SEVENTH FRAMEWORK
PROGRAMME

FP7-SEC-2011-284725

SURVEILLE

Surveillance: Ethical Issues, Legal Limitations, and Efficiency
Collaborative Project

SURVEILLE Deliverable 2.3: Paper by local authorities end-users

Due date of deliverable: 28.02.2013

Actual submission date: 28.02.2013

Start date of project: 1.2.2012 Duration: 39 months

SURVEILLE Work Package number and lead: WP02 Prof. Tom Sorell

Author(s): Sebastian Sperber, Maye Seck, Elizabeth Johnston

SURVEILLE: Project co-funded by the European Commission within the Seventh Framework Programme		
Dissemination Level		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

1. Local authorities and research on surveillance technologies

1.1 Why discuss efficiency and ethics with European cities?

In recent years, security has become an increasingly critical political and social issue. Not only crime but also fear of crime is a fundamental concern for people in most European countries (Efus 2006b). Cities, which are still growing rapidly, are at the centre of these developments. According to the Massachusetts Institute of Technology (MIT), 90% of population growth, 80% of wealth creation and 60% of energy consumption will occur in the future in cities[1]. Crime also concentrates in cities, where the crime rate per person is higher than in rural areas (Efus 2006b). Security and the perception of security are therefore key issues for towns and cities in Europe.

Mayors and locally elected officials in general are first in line to have to deal with issues of insecurity. The citizens of their towns and cities expect that they address their security problems. Since crime occurs at the local level, it is at this level where the situation and its context are best known, and where it is efficient to develop and implement security strategies (Efus 2004). As developed in the UN Crime Prevention Guidelines, in order to take into account the multiple and complex causes of crime and different responsibilities, cooperation and partnership are key (UN Economic and Social Council 2002). Local communities often hold several levers for action: social policy, youth and educational policy, public policy, land use and urban planning, etc. Thanks to the democratic legitimacy of elected officials, they can assume the public leadership advocated by UN Guidelines, a role particularly emphasised by the UN Safer cities programme, which stresses the "key role of local authorities" (UNHabitat 2007: Safer Cities, p. 4.). In many European countries and throughout the world, municipal authorities have become central actors with regard to urban security, and work closely in partnerships with other stakeholders such as the police, the criminal justice system, but also representatives of civil society. In many countries local authorities control local security partnerships.

It is in this context that local authorities have taken charge of the instruments of security and surveillance technologies. Whether in public, semi-public or private spaces accessible to the public or on public transport, cameras are part of the reality of cities. Despite the differences from one country to another, and between the laws governing its use, in the last twenty years the use of CCTV in European cities has become much more frequent.

[1] MIT City Science http://cities.media.mit.edu/

Local communities have become users of these surveillance technologies. As Töpfer stated (2010, 86) "Across Europe, the true driver of development (the use of CCTV) is found at the local level. Civil servants, local politicians and the police support or hinder the development of video surveillance according to their opinions, interests and intentions." The issue of the effectiveness and ethics of surveillance technologies, which the SURVEILLE project addresses, are also of utmost concern to local authorities.

Does it work? As cities are responsible for ensuring the security and tranquillity of their inhabitants and preventing crime, they must question the relevance and effectiveness of the various instruments and methods at their disposal. They need information on the effectiveness of surveillance technologies, their strengths and weaknesses, as well as the conditions that allow for good performance and correct use of these instruments. The issue of efficiency is particularly important in view of the costs and ethical issues related to the use of surveillance technologies.

Is it worth it? Particularly in the context of economic crisis, empty public accounts and the need to make savings in most European countries, the issue of the cost-effectiveness of instruments is crucial. New technologies enable many increases in efficiency and productivity in many areas. Is this also the case in crime prevention? At the same time, investment and operating costs are often very high. Cities require information in order to make informed decisions about the right investments for urban security.

Can it be justified? Surveillance technologies are instruments that need to be singled out because they raise ethical issues of which local and regional officials are acutely aware. Current uses of CCTV, for example, tend to encroach on individual privacy rights (see Goold 2010, 34). These ethical issues have to be taken into account in the trade-off to use or not to use the technology.

How can the use of security technologies and protection of privacy be reconciled? This is why many cities conduct debates on ethical issues and implement safeguards in the use of these technologies. They are very interested in ethical issues related to the use of surveillance technologies and in particular solutions that strike a balance between security and respect for privacy.

All of these factors show how important it is that local authorities participate in the SURVEILLE research project, through the European Forum for Urban Security (Efus). Efus is a network of municipal and regional authorities that work together on urban security issues and is also responsible for organising, for its members, exchanges between policy makers and local practitioners in contact with the world of research. End-users of some of these surveillance technologies are in direct contact with the research that attempts to find precise answers to their questions. The results of this research are disseminated among local users of technologies in Europe and are applied directly in the field.

This exchange is reciprocal: European municipal authorities not only benefit from this cooperation, they can also directly participate in research by contributing their experiences, the know-how they have acquired in the use of technology and their perspective on issues, as explained in this report. Exchanges with municipal authorities that use technologies at the local level can be carried out on two levels:

Firstly, on a technical level: Information on technical requirements, experiences with the use of different technologies in a real-life environment, taking into account the human factor, the integration of technologies into routines and procedures, etc.

Secondly, with respect to the political economy of using these technologies at the local level: Why are these technologies used? What factors should be taken into account when using them at the local level? How are these technologies perceived by experts in the field, policymakers and citizens?

One could object that local authorities do not have the same role as the police or intelligence services and that it is therefore less important for the SURVEILLE project to talk with them about the use of surveillance technology. It is true that the role of local authorities is different from that of the police, and that municipal authorities concentrate primarily on public order and prevention of crime and violence. Therefore, they also do not have access to certain surveillance technologies.

It makes sense to take their feedback into account: firstly, their use of surveillance technology already represents today a significant part of the reality of surveillance. It is likely to grow even more in the future with an increasing amount of technologies initially developed for other purposes that can be used by local authorities for their missions. Secondly, the ethical issues arising from the use of surveillance technologies for the prevention and prosecution of serious crimes are certainly also valid for less important applications. Conversely, issues of ethics and effectiveness that arise in the use of surveillance technologies by municipal authorities will automatically be of relevance for more advanced and intrusive applications.

In certain countries, municipal authorities have a certain number of police competences. In most cases, the local police operating under the authority of the mayor enforce local administrative powers. In Belgium, the police services themselves are primarily local and under the authority of the mayor (or a "Collège de police" that gathers several mayors) (see for example Efus 2004, Efus 2006b).

1.2 The first contribution of local authorities

This report is the first contribution by local authorities to the analysis of surveillance technologies. Its primary objective is to provide a description and an overview of the use of technology by local authorities in European cities. It contributes to the creation of categories of technologies, which will then create a framework for the evaluation of these technologies (WP2). The second objective is to contribute to the analysis of the effectiveness of surveillance technologies (WP3) and to the debate on ethical and legal issues, how these technologies are perceived and their compatibility with fundamental rights (WP4). The work is therefore structured in two parts.

This report is a first contribution based on the knowledge that the European Forum for Urban Security has accumulated on these issues and is currently developing, thanks to the SURVEILLE project, with a new working group gathering European cities and regions. It will be supplemented by a second contribution based on a survey of the work currently being conducted in European cities, as well as other *ad hoc* contributions that the consortium partners will request from the Forum and its working group.

The European Forum for Urban Security (Efus) is a network of more than 250 local and regional authorities from 18 countries working together on all issues of urban security. Created 25 years ago by European Mayors under the auspices of what later became the Congress of the Council of Europe, Efus facilitates the exchange of ideas, knowledge and best practices on issues of crime prevention. In particular, it facilitates exchange throughout Europe both at the political and technical level. Efus is also responsible, for its members, for organising exchanges between policy makers / local practitioners and the world of research, as well as with European and international organisations.

Within this context Efus brought together knowledge and experiences on surveillance technologies, which led to an invitation to participate in the SURVEILLE research project, which is based in particular on the following:

- Founded under the auspices of the Council of Europe, members of the European Forum share an approach to security based on the respect of fundamental rights. The issue of access to rights and the relationship between security and freedom has therefore been a central issue for the Forum since its inception.
- In the 2006 Manifesto of Saragossa, member cities of the European Forum explicitly address the issue of the use of technology vs civil liberties.
- From 2009 to 2010, 13 cities and European police services worked together in the European project "Citizens, Cities and Video Surveillance" co-funded by the European Commission. They created a *Charter for the responsible and democratic use of video surveillance* in European cities (Efus 2010a) and a publication on these issues (Efus 2010b).
- To continue this work and disseminate the Charter, Efus launched in 2010 an initiative for the democratic and responsible use of CCTV with, in particular, activities in the Czech Republic, Poland and Serbia in 2010 and 2011.
- In November 2010, Efus' Executive Committee adopted a resolution on the use of CCTV (Efus 2010c).
- Efus participates in the SURVEILLE project and expands its work, which up until then was mainly focused on video surveillance, to security technologies and surveillance in general.
- In the framework of the SURVEILLE project, Efus' Executive Committee decided in March 2012 to create a new working group on European cities and regional issues in the use of security and surveillance technologies. It is intended to pursue the Forum's work on this subject and in particular to be the representative of the SURVEILLE project. The first meeting of prospective members was held in May 2012 in Brussels during Efus' General Assembly.
- 17.10.2012: First meeting of the Working Group with a discussion on the issues that would be addressed in the Efus SURVEILLE project; work began on a questionnaire to deepen and broaden this discussion.
- The group includes the cities of Brno (Czech Republic), Brussels (Belgium), Le Havre (France), Lisbon (Portugal), Paris (France), Rotterdam (Netherlands), Sosnowiec (Poland), Saint-Herblain (France) and Soisy-sous-Montmorency (France) as well as the region of Emilia Romagna (Italy) and the Autonomous Community of Catalonia (Spain). The cities of Munich (Germany) and the Belgian and Czech Ministries of the Interior are associate members.
- 13.12.2013: Thematic session on the use of technology, organised in cooperation with the SURVEILLE project, within the international conference "Security, Democracy and Cities: The Future of Prevention". This international conference

brought together 900 participants from a broad range of sectors, and 40 different countries, in December 2012.

- 14 December 2012: Adoption of a new cities manifesto "Security, Democracy and Cities" with a position taken on the responsible use of surveillance technologies, based particularly on early work for the SURVEILLE project.
- In total, within the framework of the Initiative for a responsible and democratic use of CCTV and the SURVEILLE Working Group, Efus has had direct exchange with 28 cities in 11 European countries regarding their system and CCTV projects: Liege, Brussels (Belgium), Le Havre, Saint-Herblain, Lyon, Toulouse, Bordeaux, Paris, Echirolles, CAVAM (France), Emilia Romagna, Genoa, Veneto (Italy), Ibiza, Generalitat de Catalunya (Spain), Sussex Police, Metropolitan Police Service (UK) Brno (Czech Republic), Budapest (Hungary), Dobrich (Bulgaria), Lisbon, Matosinhos (Portugal), Mannheim, Munich (Germany), Solin (Croatia) Sosnowiec (Poland), Leskovac (Serbia).

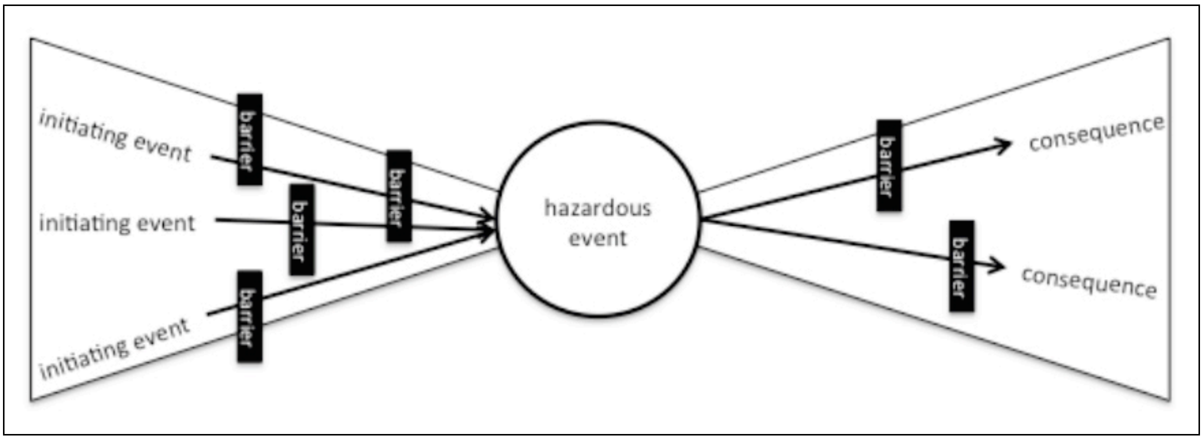
The report is based on this knowledge created primarily with members of the Forum. Forum members include cities and regions but also local communities such as agglomerations or French "departments". As most of the members are cities, the terms towns and local authorities are used as synonyms.

Surveillance technologies are the focal point of the SURVEILLE project. As can be seen in the taxonomy used (see 1.1.2), we consider "security" technologies to go beyond surveillance, and to include detection systems and alarms. This slightly broader definition lends itself to new information technologies, which are increasingly common.

2. The use of technologies

What is the actual use of security and surveillance technologies in European cities? What are the motivations to use them and for which purposes are they used? Who actually uses them? What are the trends in the use of technologies? What technological progress are cities hoping for, in order to address new challenges?

To structure this analysis, SURVEILLE partner TU Delft proposes in D2.1 to make use of the bow tie model, in which technologies are situated in the context of their application around a given incident. This model has the advantage of situating technologies in the context of their use, which can be very helpful to subsequently create a taxonomy of technologies. As can been seen in the graphic below, technologies are represented in the model in their function as barriers to prevent (left side) or to contain the effects of an incident (right side).



Bow-Tie Model according to TU Delft

Using the model in a context, in which technologies are used for various purposes, that is as different barriers, and in which there are different technologies that can represent a particular barrier, also shows the limits of the model. In order to create an overview of the technologies in use, it might be more promising to first simply discuss a list of existing technologies. Such a catalogue also presents the advantage of providing a complete overview of existing technologies. This will also allow potential end-users such as local authorities to get acquainted with new technologies and technology developments they do not know. Therefore this report uses a very straightforward list of technologies, based on the list and categories proposed by TU Delft. Efus's second report will use this first overview to contribute to the creation of a taxonomy.

In the city, or by the city?

SURVEILLE is primarily interested by the use of security and surveillance technologies by local authorities. However, it appears necessary to take into account the use of these technologies by other actors, in order to reflect the reality *in* European cities. For example, video surveillance of semi-public places or private spaces open to the public, such as stadiums, shopping centres, public transport (stations and vehicles), shops, public buildings, etc., is often not carried out directly by local authorities, but by other actors, including private companies or national authorities. Nevertheless, these cameras are sometimes of concern to local authorities. Even though this is outside of their area of competence, local authorities can engage in a dialogue with relevant stakeholders on the use of these technologies, especially when they are partners. For example, there are almost no public area CCTV systems in Germany. Its second largest city, Munich, is no exception and does not use any public area CCTV. However, its public transport system uses a video surveillance system composed of 5,500 cameras, which partially uses video content analyses (VCA). It seems all the more interesting to take this reality of surveillance in cities into account as there is a tendency to integrate private cameras into the public system (see below). Moreover, given also that private actors have an increasing number of surveillance tools at their disposal, it would seem unnecessarily restrictive to take only into account surveillance *by* cities and not *in* cities.

2.1 Technologies used in European cities

2.1.1 CCTV

CCTV is by far the most widely used surveillance technology among local authorities in Europe. There are millions of cameras and public area CCTV schemes in thousands of municipalities. According to various estimates, there are 60,000 cameras in the city of London alone (Efus 2010b : 192). For the United Kingdom as a whole estimates go up to 4 million cameras (all cameras included). Between 1999 and 2003 alone, the British government financed 680 CCTV projects (Squires 2010: 37). In France, 396,000 cameras were counted in 2007, 20,000 of which used to survey the public space (Gautier 2010: 176). The Sarkozy administration aimed at increasing this number to 60,000 public area cameras. The new “video protection plan for Paris”, the public area CCTV system of Paris, running since December 2011, uses 1,105 cameras and can access another 10,000 cameras of partners, in particular those of the public transport systems (Préfecture de Police 2011 : 12). In the Netherlands, a fifth of the 443 local authorities have set up public area CCTV systems with 4,000 cameras (Dekker 2007: 4). And hundreds of towns and cities use public area CCTV in Italy (Töpfer 2010: 76). These examples indicate that ***CCTV is the surveillance technology of choice for local authorities.***

Even though there is a strong trend indicating an increased used of this technology over the last 20 years in European cities (see for example Goold 2010, Töpfer 2010), there are important differences between countries. As Töpfer and Hempel have shown in the Urban Eye Project video surveillance in Europe, in some countries, local authorities use very often CCTV and at a relative large scale, whereas in other, only a few cities have set up public area CCTV systems and only at a small scale. The UK is certainly world champion in the use of CCTV, but other countries such as France, the Netherlands, Belgium or central European countries are well equipped with cameras and/or are increasing the use of CCTV. In other countries such as Germany, Austria or Scandinavia, local authorities seem to make use only rarely of video surveillance. These differences in the use of CCTV reflect differences in the social acceptance of this technology and the general public's perception of issues of liberty and security, which are also influenced by historic experiences or events such as totalitarianism or terrorism. Public perception is also influenced by how CCTV is regulated, who supervises it, who is in charge, who else is involved, who pays and who controls it.

In the sample of 28 local and regional authorities of the European Forum for Urban Security, all but Munich use public area CCTV. (And as seen above, Munich also has a well-developed CCTV system in its public transport). Outside this sample, there are also a very significant proportion of local authorities within the European Forum (which generally do not participate in working groups on CCTV), which deliberately decide not to make use of surveillance technologies.

The number of cameras used by these 27 municipal and regional authorities varies significantly. There are CCTV systems of 4-20 cameras such as have been used in Ibiza and Mannheim (no longer in actual use), Saint-Herblain and Toulouse; of 20 to 80 cameras as in Bordeaux and Genoa; of around 100 cameras (80-150) in Liège and Le Havre; of several hundred (150-400) cameras in Brno, Bologna, Lyon, Rotterdam, Sussex; whereas the largest systems (with 1,000 or more cameras) are in Paris, Veneto and London. Of course, the number of cameras also depends on the size of the city or the region, but the examples given above indicate that size alone cannot explain these differences.

The extent to which CCTV is used also very much depends on the approach chosen. Some cities want in some areas to complement an essentially human-based control by adding a number of cameras. Others aim at a larger scale surveillance of their territory. These differences in the use of CCTV in Europe show that the decision on whether to make use of surveillance technologies remains a political decision also in times of significant technological progress (Töpfer 2010). There is no evidence that local security policies and strategies require surveillance technologies. Indeed, surveillance technologies are not considered an imperative necessity for all security policies.

With respect to the actual ***technologies employed***, local authorities have changed to digital CCTV technology since the 2000s. Those who already had analogue systems in use upgraded to digital. (The only exception might be the camera optics, which has still remained analogue in several cases). All in all, the trend is towards digital and IP cameras, which allow high resolution while reducing the necessary bandwidth through video compression technologies.

New systems are generally set up as digital systems. An average local authority public area CCTV system today consists of PTZ cameras (pan, tilt, zoom) and/or dome cameras (that provide a panorama of 360°) linked to a digital video recorder. Operators monitor the system 24/7.

Fibre optic cabling is usually used for data transmission, sometimes completed by radio bridges. In the CCTV systems represented in the Efus working group, the Internet is currently not considered an option for data transmission for security and quality reasons. In many cases, local authorities own the optic fibre networks or have used the opportunity to invest into optic fibres (ideally in the context of other road works) that they could then rent to other service providers. In other cases, local authorities rent these networks from telecommunication companies. The issue of data transmission and its cost lead local authorities to favour wireless solutions.

As a ***general trend*** after digitalisation, it can be observed that local authority end users tend to link up different – previously distinctive – CCTV systems to large video surveillance networks. More generally, they tend to bring together different sources of information in the command and control rooms. Made possible by digitisation and important efforts to standardise the protocols of local users, the creation of surveillance networks is a logical step to optimise the use of already installed cameras. It is a priori difficult to explain to taxpayers why there are two distinct CCTV systems without any interconnections used by different police services in the same city - if it is not a measure to protect privacy. Moreover, as seen before, even towns and cities that do not run a public area CCTV scheme might be full of cameras or even CCTV systems run by public transport authorities, shopping centres, leisure centres, etc. It seems rather straightforward to build on the existing and to integrate the potential that these already installed cameras provide into the CCTV system of a municipal authority. This is particularly obvious in the case of linking up CCTV that is operated in different neighbourhoods or boroughs.

The forerunner in this trend is again the United Kingdom. The Metropolitan Police Service of London has undertaken important efforts over the years to connect local authorities' CCTV systems of different boroughs with CCTV systems and cameras of other operators into a large video surveillance network. Amongst the 12,000 cameras that it can access today, only 500 are actually owned by the Met[2]. A state of the art CCTV system, such as the one functioning in Paris since 2012, has a similar structure. It is a large polycentric network

[2] See: Project "Citizen, Cities and Video surveillance" - minutes of the visit of the project partners of the Metropolitan Police Service, 23-25 September 2009, www.cctvcharter.eu

that links in real time camera images from various source, in particular the city of Paris, the national police, the Paris public transport authority, the national railway, and others, to several CCTV control rooms. Each network partner as well as each level in the command structure of the national police, which supervises the system, have different access and priority rights to different cameras and parts of the network. This development allows CCTV systems in European cities to increase their scale and performance.

What are these CCTV systems used for?

- Since its inception, CCTV has been used to monitor and manage road traffic.
- A key application of CCTV for local authorities is monitoring public space with the goal of preventing crime.
- CCTV is also used by local authorities to protect public buildings, installations and car parks.
- For police services, CCTV is also a tool to better manage its forces, but also to supervise interventions.
- CCTV also takes on a particular role for local authorities in securing and managing large events, such as sports or cultural events but also demonstrations
- After 9/11, video surveillance has been increasingly justified and used as an investigative tool and in the fight against terrorism (see for example Töpfer 2010).
- In addition to these applications, which were usually the reasons to set up CCTV system, a growing number of “derived” uses of CCTV can be observed in European cities: combating parking violation or dog fowling, providing assistance in case of emergencies and accidents, identifying problems and malfunctions in the urban environment and others. All in all, in some local authorities, CCTV is increasingly seen as a tool to manage the city, in its different functionalities.

In many cases, one can observe that the use of CCTV is being expanded or diversified: this is the ‘function creep ‘. Function creep is a problem inherent to the all-important investments such as those required for CCTV. Understandably, many local authorities want to make the best use of their investment in a CCTV system. However, the ‘function creep’ can also be problematic, in that it makes it difficult to evaluate the performance of a system when its goal and justifications change. More importantly, there are ethical issues when new applications are added to the original use of the surveillance technology (see below), without verifying if they justify their intrusiveness on private life. Moreover, citizens are not necessarily happy to learn that the CCTV they have agreed on to fight terrorism is also used for surveillance when they walk their dog or park their car.

Used by whom? Generally, local authorities are the ones who take the decision of setting up a public area CCTV system on their territory. There are nevertheless important differences in Europe with respect to the management of the system and the role of various actors. Local authorities almost always work together with the police when they run CCTV. However, this cooperation can take different forms: an urban control centre of the city provides footage to the police as in some cases in France; the same centre can grant police direct access to its cameras as in the UK (but also in France); -a CCTV system of the local authority run by the police, as for example in the Netherlands; - or, a CCTV system of the police run in cooperation with the local authority (which provides infrastructure, supporting maintenance), as for example in Germany.

The cooperation can take different forms within a single country and can also include other actors providing cameras or CCTV system. Co-operation is formalised by an exchange of protocols between partners. The way information is shared amongst partners is an important issue for all local safety partnerships (see for example FFSU 2002) and particularly important in regard to CCTV.

The forms of cooperation among the various actors working together with CCTV very much depend on who is entitled to see CCTV images and therefore who can work directly with CCTV: Is it national police officers? Local/municipal police officers? Local civil servants? Or private companies? Police officers have certain prerogatives and duties, which make them operators of choice in certain countries. In some countries such as France, Italy and Spain, local authorities can run the CCTV systems themselves independently of the national police. In the UK and Hungary, a local authority can outsource the direct operation of the CCTV system to a private sector company. The issue of who is entitled to deal with CCTV footage is directly linked to the issue of data protection as well as to the cost of using CCTV, and ultimately to the use made of this technology by local authorities.

2.1.2 Smart video surveillance or "smart CCTV"

Smart video surveillance is the new generation of CCTV. We address it in a distinct chapter because it constitutes a significant evolution in surveillance, and because it includes other technologies such as image analysis and biometrics. This means it can go beyond the limits of current systems, which are essentially due to the inability of human operators to systematically analyse the vast amount of information and images produced by CCTV systems.

Not only does smart video surveillance produce good quality images but also, more importantly, it can analyse them and alert on or even anticipate certain situations.
At the core of these technologies are image content analysis algorithms, which can identify people, objects, gestures and situations. This is possible thanks to technological progress in biometrics and image processing algorithms. These systems can also take into account sound and might include sound analysis technologies and other technologies. This means they can not only recognise people or objects (a task which is actually much more complex than movies tend to make us believe), but also identify certain types of behaviour, which are considered risky (for instance, someone bending over while committing an act of vandalism, individuals hanging out in a parking area, or someone shouting to raise attention). New smart technologies have given rise to new concerns about video surveillance, which had not been raised by 'traditional' video surveillance (see below chapter on Ethics).

Such smart systems are not yet widespread in cities. But most cities have already shifted to digital technology, which will allow smart surveillance. They can thus add in technologies that help operators observe and analyse images, until the whole process is fully automated.

Image analysis notwithstanding, many systems already include functions that support operators by crosschecking information provided by images with geographic information systems. For instance, all cameras can automatically monitor a specific area, or automatically shift to other cameras to follow somebody, etc. Many systems also have alert options that detect when something moves or when somebody enters a particular area. In Munich (Germany), a CCTV system in public transport raises alarms when it 'suspects' somebody might be painting graffiti on a train. However, real time image analysis - a technology that is still in development - remains in the realms of science fiction for the vast majority of systems currently in use.

The intelligence of systems can also be used to protect privacy. Most of the systems presented in the working group are able to blur private places (in homes for instances), in order to prevent operators to see them. They also do it dynamically, which means that when the operator zooms in these private zones, the image automatically becomes blurred. Such systems could be further developed to protect anonymity of passers-by.

Automatic reading of registration plates (Automatic Number Plate Recognition, ANPR) is a smart function that has already been implemented for a few years. It is done with specialised cameras that are not used for general surveillance. These systems are used to monitor vehicles in the United Kingdom, the Netherlands, France, Italy, Germany and

Belgium. Not only can they analyse images in order to identify interesting details (such as the registration plate), but also they can link the information with relevant databases. The police can identify the registration plate of all vehicles caught on camera, and are also automatically alerted when the camera identifies a vehicle being sought after by the police. Similarly, vehicles that enter the London Congestion Zone are automatically identified by their registration plate and, if the driver has not paid in advance the congestion charge tax, the system automatically generates delivery of a fine to the registered address of the vehicle.

Research analysis technologies are not used exclusively by specialists. In their most simple form, facial recognition tools are already accessible on Facebook and Google for instance, and are bound to become widespread. This includes also local authorities, which for the moment do not use systematically such technologies, even though most use new information technologies.

Another development of video surveillance already in use is the mobile CCTV unit. Several police forces, including the municipal police, use them when patrolling by car or foot, and even in public transport.

The problem with most systems currently in use is that they are not always accessible at a distance, and even often unable to send images in real time. Most transportation system CCTV equipment simply records images locally. Local authorities are keen to overcome these limits, and in this respect the deployment of 4G mobile telecommunication will undoubtedly push limits further.

2.1.2 Unmanned aerial vehicle (UAV)

Another new surveillance technology at the disposal of local authorities are unmanned aerial vehicles (UAV) or 'drones'. Used by the military for years for reconnaissance and surveillance missions, these devices are increasingly cheaper and handier and therefore make their appearance in the civil domain. They are the civilian 'brothers' of military drones such the *Predator* or the *Global Hawk*, and look more like model planes than aircraft. According to a working document of the European Commission (2012), it might become normal to see them in the European sky. The American Federal Aviation Authority (FAA) predicts the use of 10,000 civil drones in five years time and even 30,000 drones by 2030 (FAA 2011:49).

One of drones' most straightforward fields of application is that of CCTV cameras – given

that drones are in a certain way flying CCTV cameras. However, drones are also quite different from fixed cameras indicated by an information sign. They can fly over any territory – including private space - and they are mobile and can therefore appear anywhere any time. Many drones, and especially micro drones of the size of a bird but also those which can observe from high altitude, cannot be seen or heard very easily, which allows discrete surveillance.
Therefore, they can be used by law enforcement agencies to observe, secure interventions, secure the transport of persons and goods, and to supervise large events and spaces (parks, beaches, outdoor sports events, demonstrations…). As with their military relatives, it would technically be possible to arm police drones. Drones can also be of interest to fire fighters, especially in case of an industrial hazard and for civil protection (as demonstrated by SURVEILLE partner Fraunhofer IOSB)[3]. The report of the European Commission talks about some 400 civilian drone applications in development across the EU in "agriculture and fisheries, power/gas line monitoring, infrastructure inspection, communications and broadcasting, wireless communication relay and satellite augmentation systems, natural resources monitoring, media/entertainment, digital mapping, land and wildlife management, air quality management."(European Commission 2012)

Have those scenarios started to become a reality in European local authorities? For the time being, only some police forces, as the SURVEILLE project partner Merseyside police service, but also the police in Rotterdam and some police forces in Germany and France, are using drones, in particular to observe large events and demonstrations. In addition to regular cameras, they sometimes also use infrared and thermal cameras, which can for example be used to detect heat emission from illegal marijuana plantations. Some fire departments as in Paris have started to test drones.

While drones are at best starting to arrive in the field, the framework for a more intense use has been set in several countries. Aviation agencies and legislators in the US, but also France and Germany have adapted regulations to allow and to be prepared for a civil use of drones. Many governments expect the development of new markets and services with drones (see for example French Ministry of Transport 2008, NY Times 2012).

Moreover, this technology has become accessible to a wider public. Quadrocopter, which send images from their on-board camera to a smart phone, which is also used to pilot them, have been on the market at least since 2011. They are now available at retail stores

[3] Project SENEKA http://www.iosb.fraunhofer.de/servlet/is/20296/

for less than 300€.[4] This accessibility will certainly also contribute to the dissemination of this technology amongst local authorities.

2.1.3 Data mining technologies

Data networks and computing power allow for another type of surveillance technology to develop, which is based on bringing together different sources of information and analysing them. Data mining technologies make it possible to go through very large datasets and identify patterns and correlations in them. It allows people to put together a multitude of elements of information, which might be of no particular value in isolation, to form a larger picture. These technologies can take into account all types of information and electronic traces, from payments to smart meters to licensed vehicles. They make possible "in depth surveys", to create for example profiles of persons and even to predict incidents of crime as for example the PredPol system (NY Times 2011).

This trend towards the aggregation of different data sources can also be observed amongst local authorities. One example is the connection of previously distinct CCTV systems to a large video surveillance system, described above. Another is the creation of local monitoring centres aimed at bringing together different sources of information such as CCTV, alarm systems, local police dispatching in a local command, and control structure. In many cases, the CCTV system is backed up by a geographical information system (GIS), which provides maps and further information on the observed ground. These GIS-systems display all sorts of information on maps. This includes all the details one can find on electronic maps, but also information on crime and disorder (where incidents have taken place, where offenders come from...), or on the population of a neighbourhood or a street. This type of preparation of information has already been used for years in local authorities as part of local safety audits and by local crime observatories. These maps allow for a better understanding of the security situation of a city in order to develop a local safety strategy. These GIS-systems have become usable in real time and have started to become mobile: as such, from an analysis and planning instrument, they are turning into an operational tool.

In general, data mining and profiling are used by law enforcement and intelligence agencies on the one hand as well as business on the other hand. However, it might become increasingly interesting for local authorities to use data mining applications on the information they are in charge of. Within the limits of the data protection regulations and depending on their actual competencies, this could also include information on persons as

[4] See, for example: Parrot AR Drone 2 http://ardrone2.parrot.com/

well as the contact they have with departments of the city or even services that they receive. The data mining application could be very helpful to fight money laundering and organised crime, a fight to which local authorities already contribute in particular with their regulatory powers.

Finally, cities are themselves collectors of personal data. Many public transport schemes (usually local but also at a national level as for instance in the Netherlands) propose electronic tickets in form of chip cards, which allows following and profiling clients. Other membership and subscription cards as for example for museums, libraries, sports facilities, but of course also ID or health insurance cards, which are becoming electronic, provide in theory the same options.

While European data protection regulations are strict, there seem to be possibilities for local authorities to sell this type of information or profiles of citizens or clients to commercial users. In Germany, a recent legislative proposal would allow local authorities to sell datasets with information on their citizens to commercial users. Citizens are obliged to provide this information as part of their obligation to be registered with the local authority they live in and would now have to opt out in order to protect their data (see for example Süddeutsche Zeitung 7 July 2012).

2.1.4 Scanners and detectors

Scanners and detectors represent another group of surveillance technologies. Scanners using waves, such as X-ray millimetre wave or radar scanners, are there to detect hidden products and materials. Local authorities or their local partners may use them for instance to control access to airports, harbours, train stations, public buildings, museums, stadia, or even schools. They usually use metal detectors and X-ray scanners.

Full body scanners or millimetre wave scanners, which allow people to be seen 'naked' and everything they have on them (including plastic surgery), which are very controversial, are currently only used at airports (which are only rarely run by local authorities). These more technologically advanced scanners, which are very expensive, have not found their way into cities yet.

Chemical detectors are used for the discovery of substances such as alcohol, drugs, explosives, radioactive materials or of DNA. They are of course commonly used in Europe, but usually by law enforcement agencies and not local authorities. The exceptions are those detectors for fire, water, gas, chemical substances, which are used to protect public building and for civil protection.

Local authorities do of course also use alarm systems, using radar or vibration detectors. Moreover biometric identification has also found its way into European local authorities, though not as part of general surveillance but in order to control access to certain building or areas (as for example a CCTV control room).

2.1.5 Dual use of technologies

In order to take into account the whole reality of the use of technologies by local authorities and all the opportunities for surveillance, it seems interesting to also look at other technologies, which are not surveillance technologies but which nevertheless provide important opportunities for surveillance. In this context, the new information and communication technologies are central.

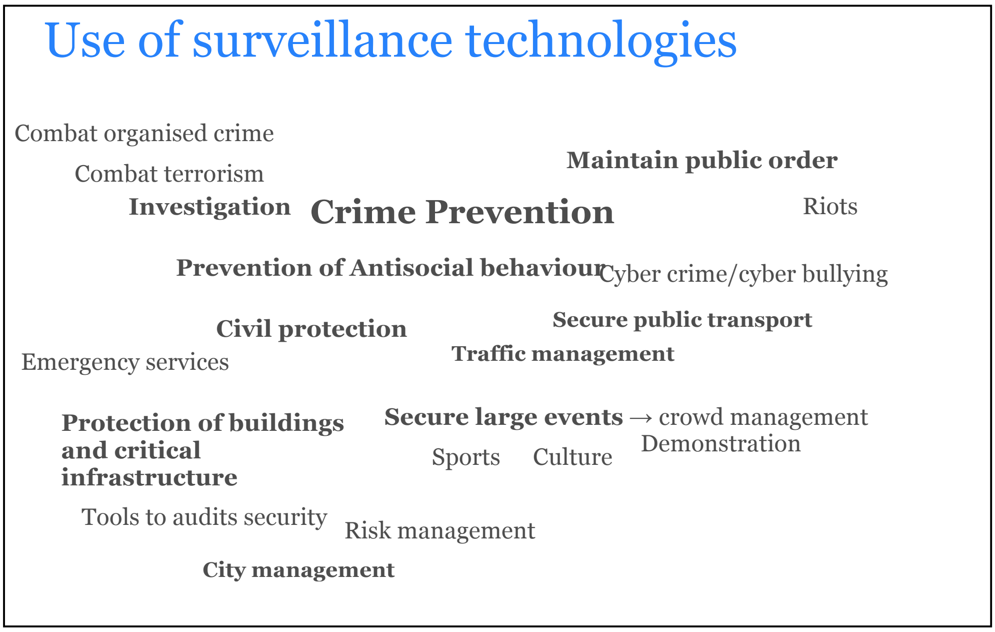
Internet research, searching blogs and social media allow everybody to find an important amount of information on a considerable part of the population, who share it more or less voluntarily. These search engines and software applications are becoming more and more powerful and are beginning to include features like facial recognition.

GPS, Wi-Fi and cell tower data also provide important opportunities for surveillance. Often this type of data, which can be used for surveillance purposes, is voluntarily shared by users to obtain services to benefit from commercial offers, or to identify friends who are in the proximity.

Radio-frequency identification (RFID) chips allow an object or a person to be identified at distance and also to be surveyed. These chips have already found applications on human beings in some European cities. For example, some nightclubs in Barcelona and Rotterdam implant those chips in order to identify guests and as a means for payment (see e.g. Lokowsky 2004).

European local authorities are still at the very beginning of fully using all the potential of new information and communication technologies. They are beginning to see them as instruments to mobilise and empower citizens, to strengthen social cohesion and to develop democratic participation. They use them to communicate to and with citizens, to allow for more interaction and to be able to provide new services. Efus encourages local authorities to make use of these opportunities.

The different uses and applications of the technologies listed above can be summarised as follows:



Use of surveillance technologies

Combat organised crime

Combat terrorism

Maintain public order

Investigation **Crime Prevention** Riots

Prevention of Antisocial behaviour Cyber crime/cyber bullying

Civil protection **Secure public transport**

Emergency services **Traffic management**

Protection of buildings and critical infrastructure **Secure large events** → crowd management

Sports Culture Demonstration

Tools to audits security Risk management

City management

2.2 The motivations to use these technologies

Local elected officials use surveillance technologies for the security of the citizens of their cities – who are their voters. The main motivation of local authorities to use (or not) surveillance technologies is their effectiveness in addressing problems. When local authorities use them, it is because they feel that these instruments fit well in the 'toolkit' they need to implement their local security strategy.

The question of the motivations to use technologies is therefore very similar to the question of the applications of the technologies, which we addressed in the previous section. However, both are not identical. Motivation is not only a technical issue but also includes the political economy of using these technologies.

The information that mayors or even local authorities as a whole have at their disposal about these technologies might be incomplete. When there is still research going on about the effectiveness of surveillance technologies, how can cities be certain that they are the best instruments for their situation? In the best case, the technology applications we see in local authorities reflect a choice under uncertainty on what seems the most adequate solution to their problem. It is for that reason that local authorities are very keen to obtain more information on the efficiency of surveillance technologies, including on methods of how to collect relevant information themselves.

There are also other reasons that influence a local authority's decision to use or not surveillance technologies. The acceptance of surveillance technologies by citizens plays an important role here. Local authorities are in some cases confronted with opposition to the use of surveillance technologies but in others with demands to use them. They will have to convince citizens why they consider such a technology to be necessary, or on the contrary, the wrong choice. They may have to explain why they cannot set up all the cameras citizens ask for (e.g., Le Havre) or explain why they have to take a camera down that a neighbourhood wants to keep (e.g. Rotterdam) (see Efus 2010b).

Especially in times of tight budgets and public debts, many European cities are interested in security and surveillance technologies in order to make savings. At the beginnings of video surveillance for example, the European Union underlined its virtues in terms of cost-effectiveness. "Cameras as crime prevention tools are, in general, a new and cost-effective way to reassure citizens preoccupied by their security," concluded the European crime prevention conference organised by the Dutch presidency of the European Union in 1997 in Noordwijk. Experiences exchanged within the European Forum have shown that CCTV is rather expensive, especially since it requires sufficient and well-trained staff to operate the system on the one hand and to follow up on identified incidents on the other hand. Nevertheless, the idea that CCTV would save personnel or that it would free human resources for other tasks is still relatively widespread. Technological progress almost always comes with the promise of increasing productivity and savings. The field of surveillance technologies is no exception. The danger is that municipal authorities are not necessarily conscious of the financial and human resources impact in the long term necessary to operate the system and to follow up on incidents, and that they are primarily appealed by technologies that are becoming constantly cheaper as well as by co-funding opportunities for the hardware by national or regional governments. Furthermore, it still needs to be seen in many cases, if these savings can actually be achieved (see also efficiency below).

Another economic reason to use surveillance technologies is the incentives given by national or regional governments. The British government had *given* CCTV to local authorities in its 'City Challenge Competitions' in the 1990s. In Italy, it is the regional level at which finances video surveillance (see e.g. Emilia Romagna or Veneto in Efus 2010). In France, President Sarkozy developed the use of CCTV with subsidies to local authorities. 60% of the national subsidies for crime prevention (Fonds interministériel de prévention de la délinquance) for local authorities were earmarked for video surveillance.[5] This was a strong incentive for local authorities to make use of surveillance technologies.

A city's decision to make use of technologies like video-surveillance can also be influenced by the fact that other cities already use it. A city might not want stay behind; a local elected official might not want to give the impression he does not do everything possible, including state of the art technologies, for the security of local citizens. Beyond mimicry or possible information on good experiences, there are cases in which local authorities are obliged to catch up, which is when they have to prevent displacement effects on their territory. When all surrounding municipalities for example use CCTV, it might be possible that certain undesired phenomena might be displaced to the neighbouring municipality without surveillance.

The use of surveillance technologies can also fit into a larger strategy of a municipal authority of becoming a 'digital city' or a 'smart city'. Beyond communicating modernity, a city might want to strengthen its competitiveness with state of the art technical infrastructure, to provide new services enabled by new technologies, to apply modern risk management methods for certain issues. Such a context might favour the use of technologies in the area of prevention and security.

Finally, as Jean-Baptiste Say[6] noted in the 19th century, supply finds its demand. Commercial offers might contribute to a decision to use a surveillance technology such as CCTV. As part of the exchanges within the European Forum, we have noted a certain commercial presence and sometimes a commercial pressure, in particular for local authorities in Central and Eastern Europe.

3. Effectiveness and ethical challenges

3.1 Effectiveness

Does it work? Are technologies proven to be useful? In general, the feedback from municipal authorities that have been exchanging dialogue about video surveillance within the European Forum, and are themselves CCTV users, is positive[7]. Almost all have success

[5] http://www.prevention-delinquance.interieur.gouv.fr/fileadmin/user_upload/04-Sur_le_terrain/Pdf/C_du_5_mars_2010.pdf

[6] Jean-Baptiste Say (1803): Traité d'économie politique livre I, chapitre XV, Des débouchés

[7] Considering of course, that our panel of cities is self-selected and therefore does not necessarily reflect a representative view.

stories to tell: a reduction of crime in areas where cameras are installed, reduction of anti-social behaviour, the disappearance of open drug scene or prostitution, offenders being caught in the act, success in some investigations thanks to the cameras. Most of these cases have also had a positive impact on the population's feeling of security.

Furthermore, municipal authorities report that their CCTV systems have recorded numerous incidents. For the sole year 2009 for instance, Rotterdam recorded a total of 23,700 incidents, or an average of 65 a day. They note the increasing demand for video surveillance images for police investigations (sometimes, system managers receive requests to provide images daily). They also stress that the feedback from their partners of the police and justice system is very positive. All of this indicates that the CCTV system does ‘what it is supposed to do’ i.e. that it records incidents. However, it does not imply that it works in actually reducing and/or preventing crime. In fact, the numbers of incidents also seem to show that the dissuasive effects of CCTV and its capacity to prevent incidents are limited.

There are actually relatively few scientific evaluations of the effectiveness of such systems. Assessing the effectiveness of technologies and ultimately their contribution very often means a comparison between the situation before and after the deployment of video surveillance. A significant number of cities conduct such analyses. However, this type of survey does not necessarily prove that the changes observed are directly linked to the use of technology. Indeed, changes in the level of security can be the result of other factors, specific measures, or external factors.

When they install a video surveillance system cities often implement in addition other types of measures such as remodelling public spaces (for instance by improving street lighting), increasing police patrols or strengthening specialised and social prevention. This puts us in a dilemma; factors that make it more difficult to evaluate the CCTV system put in place are at the same time indicators of the quality of the local safety strategy. Indeed, many security problems require an inclusive response that tackles their various causes and risk factors. This is why video surveillance should be considered as part of a global prevention strategy.

There are empirical studies on the impact of video surveillance on security, in particular in the United Kingdom where CCTV has been widespread for quite some years now. One of these reports, by Welsh and Farrington in 2002 for the UK’s Home Office, conducted an evaluation of 46 video surveillance systems installed worldwide. Results were mixed: half of the admissible evidence shows a positive impact on crime; five show a negative impact; and five no impact at all. Furthermore, video surveillance had no impact on violent crime but had a desirable impact on offences linked to vehicles and on those committed in public parking lots. In city centres and in areas surrounding social housing estates, video surveillance appears to have contributed to a significant 2% reduction of crime in experimental areas, compared to control areas.

Similar conclusions on the impact of video surveillance have been made as a result of numerous surveys and, in particular, the important study of Martin Gill and Angela Spriggs in the United Kingdom (2005). The authors concluded that video surveillance seemed to have limited effects on crime in city centres and in residential areas, and worked better in enclosed areas with controlled access such as hospitals, parking lots and commercial malls. Furthermore, video surveillance seemed to have little effect on violence and alcohol-related offences, and produced better results on premeditated crime.

As in other surveys, Gill and Spriggs also noted a halo effect; in other words the reduction of crime in neighbouring areas as well as the displacement of crime. Local authorities are aware of this. They realise that surveillance cameras tend to push illicit activities such as drug traffic and consumption, street prostitution or pickpocketing elsewhere. In these cases surveillance does not solve the problem but merely displaces it. But this can be a benefit for a community. Indeed, a community might deem a priority to first ‘win back’ and secure some specific public spaces, in particular in order to improve the feeling of security.

Overall, video surveillance seems to produce mixed results. Gill and Spriggs (2005) concluded in their survey that, “Assessed on the evidence presented in this report, CCTV cannot be beneficial”.

The relation of effectiveness to cost gives cities another very interesting indicator, in particular in times of budgetary restrictions. This indicator is efficiency. In order to estimate it, it is necessary to calculate all the costs. Indeed, municipal authorities involved in the debate on this matter with the European Forum are aware that using this technology is rather expensive. Even if equipment prices keep going down, they have seen that video surveillance requires an infrastructure, maintenance and above all staff to manage it and to react to the information it provides. However, not all municipal authorities are immediately aware of all the costs implied by the use of CCTV, and might therefore be at risk of overestimating the return on their investment.

The cost-benefit ratio is the reason for which some cities have reservations regarding the efficiency of surveillance technologies. The internal report of the police of London lamenting that only one crime is solved for every 1,000 cameras installed in London has become well known[8]. In France, the Court of Auditors (Cour des Comptes (2011)) stated that "The relation between the cost of the [video surveillance] system and the benefits for the national and local police is limited." It added that, "It is regrettable, in particular with regard to the amount of public spending in this area, that no rigorous evaluation is being done in France of the efficiency of video surveillance in public spaces."

This is precisely why there is so much interest in gathering more information on the efficiency of video surveillance and surveillance technologies. Indeed, cities have committed in the Manifesto of Aubervilliers and Saint-Denis to further evaluate their policies so as to make them more evidence based. Evaluation is planned from the conception of projects, with clearly defined objectives (a key requisite of any evaluation).

Within the European Forum for Urban Security, there is no consensus on video surveillance precisely because there are concerns about its effectiveness and efficiency. A number of cities feel that notwithstanding the ethical questions raised by video surveillance, other instruments are just as effective, in particular street lighting and human presence.
For the same reason, the European Forum does not have a public stance in this matter and considers that decisions as to whether using video surveillance have to be taken on a case-by-case basis. The Forum recommends to use it responsibly, and to thoroughly study its impact on a specific situation. It also recommends choosing, if possible and all things being equal, less intrusive means.

3.2 Fundamental rights and ethical challenges

By nature, surveillance technologies often infringe on individuals' rights to privacy. This right to privacy also applies partially to the public space. While it seems a contradiction in itself, there are in fact several generally accepted social conventions, by which people do respect the privacy of others also in public spaces. For instance, one does not get too close to someone else; one does not stare at him or read over his shoulder. The European Court of Human Rights recognised this right to privacy in the public space in its ruling in the case of van Hannover vs. Germany (2004). This right to privacy is fundamental in order to enjoy other rights such as the freedom of expression and association. (Goold 2010)

[8] See for example http://www.telegraph.co.uk/news/uknews/crime/6082530/1000-CCTV-cameras-to-solve-just-one-crime-Met-Police-admits.html

Surveillance technologies therefore come with a cost in terms of a loss in privacy, which must be taken into account when balancing whether to use them or not. As underlined in the Manifesto of Aubervilliers and Saint-Denis, member cities of the Forum are particularly aware of the fact that surveillance technologies such as, for instance, video surveillance or the use of other technologies for surveillance raise questions in terms of fundamental rights and ethics. (2012 Efus Manifesto).

The use of surveillance technologies remains an open debate among Efus member cities. Indeed, the fact that State surveillance is becoming systematic by means of these technologies is still a matter of public debate in many European countries.

Social acceptance varies greatly from one European country to the other, which is reflected by the varying degree in which these technologies are used. According to a 2003 survey in five European capital cities, 90% of Londoners were in favour of street video surveillance, whereas only 25% of Vienna's population shared that opinion (Töpfer 2010 : 78). The city of Brno (Czech Republic) conducts regular surveys of the population's feeling of security and their opinion on video surveillance. In 2005, 4.5% of respondents felt video surveillance restricted their personal freedom. Only 1.9% shared that view in 2009.

It seems that in general, public debate on the use of CCTV tends to evolve and to become less polarised. For instance in Rotterdam, where opinion polls are conducted each year, public opinion has evolved in the ten years since the deployment of the CCTV. At first, there was mistrust, questions about effectiveness and fears about infringement on privacy. Now, people seem to be attached to "their" cameras; they trust the system and consider it effective (Efus 2010: 209). In France, where there has been a heated debate on video surveillance ever since the first systems were installed at the beginning of the 1990s, 71% of the population is "in favour" of cameras in public spaces, and 28% "against", according to a 2008 survey. The United Kingdom has reviewed its use of CCTV in the middle and at the end of the past decade. With the Protection of Freedoms Act 2012 it has created new regulations for CCTV and ANPR, but also biometric data, counter-terrorism powers, enforcement actions, and extended the Freedom of Information Act and the Safeguarding Vulnerbable Group Act to "suppress the culture of intrusion in citizens' private lives". (Efus 2010: 14)

Cities and regions member of Efus do not consider that freedom and security are fundamentally opposed or mutually exclusive. On the contrary, they consider them to be linked and part of an approach based on the respect of fundamental rights. It does not make sense to defend one value against the other, for instance security against liberty. Both these rights are intertwined. Ever since the Forum was created, cities consider precisely that one of their most important tasks is to reconcile and strengthen both of these areas (see *Aubervilliers and Saint-Denis Manifesto*, 2012). “The Executive Committee [of Efus] is neither in favour nor against the use of video surveillance. It calls for a commitment to the protection of citizens’ privacy and fundamental liberties when setting up and operating CCTV systems”. (Efus 2010).

When video surveillance first began the best protection of private life resided in the technical and operational limits of the system. Big Brother at the time could not see much, or else had to pay a steep price for detailed analyses. Nowadays, technologies are far more sophisticated and threats to the respect of privacy can be greater. This is why Efus, in its *Charter for a democratic use of video surveillance,* worked on identifying general principles that could be applied by European cities to a whole range of contexts while remaining valid in spite of technological evolution.

The purpose of this Charter is to enable cities to use video surveillance in a way that is respectful of fundamental rights, which implies among others the requirement to carefully evaluate the need to use this technology in a given situation. Seven principles have been identified and are applied by the cities that endorsed the Charter. These are:

- *Legality*

Laws and regulations are the best protection of individuals' fundamental rights. They constitute a barrier against dangerous trends that can take many forms, in particular against threats to freedom. An intrinsically intrusive technology, video surveillance is a potential threat to private life if not properly regulated. Thus, the use of video surveillance must be made in accordance with the laws and regulations of the territory where this is done. The principle of legality is the basis of the legitimacy of any video surveillance system. However, the law in some countries is not adapted to these new technologies. In those cases, the Charter calls for elected officials to act and, for instance, to elaborate internal regulations on the use of the local video surveillance system. This is also the purpose of the local ethical charter.

Respecting the principle of legality means that local authorities:

- Are totally compliant with national legislation regarding the installation and operation of their video surveillance system;
- Inform citizens about the existing legislation so they are assured their fundamental rights will be respected;
- Actively strive to reform regulations, if this proves to benefit citizens, for instance by elaborating an ethical charter or internal rules, even if not required by law.

- ***Necessity***

The cost of video surveillance compels elected officials to evaluate if it is a necessity in light of the local context. This principle also means that video surveillance should be considered only if it is the only response to the local security problems and context. If it cannot be established that video surveillance is a necessity, it will be difficult to prove its contribution to security and crime prevention.

In practical terms, this means that local authorities should conduct a security audit in order to identify precisely the most urgent security problems of the locality. The audit should also establish that video surveillance is the most adequate response. This includes an evaluation of the cost-benefit ratio, not only in financial terms but also as regard quality of life and protection of privacy.

Mannheim (Germany) is a very interesting example in this regard. The necessity of the CCTV system was evaluated over several years and after five years, it was dismantled (except for one camera) because it had served its purpose.

Regarding the principle of necessity (and this concerns also the principle of proportionality, which is exposed below), it is important to take into account the "function creep", e.g. the progressive increase in the number of applications of video surveillance. On the one hand, it is important to keep in mind that the system can have other uses when evaluating the return on investment. But on the other, it is important to stick to the uses planned at the time of deployment in order to respect the principle of necessity.

- Proportionality

The use of video surveillance technologies should be proportionate to the needs. It must not result in greater interference in privacy and other fundamental rights than is justified by the actual benefit obtained for the legitimate aim of increased security. Cities must keep a fair balance. The aim of this principle is to raise awareness among cities regarding excessive use of video surveillance and excessive investment of collective resources that go beyond identified needs.

In practical terms, this means cities should:

- Precisely identify needs through an audit;
- Ensure that the system is coherent with the needs that have been identified previously;

- Refrain from an excessive use of cameras, even when called for by the local population, and evaluate any potential extension of the system as per their adequacy with respect to the principles stated in the Charter;
- Ensure that the resources allocated to video surveillance do not hamper other prevention schemes, which are equally important. This means that video surveillance should be assessed in conjunction with other local security and crime prevention schemes.

Some interesting examples in this respect are found in Ibiza (Spain), Mannheim (Germany) and Saint-Herblain (France), all of which have chosen to install a very limited number of cameras.

- Transparency

There is a certain degree of irrationality linked to video surveillance, which has prompted heated debates. Nowadays, local elected officials throughout the political spectrum agree on the advantages of video surveillance provided it is accompanied by fundamental guarantees. Transparency is one of them. This principle means that local decision makers must inform the public about the video surveillance system. Transparency also contributes to legitimacy. It is reassuring for the people, who are informed about the causes and consequences of such system and its role in their quality of life. Video surveillance aims at protection, not surveillance, as the French would say.

In practical terms, this means that local authorities should inform the local population about the necessity of installing video surveillance and its practical implications. They should also inform about the cost of investment and the expected results. Limits and safeguards should be clearly stated. Lastly, areas under surveillance should be clearly identified as such.

Member cities of the European Forum have designed a template for public signs alerting of the presence of video cameras, basing themselves on good practices implemented in several European cities, in particular Lyon (France). The design created by Efus has since been used by the city of Paris (France).

- Responsibility

Given the fact that video surveillance is a threat to fundamental liberties, its usage must be under the responsibility of local authorities. In a great number of countries, legislation restricts the number of public institutions that have authority to monitor public spaces. Indeed, such guarantees are necessary given that it is such a sensitive tool. Local authorities must make sure that all the people involved in operating the system are aware of their responsibility and of the risks incurred in case they do not comply.

It is also necessary to define the chain of command, with the specific tasks and responsibilities of each stakeholder. Safeguards must be put in place to protect this chain of command. The people in charge must be identified and remedies and claims procedures must be clearly explained.

- ***Independent oversight***

Users of a video surveillance system are not best placed to control if it is deployed with due diligence. This is why the Charter recommends local authorities should put in place an independent control system. This principle aims at ensuring neutral control. In this respect, it is recommended to work together with scientific and/or academic researchers. In practical terms, cities are advised to think how such an independent control can be put in place, including when not required by law. It is recommended to put in place *ad hoc* organs such as an ethics committee.

Also, independent control must be made in conjunction with the evaluation of the scheme. This control can be done in various ways. For instance French cities such as Le Havre, Lyon, Bordeaux, Toulouse, and Paris have set up ethics committees that oversee their video surveillance systems. In Sussex (UK), citizens participate directly in supervising the system through the ‘independent visitor scheme’.

- Citizen participation

Citizen participation in local security and crime prevention policies is desirable. This is also true of video surveillance. The Charter thus calls local authorities to consult citizens when conceiving and operating a CCTV system. The more they involve citizens, the more citizens will be aware of security matters and capable of providing well-informed advice.

In practical terms, this means:

- Using participatory democracy tools (opinion polls and surveys, neighbourhood meetings, etc.) in order to measure local inhabitants' reactions to and expectations from the video surveillance system;
- Ensuring that citizens take part in controlling and evaluating the system;
-Ensuring that citizens are properly informed through educational or informative publications or other means.

Among the good practices known in this respect, Rotterdam regularly consults citizens about its video surveillance system. In a certain number of other European cities citizens are also consulted about the use of video surveillance.

The seven principles presented here are not an end in itself. Cities must put in place evaluation schemes in order to demonstrate the validity of the system. It is also recommended to periodically evaluate the compliance of the system with the principles exposed in the Charter.

References

Cour des comptes (2011) : L'organisation et la gestion des forces de sécurité publique – juillet 2011 http://www.ccomptes.fr/Publications/Publications/Organisation-et-gestion-des-forces-de-securite-publique

Dekkers, S. et al. (2007): *Evaluatie Cameratoezicht op OpenbarePlaatsen. Éénmeting*. Eindrapport. Regioplan publicatienr. 1515. Amsterdam, Mai 2007, p.IV.

European Forum for Urban Security (2012): Le Manifeste d'Aubervilliers et de Saint-Denis

European Forum for Urban Security (2010a): Charter for a democratic use of video surveillance

European Forum for Urban Security (2010b) : *Citoyens, villes et video surveillance. Vers une utilisation démocratique et responsable de la vidéosurveillance*

European Forum for Urban Security (2010c) : Resolution of the Executive Committee on video surveillance

European Forum for Urban Security (2006a : Le Manifeste de Saragosse

European Forum for Urban Security (2006b) : Cultures de prévention – les politiques de prévention de la criminalité urbaine en Europe : Vers une culture commune?

European Forum for Urban Security (2004): Local elected officials and crime prevention

European Parliament (2012) : Fighting cyber crime and protecting privacy in the cloud. Study of the Policy Department C: citizens' rights and constitutional affairs.

European Commission (2012) : Towards a European strategy for the development of civil applications of Remotely Piloted Aircraft Systems (RPAS). Staff working document SWD(2012) 259 final

European Court of Human Rights (2004): Case of Von Hannover v. Germany

Federal Aviation Agency (2001): FAA Aerospace Forecast. Fiscal Years 2011-2031

Farrington, D.P. and Welsh, B.W. 2002. Effects of improved street lighting on crime: a systematic approach, Home Office Research Study 251.

Ferenbok, Joseph and Andrew Clement (2011) : Eyes Everywhere. The global growth of camera surveilance. In :Randy Lippert, David Lyon (ED) : The Global Growth of Camera Surveillance. Routledge.

French Forum for Urban Security (2002): Secrets, partage, informations

Gautier, C. (2010): Invitation to join the Forum's initiative for a democratic use of CCTV. In: Efus (Ed): Citizens, Cities and Video Surveillance Towards a democratic and responsible use of CCTV. p.99– 07.

Gill M. and Spriggs, A. 2005 Assessing the Impact of CCTV. Home Office Research Study No. 292. London: Home Office Development and Statistics Directorate.

Goold, Benjamin (2010): CCTV and Human Rights. In: Efus (Ed): Citizens, Cities and Video Surveillance Towards a democratic and responsible use of CCTV, p.27-37.

Hempel, L. & Töpfer, E. (2004): *CCTV in Europe. Final report of the Urbaneye Project. Zentrum Technik und Gesellschaft,* TU Berlin.(Urbaneye Working Paper No. 15), p. 44. En ligne : http://www.urbaneye.net/results/ue_wp15.pdf.

Losowsky, Andrew (2004): I've got you under my skin. The Guardian, 10 June 2004. http://www.guardian.co.uk/technology/2004/jun/10/onlinesupplement1

New York Times (2011): Sending the Police Before There's a Crime
http://www.nytimes.com/2011/08/16/us/16police.html?_r=4&

Préfecture de Police (2011): Plan de vidéoprotection pour Paris (PVPP)
http://www.prefecturedepolice.interieur.gouv.fr/Prevention/Videoprotection/Plan-de-videoprotection-pour-Paris

Recommandations de la conférence européenne "Prévention de la criminalité" 11–14 Mai 1997. Paru dans : European Journal on Criminal Policy and Research, Vol. 5, No. 3 (Septembre 1997), pp. 65-70 (66).

Süddeutsche Zeitung (Prantl, Heribert) (2012) : Städte dürfen Daten Ihrer Bürger verkaufen, issue 7 July 2012.

Squires, P. (2010): Citizens, justice and CCTV: democracy, privacy and effective crime prevention. In: Efus (Ed): Citizens, Cities and Video Surveillance Towards a democratic and responsible use of CCTV, p.37-57.

Töpfer, E. (2010): The use of CCTV in Europe – a political choice. In: Efus (Ed): Citizens, Cities and Video Surveillance Towards a democratic and responsible use of CCTV, p. 65-81.

UN Economic and Social Council (2002): Guidelines for the Prevention of Crime
(Council resolution 2002/13)

Van den Hoven, Jeroen (2010): Privacy by Design: the case of CCTV. In: Efus (Ed): Citizens, Cities and Video Surveillance Towards a democratic and responsible use of CCTV, p.57-64.
Welsh, B. and Farrington, D. 2002 Crime Prevention Effects of Closed Circuit Television: A Systematic Review, Home Office Research Study, No.252, London : HMSO