Digital Enlightenment Forum

"Personal Data and Citizenship in the Digital Society"

Crowne Plaza, Brussels, 19 September 2013

Day 2: Policy, Visions and Debate - Opening Session

Peter Hustinx
European Data Protection Supervisor

Keynote speech

I welcome the opportunity to contribute to this Digital Enlightenment Forum 2013.

The digital environment in which we are now all living is without any doubt an area of tremendous creativity, innovation and technical accomplishment. However, let me say immediately that more creativity is needed to ensure better digital governance and real citizenship for all in the digital society.

Recent events - now often referred to as the Prism story and similar revelations - have exposed the vulnerabilities of our current digital environment, due to lawful or unlawful monitoring, interception and extensive screening of most, if not all global electronic traffic.

This seems to be a story in instalments, and the details are therefore only developing from week to week.

But the most striking from all we know at this stage are not only the scale and the depth of the monitoring that has been going on, but also the number of private actors, such as well known internet service providers, that have apparently been involved, either actively or passively, and also building backdoors in encryption, with far reaching perverse effects and tremendous

damage to the public trust on which the existence and further development of our digital environment depends.

All this has indeed produced and is still producing shockwaves around the world.

However, we should be aware that these vulnerabilities also stem from other factors, which have grown more gradually over the years, such as the current division of power on the internet, reflecting both its architecture and the economic conditions under which it is functioning.

Another factor is the fact that many people have become used to the availability of free services in exchange for extensive monitoring of their behaviour, almost on a permanent basis. Not everyone is fully aware that free services do not exist in reality. This has now created the basis for the wide scale involvement of private actors in public sector monitoring.

What we observe is a paradigm shift - where confidentiality of communication was - not so long ago - a strong principle and a carefully guarded practice, we now see transparency of communication developing, even being celebrated by some, and all without any constitutional change, or any kind of informed debate. Indeed, it seems mainly driven by fashion and by fascination for technology and ease of living.

However, it remains true that digital trust in the years ahead crucially depends on our capacity to provide legal and technical infrastructures that can generate and preserve trust based on widely shared principles and practices of good citizenship in the Digital Society.

The EU is now engaged in an ambitious review to update its current legal frameworks for privacy and data protection, in order to make them more effective in practice and more consistent across the EU. This is based on a recognition of those concepts as fundamental rights in the European Charter of Fundamental Rights, which the Lisbon Treaty has made binding, not only for EU institutions and bodies, but also for member states, when acting within the scope of EU law.

Making data protection more effective in practice means stronger rights for data subjects, stronger responsibilities for organisations using personal data and stronger supervision and enforcement by data protection authorities. The proposed Regulation which is to replace the

current Directive will provide for much more consistency across the EU. It will apply to all those who offer their goods or services on the European market and therefore provide a more extensive level playing field than the current legal framework.

Commission, Council and Parliament are working very hard to deliver this new legal framework before the European elections in the spring of 2014. The LIBE Committee of the Parliament will vote on its report within a few weeks from now. After that vote we will probably see extensive efforts to come to a common text that will find support in Council and Parliament. I am confident that this will happen within the time available.

Adoption of this new legal framework will make it possible that excessive tracking and tracing, monitoring and profiling of behaviour on the internet are addressed more effectively than is the case now. This will also provide more weight against current trends on the internet and can begin to help restore a more acceptable balance of interests and build more trust in this environment.

Industry practices based on Privacy by Design, transparency and accountability should follow these efforts. Make no mistake: it is neither possible nor desirable to "regulate" innovation, but the law can create the right responsibilities and allocate the right incentives, and that is exactly what the new legal framework will do.

The question to what extent governments and entities acting on their behalf should be allowed to intercept electronic traffic, and if so under what conditions and safeguards, should also be addressed, and certainly at all relevant levels, but as a separate matter.

The case law of the European Court of Human Rights is crystal clear on this subject and goes back several decades. It applies to all member states, and can also help to inspire discussions across the Atlantic when the time is ripe to make progress in this field as well.