The right to privacy and the protection of public security

A struggle?

Peter Michael
Data Protection Secretary of the
Europol Joint Supervisory Body

In the last 50 years of its history, the world has not been confronted with so many and so intrusive problems. One of these issues, the public security is subject of this plenary session combined with the right to privacy. The organisers of the International Conference have shown trust in the future to combine these two items that always seem to contradict: the right to privacy **and** of public security.

This contribution focuses on certain developments in the European Union: developments in the fight against terrorism. It will also touch upon the struggle to combine those developments with sufficient data protection safeguards and present some ideas to achieve a balanced situation as described in the title of this plenary session.

The establishment of the area of freedom, security and justice in the European Union was a new objective set for the European Union by the Treaty of Amsterdam in 1997. The Tampere European Council in October 1999 placed this objective as a priority of the Union's agenda and set an ambitious program dealing with all the aspects that could contribute to that objective.

In its assessment of the Tampere program, the European Commission reiterated in June 2004 the need to maintain the priority status for the prevention and fight against terrorism.
It should be stressed that terrorism must not be seen as an isolated act. Many forms of (serious) crime are connected with the preparation of terrorist acts. The prevention and fight against terrorism thus includes the prevention and fight against serious forms of crime.
Furthermore, it is generally recognised that the fight against terrorism and serious forms of crime is a combined responsibility of all Member States of the European Union as member of the world community.

The Council of the European Union has adopted many proposals in the area of the fight against terrorism and serious crime or is in the process of adopting such proposals. The main characteristics of these proposals are: more cooperation between law enforcement authorities and intelligence services, more processing of more personal data in the investigation phase as well as in so called "fishing expeditions" and the combination between the fight against terrorism **and** other serious forms of crime. These developments are not reserved for the European Union. The establishment of the Department of Home Land security in the United States of America and the use of air passengers data throughout the world are just some examples of a world wide effort to improve security. And of course all these developments create a situation in which worldwide a greater number of authorities will receive and further process a larger number of personal data.

The European Commission also issued its orientations on the future. These clearly visualize a Europe where the area of freedom and security seems to be assured: Strengthening of the position of European law enforcement authorities such as Europol and Eurojust, creating a coherent criminal justice, increasing the operational capacities of cooperation between the European Union Member States, creating a framework to improve information exchanges, creating an information exchange center, developing a policy on intelligence for preventive and enforcement purposes, introducing new large scale computer systems, and the development of public-private partnership combining information available to the private sector and to police services.

According to the Eurobarometer conducted by the European Commission in December 2003, 71% of European citizens consider joint decisions and joint actions the best way of preventing and fighting crime throughout the European Union.
Clearly the fight against terrorism and serious crime is taken seriously by everybody.

However, this is not the only program for Europe. Another important value of the European Union is the improvement of the protection of persons in the exercise of their fundamental rights. The Charter of the European Union and the creation of the Constitutional Treaty are important milestones for fundamental rights including data protection.
It should also be stressed that all the proposals just mentioned and all other initiatives still under discussion always mention that fundamental rights and data protection should be respected.

The only question is how: is it possible to have a secure area of freedom and security and at the same time respect for fundamental rights? How to establish a world in which the fundamental right to live in security is combined with the fundamental right of the protection of personal data.

Data protection is frequently presented as a balance, a balance between the individual rights and other interests. Instrumental in creating such a balance are principles that data should be processed fairly, for specified purposes and on a legitimate basis laid down by law (Article 8 Charter of Fundamental Rights in the European Union)
And when such a legitimate basis is proposed how to assess these proposals against the European Convention on Human Rights. How to assess whether such a proposal is necessary in a democratic society in the interests of national security or public safety. How to find that balance between security and data protection?

In April 2004, at the Spring Conference of European Data Protection Commissioners in Rotterdam, Professor Colin Bennett of the University of Victoria proposed not to use the word "balance" anymore. He motivated this by showing that data protection people always seek a balance between subjects that you cannot measure and which are difficult if not impossible to compare. How to compare security with data protection? Which values should be measured and are they measurable? Perhaps Colin Bennett has a good point, but fundamental rights, certainly in conjunction need balancing. But the question remains how and which parameters to use?

Perhaps objective criteria could be of assistance. For example, is the number of terrorists attacks on an annual basis an important element in the discussion whether a legitimate reason exists to introduce more intrusive measures in the fight against terrorism and serious crime ?. If so it is interesting to know that according to US government's figures the most active period of international terrorists activities was in the mid-80s. The year 2003 presented perhaps the lowest (detectable) rate of terrorist activities in Europe. Does this mean that the already improved cooperation between intelligence and law enforcement authorities already created a more secure area in the European Union? And if so why the need for further measures? Apparently these objective figures do not play an important role in the discussion. It is perhaps more the observation that an open democratic society is vulnerable and combined with the notion of fear that seems to stimulate creating more powers and instruments to ensure security. One simply cannot balance fear especially when that fear is perhaps influenced by world politics in a changing world.

Perhaps the only instrument to assess these proposals and to find a balance is the **proportionality** test. And here we stumble on a very specific aspect in the fight against terrorism and serious crime that makes it different from all other data protection issues. One of the core elements of that fight is prevention. This element creates a new dimension in the process of establishing the area of freedom, security and justice, a new dimension that challenges data protection commissioners to deal with the conflicting interests.

Prevention of terrorist activities begins by creating an information position on terrorists. Based on the knowledge available on how terrorists activities are planned, prepared and executed an information position must be established on financing, travel movements, housing, and all other side activities that are connected with preparing a terrorists attack.

Prevention of terrorists attacks thus starts by processing personal data and looking for patterns or identifying persons, processing of data concerning persons that do not yet fit into the category "suspected persons". The present world-wide use of telecommunications, travel and financial data seems to be inevitable.

Basically this is not a new phenomena. Law enforcement authorities already use these methods to fight specific forms of organised crime. The difference however, is the scale in which this takes place. Enormous amount of personal data concerning (at least most of them) innocent people are processed, coming from different private and public sources and without any real grip on what is happening in that process and the further transfer of those personal data. The use of biometric technologies makes it even more intrusive.

The individual right of the presumption of innocence or the basic condition for investigating a person that there must be a reasonable suspicion seems to be eroded by a general concept that within a large group of individuals there might be a terrorist or a criminal and that alone seems to justify that the whole group is subject of law enforcement or intelligence activities.

Is this proportionate? Or is this an aspect of a changing society that we must accept in return for our security. Does prevention of terrorists attacks and of serious crime always lead to a legitimate reason to process personal data? The answer should be a definite no, but we need to use all the ingredients of the data protection models we use and engage in discussion with the policy makers.

Quoting from a speech of Peter Hustinx on Data protection at crossroads, technological change and global challenges can be addressed adequately from the perspective of the European model of data protection but it takes imagination and a co-operative spirit to get inspiration when making the necessary choices to find a sensible direction.

Let me present you one suggestion for such a direction.

If our fundamental right to have security and freedom is really at stake and the world is moving into a direction where prevention of activities that seriously undermine that fundamental right is needed, we should perhaps invest in developing new data protection instruments as an extra data protection weight in the balance. When the interests to balance have such different impact and are so difficult to compare, such an extra weight might support the data protection interests.
Especially in the area of prevention and in view of the possible intrusions in our private life by the processing of enormous amounts of personal data on innocent people, we should perhaps invest in new mechanism establishing a data protection controlled environment for the processing of personal data for prevention purposes.
General data protection principles should be transferred into specific sets of binding rules for intelligence and law enforcement authorities. Rules, tailor made and specifying which data for which specific purposes may be processed. Enhancing the controllability of the controller for example by introducing a compulsory privacy audit on annual basis for intelligence and law enforcement authorities. Perhaps even develop new technologies such as software agents for data protection control purposes. And as a last keystone invest in adequate supervision and ensure liability and legal remedy.
This leads to a situation where measures necessary to fight terrorism and serious crime are processed in a data protection controlled environment.

Perhaps this might contribute in creating the right balance.