolen items to be returned to their rightful owners. One technique that is of much interest at the moment is RFID, 'Radio Frequency Identification'. It functions in the same way as the security bar code, but it is so cheap and so small that it can be inserted during the manufacturing process of virtually any product. This technique could replace the barcodes as an effective means of preventing shoplifting. The privacy aspect of this development, as it is, in principle, possible to collect information unobtrusively about what products a person has, has led to much discussion.⁶

Finally, mention must be made of the GPS, the 'Global Positioning System'. Apart from being used for navigational purposes, this system can also detect the precise location of a person or a thing, for example a car. If this information is then passed on

⁵ See A. K. Jain, L. Hong, S. Pankanti & R. Bolle, 'An identity authentication system using fingerprints', *Proceedings of the IEEE* 85 (9) (1997) 1365-1388.

⁶ An extensive report about RFID that pays attention to technical aspects as well as privacy aspects is published by the US Government Accountability Office (GAO), *Information Security, Radio Frequency Identification Technology in the Federal Government*, WWW, <www.gao.gov/new.items/d05551.pdf>, read 12 October 2005.

to the police, for example via a GSM connection, it makes it much simpler to track down stolen goods. When this system is applied to persons in the form of an ankle tag, new possibilities for electronic house arrest arise.

2.4 Surveillance techniques for detection and prosecution of crimes

Many of the techniques described above are suitable not just for the purposes of crime prevention, but also for detection and prosecution when a crime has been committed. For example, cameras can be used for face recognition, data from data exchanges and location data can be stored by computer and biometric methods can be used. Such techniques affect criminal procedure; evidence obtained through the use of highly advanced technology⁷ must comply to the same standards of validity and reliability as evidence obtained in a more traditional way, for example by witness statements. The use of new technology can cause problems for judges, whose lack of familiarity with the technology involved means they have to rely heavily upon the expert opinions of those behind the technology. It is of great importance to deal with this problem because the probability is that the use of evidence obtained by technology will increase rather than decrease.

2.5 Conclusions regarding surveillance technology

In the future, surveillance technology will make use of various techniques. Information in a digital form makes it possible to use techniques that were unknown only a short time ago. Equipment can be used not only for (passive) registration, but also for analysis and interpretation. One example of the combination of techniques can already be found in American airports: video cameras utilising image recognition software used in combination with pre-existing information. This method is also used to deal with hooligans at football matches, rather than checking their individual club cards. Surveillance technology also includes fingerprint and DNA techniques. These methods are not only used for active control, for example to gain access to restricted areas, but also retroactively to reconstruct a given situation. Digital technology is also responsible for the increasing use of biometric techniques.

Surveillance technology has, without doubt, made an impact on society. *Technological advances*, in general, have been considerable over the last 150 years. It is a period that has seen the Industrial Revolution superseded by the Information Revolution. Technological applications are numerous and various, and have become integral to the society we know today. That technology should be used for surveillance is, in this context, not extraordinary. Indeed, its application is rather obvious given that the techniques are easily applied to surveillance and that society as a whole has acquired a more technically orientated character.

What perhaps is less obvious, is that technology offers diverse possibilities with respect to complex relations. *Management* is of vital importance in carrying out tasks, whether those tasks are related to business or public sector organisations. Technology can assist in planning, control and communication.

It has also affected people at an individual level. That there are more and more options open to people, and more and more information, makes it necessary for

⁷ For background information about the use of DNA profiles, see B. Budowle, G. Carmody, R. Chakraborty & K.L. Monson, 'Source attribution of a forensic DNA profile', in: *Forensic Science Communications*, July 2000, ISSN 1528-8005.

people to approach decision-making *rationally*. Increasing wealth and economic independence have prompted a process of individualisation. Traditional social structures have become less a matter of course, indeed they are sometimes experienced as obstacles in the way of reaching individual goals. The rational model of man is arguably now the best predictor of human behaviour.⁸

These aspects are partly responsible for, or augment, the tendencies listed below:

Globalisation

Technology has increased mobility and thereby accelerated the process of globalisation. Not only can people travel more quickly from place to place, but communication has become much easier and faster with the advent of Internet and the mobile phone. The world order as we have known it is changing and that makes directing, controlling, enforcing traditional norms or obtaining an overview of society in general more difficult. Change brings uncertainties with it.

Resistance

The use of technology has become commonplace. It is, therefore, nothing out of the ordinary that technology has been used for various forms of surveillance and for the enforcement of established legal aims. Nonetheless, the implementation of new technology invariably leads to public resistance. In the time of the Industrial Revolution, it was argued that the working man would see his livelihood taken away from him by a machine and that poverty would be his lot. An updated version of this fear was voiced with respect to the Information Revolution: there would be massive unemployment because office workers would become superfluous. In both cases, although some forms of traditional work did fade, new work replaced it. The Industrial Revolution took people out of the fields and put them in factories. The Information Revolution took people from filing cabinets and put them at the computer. In both cases, women became an increasingly important part of the salaried workforce. The general level of welfare in the technically progressive West has never been so high. Yet despite a certain level of public familiarity with technological applications, surveillance technology has met with some public resistance. It is, however, very likely that that resistance will be overcome. Surveys already indicate that members of the public feel safer where there are cameras, for example in shopping centres.

Easy use for all

There are many useful applications for technology and technology is becoming increasingly accessible to the public. Simplicity of use, smaller sizes and lower prices have meant that the kind of equipment once only found in a professional setting has now become a consumer product. There is, however, a darker side to this development. It has become much easier for individuals, even those without much technical knowledge, to use modern technology for the purposes of terrorism or other criminal activities. The potential harm they can cause is huge. Businesses can be seriously undermined by computer viruses. Members of the public can be the victims of terrorist attacks on public transport. Public facilities in general form other potential targets, such as the energy supply or drinking water. The use of surveillance technology must be seen against this background; technology is used to combat the harmful use of other forms of technology.

⁸ See note 3.

Changing norms

The most important factor in the implementation of new technology is the expected level of efficiency and effectiveness. The use of technology depends on what it can achieve and how much it costs. Less obvious perhaps is that it is also responsible for a shift in norms. Technology has made things possible that were once not possible; this ranges from copying films from the Internet at home to interactive television to in vitro fertilisation. New technology has made existing norms less self-evident; indeed some norms seem to change with the times. A person who would not dream of going to a cinema without paying for a ticket, could easily be prepared to download a new film at home.

If the technology is available, it is not difficult to predict that it will be used for surveillance and detection, geared up to the needs of the day. This shifting in norms also applies to the use of technology for surveillance, detection and law enforcement. It affects those who introduce the technology as well as those who are against it. Those working in the public sector not infrequently show a rather creative approach, which does not always conform to the demand for legitimate administration. Although the 'creativity' of public officials must be monitored, it would not be efficient to require a change in the law before new applications of existing technology can be implemented. The police and the judiciary would then be constantly one step behind. It is, however, necessary to evaluate the law in order to determine whether the creative use of technology falls within existing legal parameters or whether new laws are necessary to legitimise its use.

3. Legal considerations

This article will focus on five problem areas. These areas include the invasion of personal privacy, the use of surveillance technology by the authorities with respect to criminal law, surveillance technology as a means of social control, whether surveillance technology leads to a better use of resources, and the principles of proportionality and subsidiarity.

3.1 Privacy versus safety?

One opinion that is often voiced is that people find it unpleasant to be spied on and to know that their movements can be checked out later. However, when members of the public are asked if they would like to see more uniformed policemen on the street, the vast majority answer in the affirmative; most people apparently find a police presence on the streets reassuring. Is it, then, a question of finding the right balance: yes to surveillance in itself but no to surveillance in an extreme form? If that is the case, it implies a remarkable conclusion; that we actually want a certain level of uncertainty. Research has shown that the public judges risk not just in terms of the chance of something happening or the effect of that something happening. That other considerations play a role comes to the fore where behaviour in traffic or smoking habits are concerned.

With respect to the relationship between privacy and safety, the question seems to be how much of our privacy are we prepared to surrender in order to increase our safety? These two basic rights, the right to privacy and the right to protection, seem to be uneasy partners. However, the question itself is not as straightforward as it may seem. Why is it that most of us are perfectly prepared to have our baggage examined in airports but resent our past being looked into? Privacy is not a clear concept; the term

includes various aspects of private life. It may encompass various dimensions, such as the spatial dimension. This spatial dimension is concerned with our freedom of movement: if there were no controls at airports would we feel freer or less free to go as we pleased? And if our past is looked into, would the examination of our baggage no longer be necessary? Privacy and safety do not have to be opposites, but the one can affect the other. It would be hard to think of something that was a greater infringement of a person's privacy than having to undergo a body search, or having personal belongings searched, or even the threat of it.

Constitutional rights have a special place in the relationship between the authorities and members of the public. Rights and freedoms are formulated that are intended to protect citizens against the arbitrary use of power by the authorities. In the course of time, the concept of the horizontal working of constitutional rights has developed. The right to respect for personal privacy is not just between the authorities and the public, but also between members of the public themselves. In former times, it was necessary to protect citizens from the arbitrary behaviour of the authorities (or the monarch). Today, in the developed democratic states of the West, it would seem that the 'danger' emanates not so much from the authorities, which are open to public review, but from those who reject authority. Fear restricts the movements of citizens, either because they are not sure if it is safe to take an airplane or the local metro, or to voice a possibly controversial opinion. It would now appear that it is the authorities that have become the champion of constitutional rights, rather than the body which could be guilty of flouting them. The question now before us is which aspects of privacy must weigh heavier in a given situation? The means used will depend upon how that question is answered.

Another question that comes to the fore in determining whether someone's privacy has been infringed, is what criteria should be used. Where there is a choice or where there is an advantage to the person concerned, it is less likely that an infringement of privacy will be considered as unacceptable. In order to respect personal privacy it would seem more important to formulate these criteria rather than paying attention to actual forms of behaviour, as this does not sufficiently take into account the personal character of privacy.

However, the choice for applying surveillance technology, or being placed under such surveillance, is often not one made at an individual level. This runs counter to the present day tendency whereby the individual plays a central role. That is because the protection of privacy is not just an issue for individuals; it must also take collective needs into account. Paradoxically, it would seem that the 'protection' of constitutional rights justifies a certain selective infringement of those rights. This can be explained in terms of the relative utility of the application. To the extent that it affects individuals, legislators must be careful not to make unwarranted generalizations, as this could result in the public rejecting the use of technology. This would be a pity as research into such matters as the registration of DNA and the use of extensive databanks holding sensitive information, has shown that many people attach more importance to safety than to privacy.

3.2 Suspects and non-suspects

When it is contended that surveillance technology infringes personal privacy, one aspect that is brought to the fore is that surveillance technology does not differentiate

between people; the surveillance entails the monitoring of both suspects and non-suspects. This infringes the legal principle that coercive measures should only be used against those for whom there are reasonable grounds to suspect them of criminal activity.

Modern technology means that an innocent person's privacy can be infringed as a side effect of tracking a suspected person's movements. It is this, rather than the use of technology against the suspects themselves, that causes problems; those who are not considered to be suspects must also accept that they too are subjected to the coercive measures made possible by the application of this technology. This would seem contrary to the usual principle of criminal procedure that a person's status as 'suspect' must first be established (for example, that reasons for suspicion are first presented to a judge in order to obtain a search warrant before the premises of a suspect may be searched).

In the first place, it is not the case that the authorities, including the police and the judiciary, may only do what has been laid down in detail. To a certain extent they may, just like ordinary citizens, ask people questions, telephone people and send sms messages. These activities cannot be categorized as coercive measures, for citizens are free in deciding whether to answer or not, nor are such activities limited to 'suspects'. That people do not like to be spoken to by the police, that they could feel intimidated, means that the police must be careful in the way they approach the public, but there is no reason, and indeed it would not be desirable, to fetter their capacity to ask questions. This applies even where if a person refuses to answer the question, he could become a suspect, and as such the subject of coercive measures.

Nor does receiving an sms from the police mean that the recipient must be considered to be a suspect. During an investigation, the police need to contact people as potential witnesses. In the case of the sms messages sent after the football riots in Rotterdam, the sms messages were sent to ask whether anyone had seen anything of interest to the investigation. The police could have achieved the same result by carrying out a house to house check or have asked questions to all those attending the next football match in Rotterdam. The choice to send an sms would seem more attractive: only those people who were in the vicinity of the football stadium at the time of the riots were 'bothered' by the police, it is much less labour intensive to send a message than to send out police officers, an sms saves time and the costs of an sms are relatively low. An sms is also probably less intimidating than a personal encounter with the police.

Nor is it the case that the authorities may only exercise coercion against someone who is suspected of an offence. In many cases, the law lays down a general competence for a certain activity. For examples, returning an income tax form is compulsory and surveillance cameras may be used to detect speeding. Checking that drivers do not exceed the maximum speed limit does not make all road users 'suspect'. And a possible automation of the surveillance of income tax forms, which could include coupling this with data from other sources, is, in principle, not an extension of tax control. Making data available - coupling files - should take place in accordance with existing legal regulations. However, because computers have made it easier to compare data, this area might be subject to further legal regulation.

3.3 Technology and social control

The use of surveillance technology, as illustrated by the above example of tax supervision, does not always entail an extension of an existing competence. It is more often a means by which that existing competence becomes more effective and efficient. The simple fact that something is useful, or more useful than it used to be, leads in itself to a certain shift in norms. It is, however, important that it is borne in mind that technology is itself primarily a 'means'; it is a means to make possible those things people find useful. Surveillance technology is, in this sense, a tool to enforce norms, in the same way as the law itself is a tool to enforce norms.

When people go on holiday, they often ask their neighbours to keep an eye on the house. If someone hangs around the deserted house, the neighbours might ask whether they can 'be of help'. That a police car would drive past the house more often while they were gone would also be welcome. In former times, it was far more common for people to keep an eye on the behaviour of others. There are various reasons why that is less the case today. One reason is the tendency noted above for increased mobility and individualization. People are also aware that an intervention may not be without risk.

The social control and cohesion typical of society several decades ago no longer exist, at least not in that form. It is generally recognized that social control and social cohesion have a useful function. The gap left by the lack of social control can be filled by the use of technology; it can give social control and social cohesion form once again. In any evaluation of surveillance technology, factors to be taken into account are not only the costs and disadvantages, but also what it contributes and its social advantages.

3.4 Technology and solidarity

Whether a decision is made to use surveillance technology seems to be largely a matter of efficiency. Efficiency is a norm more often associated with the private sector, yet this consideration is relevant with respect to the public sector as well. Although it would seem that efficiency as a norm has achieved greater acceptance in the private sector than the public sector, it is not the case that the aim of efficiency is without criticism in the private sector, for example with respect to commercial profit at the cost of service. When this criticism is analysed, it would appear that the services sacrificed are those that were not sufficiently profitable or provided at a loss. What the private and public sectors share is that those individuals who are affected want a result that suits them, even if it is disadvantageous for others, although they are not personally willing to contribute more. This leads to a conservative approach. Efficiency as a criterion is nevertheless an important guarantee of solidarity. The use of technology can promote efficiency.

An important question is to what extent people will be prepared to contribute financially to an expensive system of redistribution, in which not all those who are intended to benefit from the redistribution do so, and some of those who do benefit were not intended to do so. Many of the organizations charged with the task of redistribution are founded on the principle of solidarity. This solidarity could be in the form of unemployment benefits, insurance, housing or social security benefits, contribution to church funds, or charitable organizations. An important factor here is the tendency pointed out above; the increasing complexity of society, increased

mobility and individualization. As a consequence, it has become more difficult to reach those who have the right to such assistance, and more difficult to prevent fraud by those who do not have the right to this assistance. This puts solidarity under pressure and makes it crumble away. Surveillance and control could be made more efficient by using technology, for example to prevent the fraudulent use of social security systems, and indeed its use could be demanded.

In practice, it is no longer possible to implement complex legal projects without the use of technology. Technology has, in turn, influenced the content of these legal rules, as the automation process itself may impose certain requirements and restrictions. Creating and keeping consensus depends on correct implementation, certainly in the long term. Using technology as a means of control or as a means to support the enforcement of control, could give those involved a greater feeling of certainty. It is because we have computers that we can refine general rules, so that relevant individual circumstances can be taken into account. It is this very ability to distinguish between cases that makes it possible to uphold the principle of equality. In this way, technology could contribute to a feeling of solidarity.

3.5 Subsidiarity and proportionality

The use of surveillance technology cannot, in general, be seen as irreconcilable with the right to the protection of personal privacy. Safety is not in opposition to privacy, but an aspect of it. Furthermore, it could be argued that the right to personal privacy is not an absolute right; other factors can, and sometimes must be, taken into account. Thirdly, it has already been pointed out that the scope of the concept of privacy, and its interpretation, must be seen against a background of technical and social developments.

Similarly, it has been argued that a general application of surveillance technology does not have to be contrary to the principle of criminal procedure that there should be reasonable grounds to see the subject as a suspect. That is because surveillance technology is not in itself a coercive measure. Surveillance technology is a means that is not confined to use for the purposes of criminal procedure. A person may cooperate, for example at a check-point, without having first to be identified as a suspect.

There are also positive effects, such as the use of technology to increase the usefulness of services to the public and to respect the enforcement of basic rights.

It is often not necessary to change the law in order to implement surveillance technology. Technology can already be implemented within the existing legal context. However, the use of technology, either in general or for particular forms of surveillance, can lead to shifts in norms.

With respect to surveillance technology, just as with other means, attention should be paid to the legal issues that may arise from one situation to another. The boundaries for legal application are usually determined by the principles of subsidiarity and proportionality. In the example of the sms messages sent by the Rotterdam police, it can be argued, without trivializing the potential threat this could form, that this application stayed within accepted limits. Another example is the experiment with camera surveillance last year in the centre of Groningen, a city in the north of the Netherlands. These cameras did not operate continuously, but were triggered when the microphones that were attached to the cameras picked up sound. Although it could

be said that the surveillance was continual, nonetheless the system was only activated if there was a reason: the sound registered by the microphones. This is a good example of proportionality; modern technology made it possible to limit the infringement of privacy.

In setting down legal conditions for use, it should be realized that a too conservative approach could unfairly favourable the criminals. While acknowledging that there should be reasonable grounds before someone is considered to be a suspect, it should also be borne in mind that it is increasingly the case that the threat could come from an unknown source, as is often the case with terrorist threats. What should be taken into account is that surveillance technology does not only have to be seen as a means of repression: it is also a means of prevention. It gives a high quality service and is cost effective (for consumer and tax payer). It is possible to organise the surveillance in such a way that not all the information need be made known. It is sometimes sufficient that it can be made known. To use the example of the Rotterdam police once again, it would seem that no names or addresses were made available but only the telephone numbers. Much work is taking place in the field of so-called privacy enhancing technology (PET) and techniques to ensure anonymity. It is, of course, necessary to consider safety precautions, any loss of data and possible claims by those affected by a loss of data, misuse of data or use that causes damage. In general, it would seem wise to make the legal framework known on the introduction of the technology.

4. Conclusions

In part, the objections to surveillance technology arise when people are the objects of that surveillance: we do not mind if others are subject to surveillance, but we do not want to be the subject of that surveillance ourselves. If we see ourselves as honourable citizens, for whom surveillance is an unnecessary restriction on our privacy, there is indeed room for indignation. Not only is such surveillance unnecessary, it is straightforwardly insulting, as it implies we too are suspected of criminal behaviour. Nonetheless, the public appears to benefit from surveillance by the authorities. Most of the criticism emanates from lawyers and institutions, such as Amnesty International, Liberty, socialist political parties and law faculties. Given the rational model of man, it is quite easy to explain why the objections come from this direction: it is in the self-interest of these groups to protest (which is not the same as saying that their interest is a selfish one).

Furthermore, it would seem that resistance is a characteristic of the assimilation process of new technology. It is resistance to technology and resistance to change. Not knowing whether there is surveillance, what the scope of that surveillance is, who is carrying out the surveillance and what will be done with the data can make people feel uncomfortable. It is rather like the situation of 'I can't see you, but you can see me'. Without transparency with respect to these issues, it is quite possible that people feel more vulnerable rather than less. That would inhibit the assimilation process, which would be a pity given how important it is that the usefulness of this technology is acknowledged; one conclusion that is rarely seen in legal literature is that technology, also surveillance technology, actually makes it easier to respect and protect basic rights.

A good example of how the authorities can use new technology is the questioning of potential witnesses on the basis of their locations revealed by their mobile phones. Another example of how authorities can use technology to deal with new, and partly unknown, threats is to keep data from networks for a certain period with the help of internet or telephone providers. These examples show how new technology can be used for the more effective enforcement of existing norms. However, there is a clear possibility of the infringement of rights such as the freedom of information privacy rights. That the norms will adjust is a logical consequence of the technological developments. An important criterion is whether it works; the effectiveness must be tested.

Five points to be taken into account were presented above. The points were 'privacy and safety', the importance of the presence of a 'suspect', 'technology and social control', 'technology and solidarity' and 'cost effectiveness'. The conclusion has to be that surveillance technology leads to a new consideration of values and interests.

The right to privacy – and other rights that have arisen from technological and social developments like copyright- are ripe for review. The automatic reaction of support for these rights is no longer adequate. The right to privacy is no longer just under pressure with respect to the concerns for safety, but also in its relationship with other rights, such as the freedom of information and there are even conflicts within the right to privacy itself. Often the privacy of one person means the infringement of the privacy of another person.

There is a steady, and growing, market for gossip publications; apparently people are quite happy to read privacy sensitive stories about others. Perhaps an even more important consideration than the dichotomy privacy/safety is that between privacy and the right to information. Where more weight is given to privacy than the right to information, the current trend for weblogs could be made impossible. A redirection concerning privacy is also in order for claims to privacy regarding a change of gender and age, for example. Limiting constitutional rights, or reassessing them, means that it is desirable to put into place an effective control on the power of the authorities. Those who object to surveillance technology not only point out the dangers to individual rights and the costs, but in particular the danger of misuse by the authorities.

Technology not only makes surveillance a more practical matter; in a more complex way it leads to a new organization of state power. This is possibly the most important point of discussion with respect to legal and social change as a response to technological progress. De Mulder⁹ argues that a new fourth power is inevitable; just as the appearance of an executive power was inevitable once the law could not only be written but also printed. That development led to the large-scale bureaucracies we seen today. The technical possibilities offered by computers and the Internet will not be less far-reaching. The appearance of a new power, a monitoring power, would seem likely. We have already witnessed this development in the form of such institutions as the Ombudsman, the National Audit Office and the National Competition Authority.

⁹ Mulder, R.V. De, 'The Digital Revolution: From Trias to Tetras Politica', in: Snellen, I.Th.M. , Donk, W.B.H.J. van de (Eds.), in: *Public Administration in an Information Age. A Handbook*, p 47-56, Amsterdam: IOS Press 1998, ISBN: 90 5199 395 1.

This new power, the result of social change, will have far-reaching consequences for the law, and for the functioning of the state of law and the legal profession. The growth of the executive power led to large-scale bureaucracies. Bureaucracies may be of use, but can easily lead to excesses. The systematic monitoring of those in charge of the use of surveillance technology in a democratic state is a necessity. In a globalizing and increasingly technological world democracies will need monitoring powers to supervise the use of surveillance techniques.