SPEECH/

Viviane Reding

Vice-President of the European Commission, EU Justice Commissioner

Outdoing Huxley: Forging a high level of data protection for Europe in the brave new digital world

Digital Enlightenment Forum

Luxemburg, 18 June 2012

Ladies and gentlemen,

I am delighted to have the opportunity to speak to you today. The issues that will be addressed at the conference, about privacy, about technological change, about the future of the Web are of fundamental importance. They are also at the heart of the data protection reform proposals that the European Commission adopted at the end of January. I know that many of you have been following this important subject closely.

The backdrop to this debate is clear.

The world has changed profoundly since 1995 – the year the existing EU data protection framework was adopted. We now live in a world of immense communication possibilities. We can update our friends and family on our every move and real time. We have access to an infinite pool of knowledge through highly refined search engines and we can entrust our private data to a cloud service provider without ever having to worry about storage space.

Our current data protection rules already contain solid data protection principles. But they were drawn up in 1990 and adopted in 1995, when only 1% of the EU population was using the Internet. In 1995 a 28.8 Kilobytes per second modem cost more than 500 euros, Amazon and eBay were still being

launched and the founder of Facebook was only 11 years old! It would still be 3 years before the arrival of Google and other household names. But gone are the days of mobile phones the size of bricks and punched card computer programming! Today, just as your computing operating systems and smartphones need regular updates to take new technological developments into account, our data protection rules also needed to be modernised. So we are updating our rules to ensure that they continue to protect individuals in this brave new digital world.

And we are updating them to make it easier for companies to take advantage of our digital single market with its 500 million potential customers. The prospect of the increase in growth and competitiveness that could flow from these changes is enormous. Thanks to information technologies, cloud computing and seamless logistics, there is now a market of more than 2 billion internet users and more than one billion smart phone users worldwide. This brings with it a huge potential for growth - We in Europe must harness this potential.

For us policy makers, and for businesses that handle personal information, this is a real challenge. How can we ensure the protection of data in a world of total connectivity? How can we nurture consumer confidence in a world of exploding data volumes? How can we reconcile privacy and digital growth, the rights of individuals and the needs of business?

A number of these questions will be discussed in your panels. The development of technology and the law. The role of data protection for privacy. The trusted provision of services in the cloud. These are all questions that the Commission addresses in the newly proposed data protection Regulation.

Today, I would like to contribute to your debate by explaining why I think Europe needs to guarantee a high standard of data protection. For the citizens of Europe, of course. But also for citizens beyond Europe's borders. A high level of data protection will turn the European Union into an international standard setter that will improve internet governance worldwide. The digital Single Market will also benefit. Only a high level of data protection will generate trust between citizens and private enterprises.

However, we must be very careful how we develop these rules. We must act with the right firmness of touch, tailoring the rules we introduce to the needs of Europe in the 21st century. We cannot introduce rules that place an excessive burden on business. Nor should our concern with privacy blind us to the need to respect other rights.

A high level of data protection

Data protection is a very important fundamental right in the EU. The reason for this is rooted in our historical experience with

dictatorships from the right and from the left of the political spectrum. They have led to a common understanding in Europe that privacy is an integral part of human dignity and personal freedom. Control of every movement, every word or every e-mail made for private purposes is not compatible with Europe's fundamental values or our common understanding of a free society. This is why the Union's Charter of fundamental rights recognises both the right to private life in Article 7 and the right to the protection of personal data in Article 8. But this is not all: Article 16 of the Treaty on the Functioning of the European Union also gives the European Union the legislative competence to establish harmonised EU data protection laws that apply to the whole continent and that make the right to data protection a reality. Data protection is thus one of the rare fields where we have full coherence between the fundamental right and the EU's legislative competences of the EU. This makes data protection a particularly powerful fundamental right in the European Union, and the Commission's proposals from 25 January have been designed to put this right into practice everywhere in our internal market.

These principles are reflected in my proposals. I have sought to ensure a high level of data protection in three ways.

First, the Commission has delimitated clear responsibilities and accountability for those processing personal data. In the

Regulation, we have included incentives for controllers to invest, from the start, in getting data protection right. For example, we have foreseen data protection impact assessments, data protection by design and data protection by default. These principles encourage data controllers to think about data protection from the very beginning when designing new applications or services.

Second, we have strengthened citizens' rights. The new rules clarify the notion of consent and have introduced a general transparency principle. There is an obligation to notify clients of data breaches, which will apply to all sectors. The "Right to be forgotten" is an important pillar of the proposals. It empowers users, under certain well defined conditions, to ask a company to delete personal data they have given said company. Citizens will also be able to transfer their data from one service provider, such as a social network, to another – just as they are able to keep their mobile number when changing telecoms operators. Choice drives competition. For me, the "Right to data portability" is a modern way of putting the principle of it being the individual who decides what happens to his/her data into practice.

By choosing a Regulation the Commission is establishing uniform rules for data protection everywhere in Europe. But, as everyone knows, what is the use of uniform rules if they are not

enforced? In the interest of legal certainty and of fair competition, we have introduced a one-stop-shop system.

For the consumer, this means that they will always turn to their national data protection authority when they have a problem with a company – no matter where the company is based. They will not have to labour through the process of contacting authorities in different EU countries, riddled as it is with problems of different languages or procedures. We make things easy for the consumer.

The same un-bureaucratic one-stop-shop exists for companies as well. They will only have to deal with one data protection authority: in the country in which they have their main establishment. This cuts costs while increasing legal certainty.

In the end, it will not matter which data protection authority deals with a citizen's complaint or a company's case. Why? Because what the Commission has proposed is one single rule for the entire European continent. Each case will be decided on the basis of this single law – the same for all 27 EU countries – guaranteeing that the outcome will be the same, no matter which data protection authority is in charge.

For this to happen we need to be sure that in cross-border situations, national data protection authorities cooperate closely, reliably and quickly. We have put in place a so-called

"consistency mechanism" that is currently being tested for the first time - by the national data protection authorities investigating Google's new privacy policy.

European countries are interconnected. Data flows across borders as easily as the air we breathe. There is no single national or even regional authority that can protect its citizens effectively on its own when we are facing the challenge of cross-border online services. Today we are bearing witness to closer cooperation and coordination between Member States when it comes to their economic policies. The same logic should be applied in the field of data protection: national regulators in Europe need to cooperate more to make sure there are no data protection loopholes which can be exploited to the detriment of our citizens.

So you see, these are some of the ways in which my proposals will protect and empower European citizens in the 21st century.

A worldwide influence

But the benefits of a high level of data protection do not stop at Europe's door. They will also be felt outside the Union. I believe my proposals already have and will continue to have an influence worldwide.

Data flows don't stop at national borders, and they don't stop at the borders of our continent either. Our personal data is increasingly stored on servers located in California, the Caribbean or in the Cloud. Any trip by aeroplane can result in personal passenger data being exchanged worldwide. Any bank transfer can trigger the access of foreign companies or government agencies.

With our new proposals and our willingness to push for a high level of data protection, Europe is taking the lead in responding to the concerns of individuals worldwide about their personal data.

First, our rules will apply to any data controller which offers goods or services to an individual residing in the EU. It will make no difference whether the data controller is established within the European Union or not.

Second, the European Union is setting the agenda of the political debate across the globe. I will follow with interest the way the U.S. Congress will act on the policy principles set out by President Obama, four weeks after our European proposals, in the paper on "Consumer Data Privacy in a Networked World". In this context, I have also taken note of the interest that NGO's and other stakeholders in the U.S. are showing in these

proposals and the fact that they are urging the U.S. Congress to pass legislation to protect peoples’ rights.

Trust in data processing

The benefits of a high level of data protection within the European Union can be measured not just in terms of citizens' rights. Personal data has become a highly valuable asset. The market for analysis of large sets of data is growing by 40% per year worldwide. The currency of this new digital economy is data and in many cases personal data.

But the free flow of any currency depends on a precious commodity: Trust. It is only when consumers can 'trust' that their data is well protected that they will continue to entrust businesses and authorities with it by buying online and accepting new product developments and services.

And trust is waning. 70 percent of European citizens are concerned that their personal data held by companies may be used for a purpose other than the one for which it was collected.

This trend needs to be reversed. Reliable, consistently applied rules make data processing safer, cheaper and inspire users' confidence. Confidence in turn drives growth.

Developing the Digital Single Market

Indeed, in drawing up our rules on data protection, we mustn't lose sight of the economic implications of the reform.

The modernisation of the European data protection laws should strongly stimulate the development of the digital economy across the EU's single market. The current Directive from 1995 resulted in 27 different and often contradictory data protection rules - A real patchwork in terms of requirements and standards that has led to unnecessary financial burdens and administrative red tape.

The current differences affect the competitiveness of European companies. A directly applicable Regulation, on the other hand, will greatly reduce legal fragmentation and provide legal certainty by introducing a harmonised set of rules and contributing to growth and the functioning of the internal market.

The fact that there will be one single law and one single national Data Protection Authority responsible in each case will greatly simplify the legal environment. We have calculated that thanks to this simplification companies will save around € 2.3 billion per year – this is certainly not peanuts.

Small and medium enterprises

The goal of stimulating economic growth would be frustrated were the Regulation to impose an additional burden on European business.

In calibrating the level of data protection provided for by the Regulation, we have taken account of this factor. We have paid special attention to the needs of small and medium sized enterprises. We must ensure a high level of data protection but we cannot sacrifice growth at the altar of data protection.

Although the data protection law should and will apply to all companies, there are several provisions that we have incorporated to make life easier for SMEs. For example, all companies that employ fewer than 250 employees are exempt from the obligation to appoint a Data Protection Officer. Let me give you a second example: Small and medium-sized enterprises are exempt from the obligation to document their data processing, provided that data processing is not their main activity.

So you see, the European idea of 'thinking small first' runs throughout our whole proposal. Europe is a continent of SMEs: 99% of our companies are SMEs. We need to help them become big – so that the next Google can be European!

Data protection and other fundamental rights

Let me end with another of the delicate balancing acts our Regulation seeks to strike: finding the right balance between the fundamental right to privacy and other fundamental rights.

We are now living in a society with multi-layered networks, and as human beings we have multiple social contacts. As an active member of society and its communication networks, we cannot claim a right to total privacy. Just as you cannot force your neighbour to forget that he saw you in the local shopping centre yesterday, you cannot enforce an absolute right to be forgotten on the internet.

In effect, data protection is a fundamental right that can easily collide with other fundamental rights. A very important practical constellation is a possible conflict with the freedom of the press.

Say, for example, a journalist wants to write an article about a film star and to publish photos about the film star sunbathing on a beach in the South of France. But the film star wants her privacy to be respected. How to solve such a conflict between privacy and freedom of the press? We discussed this extensively in the Commission before the proposals were made. We found that freedom of the press is still regulated in a rather different way across the 27 Member States. Some give it a higher importance than others. Some have explicit freedom of

press laws, others not. The EU has no competence at all to establish laws on the freedom of the press. Under the Treaties, Member States have exclusive competence over this.

However, the EU legislator cannot ignore the possible conflict between data protection and the freedom of the press. We therefore included a clause in the new Data Protection Regulation which requires Member States to provide for exemptions or derogations from certain provisions of the Regulation in their national laws, for data that are processed "solely for journalistic purposes". We are thus allowing Member States to create rules to reconcile the right to the protection of personal data with the rules governing freedom of expression.

This is certainly a difficult balancing act, and one that can only be achieved in the knowledge of the specific details of each individual case and the specific national circumstances. In short, the right to be forgotten is not an absolute right, it is a relative right. Like the general right to privacy, it is a right that needs to be reconciled with other rights which are also protected by the EU's Charter of Fundamental Rights.

Member States and national data protection authorities will play a crucial role in helping to get this balancing exercise right. Together we can be a winning team. Maybe a bit bigger than a

soccer team but certainly motivated and well equipped to meet the challenges of this brave new digital world!

Conclusion

The Digital Enlightenment Forum brings together civil society, academia and business. With your help, I hope that we will soon have a strong and coherent framework for data protection. A legislation that is fit for the digital age, for people, for businesses, for our economy and for our society. This is a joint endeavour and I am grateful for your support.