SPEECH/11/183

Viviane Reding

Vice-President of the European Commission
EU Justice Commissioner

Your data, your rights: Safeguarding your privacy in a connected world

Privacy Platform "The Review of the EU Data Protection Framework"

Brussels, 16 March 2011

Ladies and Gentlemen,

I am delighted to address the Privacy Platform to discuss the reform of data protection rules in the European Union. I am pleased to see that the European Parliament is taking a proactive approach to the reform, which is my top legislative priority.

Our Charter of Fundamental Rights and our Treaty make it clear that everyone has the right to the protection of personal data. This right is particularly important in today's world – a world in which rapid technological changes allow people to share personal information publicly and globally on an unprecedented scale.

While social networking sites and photo sharing services have brought dramatic changes to how we live, new technologies have also prompted new challenges. It's now more difficult to detect when our personal data is being collected. Sophisticated tools allow the automatic collection of data. This data is then used by companies to better target individuals. Public authorities are also using more and more personal data for a wide variety of purposes, including the prevention and fight against terrorism and serious crime.

The question today is how the Commission will ensure that privacy rights are put into action. I am a firm believer in the necessity of enhancing individuals' control over their own data.

Peoples' rights need to be built on four pillars:

The first is the "right to be forgotten": a comprehensive set of existing and new rules to better cope with privacy risks online. When modernising the legislation, I want to explicitly clarify that people shall have the right – and not only the "possibility" – to withdraw their consent to data processing. The burden of proof should be on data controllers – those who process your personal data. They must prove that they need to keep the data rather than individuals having to prove that collecting their data is not necessary.

The second pillar is "transparency". It is a fundamental condition for exercising control over personal data and for building trust in the Internet.

Individuals must be informed about which data is collected and for what purposes. They need to know how it might be used by third parties. They must know their rights and which authority to address if those rights are violated. They must be told about the risks related to the processing of their personal data so that they don't loose control over their data or that their data is not misused. This is particularly important for young people in the online world.

I want to make sure that greater clarity is required when signing up to social networking. Unfavourable conditions – restricting control of users over their private data or making data irretrievably public – are often not clearly mentioned. In particular, children should be fully aware of the possible consequences when they first sign up to social networks. All information on the protection of personal data must be given in a clear and intelligible way – easy to understand and easy to find.

The third pillar is "privacy by default". Privacy settings often require considerable operational effort in order to be put in place. Such settings are not a reliable indication of consumers' consent. This needs to be changed.

The "privacy by default" rule will also be helpful in cases of unfair, unexpected or unreasonable processing of data – such as when data is used for purposes other than for what an individual had initially given his or her consent or permission or when the data being collected is irrelevant. "Privacy by default" rules would prevent the collection of such data through, for example, software applications. The use of data for any other purposes than those specified should only be allowed with the explicit consent of the user or if another reason for lawful processing exists.

The fourth principle is "protection regardless of data location". It means that homogeneous privacy standards for European citizens should apply independently of the area of the world in which their data is being processed. They should apply whatever the geographical location of the service provider and whatever technical means used to provide the service. There should be no exceptions for third countries' service providers controlling our citizens' data. Any company operating in the EU market or any online product that is targeted at EU consumers must comply with EU rules.

For example, a US-based social network company that has millions of active users in Europe needs to comply with EU rules. To enforce the EU law, national privacy watchdogs shall be endowed with powers to investigate and engage in legal proceedings against non-EU data controllers whose services target EU consumers.

Stakeholders at a recent public consultation on data protection asked me to make clear that our data protection rules also apply to data retention. Storage of data is already included in the broad definition of "processing" but the general public is unaware that processing includes storing / retention.

One of the grounds for data retention is law enforcement. This brings me to the role of the police and judicial cooperation in criminal matters and the data protection rules that should be applied in this area to eliminate any potential gaps and inconsistencies and to ensure a high level of protection.

The EU Charter of Fundamental Rights lays down the basic principles for the protection of personal data for everyone in Europe. This includes the rights of people whose data may be required by law enforcement authorities in a variety of circumstances: bank transfers, buying an airline ticket, checking in and passing security checks at the airport, surfing the Internet or sending emails and making phone calls.

In all these cases we are talking about collecting bulk data: vast amounts of personal information on innocent, law-abiding citizens. This collection of data, which is usually carried out by private companies primarily for business and contractual purposes, may then also be used by public authorities for the purpose of investigating terrorism and serious crime.

One important change following the introduction of the Lisbon Treaty is that the Commission can now consider extending the general data protection rules to the areas of police and judicial cooperation in criminal matters. Limitations to rights in this area would need to comply with the general rules, and be clearly defined and proportionate. This is an important part of my reform.

Last but not least, allow me to mention a very important point: enforcement. To be effective, data protection rights need to actually be enforced! To make this possible I want to reinforce the independence and harmonise the powers of national data protection authorities in our 27 Member States.

Cooperation between the data protection authorities of different Member States also needs to be improved. In particular, I am referring to cases with a clear cross-border, European dimension. In recent months, you may have heard about concerns in many EU Member States related to online mapping services including pictures of streets and people's homes. A more coordinated approach at EU level is needed to address such cases in a consistent and effective way.

Our data protection reform will be key in adapting the rules to the all-encompassing digital world in which we live. I look forward to cooperating closely with Mr Voss and all Members of the European Parliament on this matter, which is of great importance both for citizens and businesses. I take this meeting as an important step for further discussions with the Parliament.

Taking your input into account, I want to present legislative proposals this summer. I look forward to hearing from you and hopefully to receiving your support.

Thank you!