PSC Europe Conference

Brussels, PSCE Conference, 8 June 2011

Speaking points

Ladies and Gentlemen,

It is my pleasure to speak to you on video-surveillance and data protection, an important topic which has also always been close to my core business activities.

I was asked by the organizers to focus on the legal and the ethical dimension of the development of video surveillance.

However, I am in front of ad audience which seems to be mainly composed by researchers, industry and users (national authorities in charge of PPDR-Public Protection and Disaster Relief).

Therefore, I am not here to celebrate the abstract value of fundamental rights compared with the needs of security and good administration. At the same time, we cannot deal with these issues on the basis that this is a territory in the full ownership of security and IT choices.

In my presentation I will mainly refer to CCTVs and video-surveillance, but the principles I am going to highlight could, where appropriate, be applied to other forms or technical means of surveillance after making any necessary adjustments to them.

1.1 The trend

We all know that video-surveillance has become a popular tool to tackle security issues.

Let me refer to a trend in video-surveillance that we would probably all agree upon: we are faced with extensive and increasing use of closed circuit television (CCTV) and now more intelligent surveillance both in private and semi-public spaces. In addition, and importantly for the topic of this conference, throughout Europe, more and more video-surveillance systems are being installed in public spaces for the purposes of crime prevention following the UK's example of deploying open street CCTV. Indeed, in many urban areas it is difficult to find a place that is not extensively monitored.

In addition, video-surveillance systems are also becoming more and more sophisticated and powerful. Modern systems capture and record digital images that are easily copied and distributed. The images can be instantaneously broadcast to a multitude of recipients or posted on the Internet with the help of today's and tomorrow's powerful techniques and digital communication networks.

Intelligent and interconnected systems are better able to retrieve and match images against a database of images or track moving targets (objects or persons) in large areas. They are also getting better at automatically identifying pre-defined, "suspicious" behaviour.

1.2 Why there is a need for data protection ? How to make sure it is respected ?

We are dealing with a fast-developing area which, at first sight, might appear very technical and reserved exclusively for IT or security management.

However, in reality, video-surveillance involves sensitive and strategic issues from the human rights perspective, considering that a number of liberties and rights are at stake.

Despite its *popularity and potential benefits*, video-surveillance poses serious concerns as regards to privacy and other fundamental rights and freedoms such as the privacy at the workplace and the liberty of movement and, sometimes, the right to be free from discrimination, the freedom of expression and the freedom of peaceful assembly - rights we cherish and all too often take for granted in Europe.

Today I will not discuss in any greater detail the many ways in which video-surveillance may effect fundamental rights and why effective data protection in this area is so essential.

Suffice it to say that growing use of surveillance and the growing use of personal data collected via video-surveillance must lead - under the rule of law! - to a growing need for protection. A balance is needed.

The topic I would like to address today therefore is what we can do to operate videosurveillance and similar systems in such a way as to minimize intrusion into individual's privacy and other fundamental rights.

In other words, I would like to talk about what we can all do - CCTV operators, suppliers of technology, law enforcement bodies, but also academics, data protection authorities, governments and legislators- to ensure that surveillance devices are used responsibly with effective safeguards in place.

1.3. CCTV laws and guidelines

In my first two years of office in 2009 and 2010 as one of the two European Data Protection Supervisors, we have developed and adopted a set of video-surveillance Guidelines.

The Guidelines have a relatively limited scope –they apply only to European institutions and bodies, such as, for example, the European Commission or the European Parliament, which each operate a network of CCTV cameras on their main sites and in

their representative offices in Member States and third countries.

Nevertheless, work on these Guidelines also gave us an opportunity to contribute to the European debate on CCTV more broadly.

EDPS Guidelines are now the most recent regulatory instrument you can find.

But, when developing these Guidelines we were able to already build on a large number of other guidelines, legislative texts, reports and other documents discussing CCTV. Just to name a few:

- the Opinion 4/2004 of the Article 29 Data Protection Working Party,
- the 2003 Council of Europe Guiding Principles for the protection of individuals with regard to the processing of data by means of video surveillance,
- the Venice Commission Report of 2007[1] ,

[1] The Venice Commission is the Council of Europe's advisory body on constitutional matters.

- CCTV laws in various European countries (e.g. UK, Italy, Belgium) and beyond (e.g. Canada, Australia, New Zealand).

I was involved as rapporteur, consultant or author of more or less all these international legal instruments, and I am happy to share my experience today, to briefly summarize few basic points.

First, I would like to briefly outline four key principles that guarded us when developing our Guidelines at the EDPS and which we believe should be the key to ensuring that surveillance systems will be used selectively and with effective safeguards in place:

- Selectivity, proportionality
- Accountability and
- Privacy by Design.

The first two of these are "old, established" principles while the third and fourth ones are to be discussed as relatively "recent developments" in the framework of the review of the EU data protection framework.

2. Key principles – 1 and 2: Selectivity and proportionality

Let me start my comments on the twin principles of selectivity and proportionality by quoting an anecdote which relates to my past activity as Secretary General of the Italian DPA.

The Italian DPA has adopted in 2004 a detailed decision - recently updated in 2010- to be applied to all controllers of video-surveillance systems in the public and private sectors. This was done in close cooperation with the Police Department of the National Home Office the Chief of which circulated strict instructions to all relevant police offices and local municipalities with a view to be extremely cautious in introducing new systems and in connecting them to the centralized police emergency services.

In other words, selectivity and proportionality were considered crucial first by a public order point of view, with a view to reduce expectations that any minor emergency could be managed by police forces via the emergency service in a caotic and not selective approach.

I hope this small anecdote illustrates well that fundamental rights and security do not have to be mutually exclusive. Using a pragmatic approach based on the twin principles of selectivity and proportionality video-surveillance systems can meet security needs while also respecting our privacy.

Cameras can and should be used intelligently and should only target specifically identified security problems thus minimising gathering irrelevant footage. This not only minimises intrusions into privacy but also helps ensure a more targeted, and ultimately, more efficient, use of video-surveillance. Proportionality is also relevant with regard to all practical modalities of the collection and of the processing of data.

3. Key principles - 3: accountability - ensuring, verifying and demonstrating good administration

Another key principle is accountability.

In our view, within the limits provided by data protection law, each entity operating a video-surveillance system has a degree of discretion on how to design its own system.

At the EDPS we are not in favour of an overly prescriptive approach by regulators and legislators: reality can always come in much more colourful shades than it can be foreseen in advance from a government office or even via an informed legislative debate.

Flexibility is also needed for changing circumstances, developing new technologies and accommodating specific circumstances.

At the same time, each organization must also demonstrate that procedures are in place to ensure compliance with data protection requirements.

Recommended organisational practices include adopting a set of data protection safeguards that are to be outlined in the organization's video-surveillance policy and periodic audits to verify compliance.

In addition, when the circumstances such as the complexity of a system and its impact on fundamental rights justify, we recommend that an impact assessment should also be carried out and documented in an impact assessment report.

I think we do not have now time to enter into greater details about policy, audit and impact assessment.

But crucial is to say that data protection should not be viewed as a regulatory burden, a "compliance box" to be "ticked off". Rather, it should be part of an organisational culture and sound governance structure where decisions are made by the management of each organization based on consultations with all affected stakeholders, and when such is available, based on the advice of the organization's data protection officers.

4. Key principles - 4: Privacy by design

4.1. Building privacy into the design of the system

Last but not least, I would like to emphasize the importance of a fourth key principle what we have come to call “Privacy by design”.

By this we mean –by and large– that data protection and privacy safeguards should be built from the very beginning into the design specifications of the technology that the organizations use as well as into their organisational practices.

In addition, “Privacy by design” also means timely consideration of data protection issues.

When installing or updating a video-surveillance system, an initial data protection assessment should be carried out (with the assistance of the data protection officer, if available) well before any financial commitments are made. This will help prevent costly mistakes.

5. Conclusions and “take-home” message

A surveillance system is a powerful technological tool with many potential benefits but also posing significant risks to privacy and other fundamental rights.

To harness its powers and realize its potential, adequate safeguards should be developed based on four key principles I have mentioned.

We are all in this together. There is space for a joint effort from all relevant stakeholders, industry, law enforcement bodies and other operators.