SPEECH/07/728

Franco Frattini

European Commissioner responsible for Justice, Freedom and Security

Closing speech on Public Security, Privacy and Technology

Conference on Public Security, Privacy and Technology

Brussels, 20 November 2007, Charlemagne building

Working together

On the occasion of the Data Protection Day on 28 January this year I announced my intention to organize a conference on technology and data protection in the autumn of 2007, and here we are, today, meeting and debating about public security, privacy and technology - a very challenging topic. I would like to thank to all of you for coming to this event and for contributing to its success.

We live in the era of globalisation, and for that reason we welcomed our American partners to consider these issues from a transatlantic perspective.

Although the respective requirements of public security and privacy at times may seem to be in conflict, they are very closely interlinked. And we witness it in everyday life. Today's technology enables information to go around the world in a flash. This technology also enables us to better control access to data, and to pinpoint relevant data. Today's presentations showed that a proper deployment of technology could be a key reconciling security and privacy needs.

Today's debate showed how important it is to continue working together: the public / private sector; the supply / demand sector; the EU and international partners including the USA and national partners, to shape a true European area of justice, freedom and security.

An area of justice, freedom and security is based not only on legislative measures, but also, more importantly, on people's trust both that their fundamental rights will be respected, and their security will be guaranteed. This trust is the very foundation of this whole concept.

Indeed, we must work together, and at all levels. This cannot be done without strong support from our Member States. I am grateful for the importance that the Portuguese presidency is attaching to this work by its activate participation here today.

Security issues are ever-present. Security is a long-term concern. For this reason, developing technologies to enhance security and privacy is vital for long term planning. We have already taken strong action: the Council and the European Parliament have significantly increased funding to meet this new challenge.

Examples of funding:

Under the Fundamental Rights and Citizenship Programme we promote the development of a European society based on respect for fundamental rights. The financing of this programme amounts to 94 million Euros for the period 2007 – 2013.

Concrete projects in the field of data protection and right to privacy to be financed from this Programme in the next year include, for instance, studies on the economic benefits of Privacy Enhancing Technologies (PETs) and studies on developing standards for deployment of PETs. We will also organize seminars for data controllers on the deployment of PETs.

Over the next seven years, almost 750 million Euros will be spent on policies to improve our common security, and support Member States' work in this field.

Nearly one and a half billion Euros is available for security research from the 7th EU Framework Programme on Research, to develop technologies and improve our ability to fight terrorism and crime, secure our infrastructure, border security and civil protection.

Preparatory Action on Security Research (PASR) will enable us to always be few steps ahead in constantly improving security measures.

Public-private dialogue on privacy and security

At present the various parties concerned do not always communicate, or do not communicate sufficiently. This must improve. We must have a shared and clear view of European security research priorities, needs and limits.

Companies, government, industry and universities, to name a few, carry out research. We must avoid doing technology research in isolation from one another.

We must better coordinate research at regional, national, European and international levels. EU funding encourages partnerships.

We must fully involve all stakeholders: Those responsible for providing security; representatives from the Parliaments, from Data Protection Authorities, from the Member States governments and also the executives and the judiciary; civil society and citizens; must all be involved from the very beginning so they can help shape workable policy.

Public-private dialogue to exchange ideas and develop state of the art technology is crucial. In September, the first European Security Research and Innovation Forum was held here in Brussels. The Forum, by bringing together the supply and demand sides of security research and innovation, should ensure the relevance of research results and their use in policy-making.

If each of us better uses security research in policy making, we can deliver more effective policies and ultimately this means better security for all EU citizens.

At the same time, we have to ensure that all our policies respect fundamental rights, such as the right to privacy and the right to the protection of personal data. These are shared values in the EU.

Privacy Enhancing Technologies:

The Communication on Privacy Enhancing Technologies, adopted in May this year, aims at involving a vast array of actors, including the Commission, national authorities, industry and consumers to identify needs and technological requirements for these technologies.

Our aim is to provide the foundation for user-empowering privacy protection services reconciling legal and technical differences across Europe through public-private partnerships. Various stakeholders groups are invited to look into evolving technology to detect any dangers it might pose to privacy and the need to safeguard public interest, such as public security.

We already work with industry. This has brought real results. For example, in increasing the level of security. In the telecommunications sector we agreed last year on new measures to retain data on telephone calls and internet use.

Moreover, industry, especially the ICT (Information and Communication Technologies) industry, as the primary developer and provider of technologies, has a particularly important role to play in developing and designing technologies enhancing both privacy and security and, together with us, shaping how it is used.

Information and communication technologies (ICT) constantly offer new services to improve people's lives. But along with the benefits, new risks for individuals arise, such as identity theft or fraud. Through a good use of technology we could increase security and at the same time enhance protection of privacy and personal data.

Work done already – examples

Border security and Schengen. The Commission's project "Preparatory Action on Security Research" provided research which was useful in developing security policy. In the Schengen area we have removed the necessity to stop at border controls. This enhanced freedom of movement internally necessitates better securing the EU's common external borders. Projects on border security helped us to identify the technical standards needed to improve border security while respecting data protection requirements.

Next year, I will present a Communication on how new technologies can be used for efficient border management. There is a need to identify "overstayers", persons who entered the EU legally, but overstayed their welcome. The time is certainly ripe for thinking about how to replace manual stamping of passports with an electronic system that generates automated alerts.

Data protection and privacy. In the field of privacy and data protection, we work with Member States on proper implementation of the relevant legislation in order to achieve harmonization throughout the EU, and, where necessary, we will launch official infringement procedures so as to ensure a common playing field for all Member States.

We will continue to monitor the implementation of the Data Protection Directive, work with all stakeholders to further reduce national divergences, and study the need for sector-specific legislation to apply data protection principles to new technologies and to satisfy public security needs.

Conclusion

To conclude I would like to repeat that we cannot live without freedom and fundamental rights; nor can we live without security.

People's trust is twofold – our citizens entrust us with the task of protecting them against crime and terrorist attacks; however, at the same, they entrust us with safeguarding their fundamental rights. We cannot risk losing this trust.

This means that any necessary steps we take to enforce security must always be accompanied by adequate safeguards to ensure scrutiny, accountability and transparency.

The protection of fundamental human rights such as privacy and data protection stands side-by-side public safety and security. This situation is not static. It changes, and both values are able to progress in step with technological advances. But it also means that there must be lines which cannot be crossed, to protect people’s privacy.

Today's problems require us to use dedicated technological solutions. We must develop these. We must be innovative. And we must always be a step ahead of criminals, terrorists or those who try to undermine our privacy and security.

Thank you for coming today. And making sure we continue to work together.