

Viviane Reding

EU Justice Commissioner

EU data protection reform and social media: Encouraging citizens' trust and creating new opportunities

Check Against Delivery
Seul le texte prononcé fait foi
Es gilt das gesprochene Wort

Economist conference "New frontiers for Social Media Marketing"

Paris, Tuesday 29 November 2011

Ladies and gentlemen,

I am delighted to speak at this conference on social media marketing today. As you probably recall, I previously served as the European Commissioner for Information Society and Media. At that time, we laid the foundations for what is now Europe's Digital Agenda – the EU's action plan for enabling our digital future. So I'm very aware of the challenges the digital environment poses, but also the benefits it can bring.

We are facing completely new ways of doing business online, new sources of revenue, new ways of interacting, of exchanging information and services among businesses. These innovations are of vital importance for the digital economy. In these times of crisis, we need to encourage innovation to get the economy moving.

This is clearly a challenge for traditional media. They may have to reinvent themselves to find and maintain their brand in this changing environment. This is also a challenge for me, as the European Commissioner for Justice and Fundamental Rights: how can we make sure that the fundamental rights of people continue to be protected in the age of digital advertising?

In today's digital environment, the scale of data sharing has increased dramatically: Vast amounts of personal data are transferred and exchanged every day, across continents and around the globe in fractions of seconds. In this ever increasing connectivity, online advertising has become a key source of income for a wide range of online services. It has become a crucial factor for the growth and expansion of the internet economy.

Many people say, and perhaps rightly, that without online advertising, the internet would have evolved into something very different from what we know today. The evidence for the importance of online advertising in the development of the World Wide Web is quite clear. Recent data¹ puts estimated advertising expenditure in 2009 at €14.7 billion in Europe and €16.3 billion in the US – this is an economic contribution we cannot afford to ignore.

But, of course, I am preaching to the converted here about the importance of online advertising! I would like to make a different point: For digital advertising to continue to grow, it needs the right set of rules. To create growth, we have to encourage trust in emerging technologies, so that citizens feel comfortable using them. The full potential of cloud computing, for example, can only be realised if users see it as a trusted way of storing data. Consumers are hesitant to buy online or accept new digital services if they lack trust.

I strongly believe that privacy is key for a continuous growth of the internet economy. Stronger, more coherent data protection rules will encourage trust. Fostering this environment of trust is also in the economic interests of advertisers.

I don't have to tell you that some practices, such as behavioural advertising, have raised serious concerns about data protection and privacy.

Concerns about transparency, in terms of the practices used when processing personal data in online behavioural advertising; concerns about how well informed users are about the processing of their data; and concerns about whether users are offered the chance to give meaningful consent, particularly if they are not well informed.

Often, people are not aware of the harvesting of personal information taking place while they are online. They don't know who is collecting data, and for what purpose. When people sign up for an online service, are they aware that they have given permission to have their data shared with advertisers? It is not always clear whether

¹ from IAB Europe

individuals have meaningfully consented to their online movements being tracked across the web, and to being the recipients of behavioural advertising. People are often surprised that their preferences, location and buying history are being shared with advertisers. This is not an environment in which we can easily gain the trust of users.

We Europeans place a high value on privacy and data protection: they are our fundamental rights. That is why we have put in place laws and regulations to guarantee data protection and privacy.

The EU's current data protection legislation was adopted in 1995, when the full potential of the internet had not yet been realised. Although the basic principles and objectives of the 1995 Directive remain valid, these rules must be adapted to this new challenging environment. We must ensure a high level of protection for individuals and enable the free movement of personal data across the borders of EU Member States, whatever challenges the digital age might create for us.

The reform will address challenges to privacy and data protection created by recently emerging practices and technologies, such as online behavioural advertising and social networking sites. The framework for data protection must be future proof. It is important that personal information remains protected, no matter what technology we are using in ten, fifteen or even thirty years.

So what are the main aims of the data protection reform?

Firstly, I want to put individuals in control of their data. With social networking sites, cloud computing, location-based services and smart cards, we leave our digital footprints everywhere. I want to improve the effectiveness of the fundamental right to data protection and ensure that individuals are always in a position to take informed decisions about how their personal data is used.

Secondly, I want to create a level playing field for companies in the EU and a more business-friendly regulatory environment. Inefficient data protection regulation holds back businesses. I want to simplify the situation and eliminate unnecessary costs and administrative burdens. If we want to encourage businesses to take advantage of new technologies and operate across borders, we need to make it simpler.

Finally, I want to enhance the coherence of the EU data protection framework. Following the entry into force of the Treaty of Lisbon, we need also new rules for data protection in the area of police cooperation and judicial cooperation in criminal matters.

How will we achieve those objectives?

To create a more business-friendly regulatory environment, we need to drastically cut red tape. This means doing away with the general requirement to notify data processing to data protection authorities. Instead, I will focus on those requirements which enhance legal certainty and are of real value.

I also want to provide consistency and coherence. We need legal certainty and a level-playing field for all businesses that handle EU citizens' data. At the moment, firms processing personal data in several Member States are subject to different laws and decisions. The administrative burden associated with this fragmentation costs businesses an estimated 2.3 billion euros per year. In the new rules, one law would be applicable and one single authority would be responsible for companies operating in several Member States.

The authorities responsible for data protection must be provided with sufficient powers to enforce the law and they must have sufficient resources to exercise their

powers. At the same time, we must strengthen coordination and cooperation between national data protection authorities to make sure that the rules are enforced consistently. As a result, companies will be able to sell goods and services under the same data protection rules to 500 million people, a fantastic business opportunity!

But what about outside the EU's internal market? The existing data protection rules apply to all businesses having an establishment or data processing operations in the EU and not just to European companies. Companies operating in Europe and elsewhere find that a high level of protection for personal data is a necessary condition to establishing a trusted relationship with their customers.

In a world where the free flow of data is imperative for our global businesses and physical boundaries are meaningless, we also need to rethink the way we transfer data. I want to improve the current system of binding corporate rules to make this type of exchange simpler and less burdensome and to cut down on the time and money invested by companies.

These are the ways in which the new rules will help businesses. But I also expect businesses and other organisations to do their share. As part of the reform, we also need to increase the effectiveness of the fundamental right to data protection and put individuals in control of their information. And this is where the responsibilities of businesses come in.

What does this mean in practice?

Firstly, businesses must ensure transparency for individuals, who must be provided – in a simple and understandable language – with appropriate information about the processing of their data.

Users must be told 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 should be put in a position to make informed decisions about when to disclose their personal information.

Secondly, this responsibility means that whenever users give their agreement to the processing of their data, it has to be meaningful. In short, individuals should be well informed about privacy policies and their consent needs to be specific and given explicitly.

Thirdly, this responsibility means that individuals should be swiftly informed when their personal data is lost, stolen or breached. Frequent data security breaches risk undermining consumers' trust in the digital economy. Our proposal will introduce a general obligation for data controllers to notify data breaches. In concrete terms, that means notifying data protection authorities and the individuals concerned when a data breach is discovered.

Finally, this responsibility means giving individuals better control over their own data: that's why the reform will include easier access to one's own data which should be free of charge as a general principle.

More control for citizens can be created with better data portability. If users request their data (photos, agendas...) back, it should be given to them in a widely used format which makes it simple to transfer elsewhere. I strongly believe that users should not be bound to one provider simply because it is inconvenient to move their information from one service to another.

I also want to create a right to be forgotten, which will build on existing rules to better cope with privacy risks online. The current Directive already gives individuals the possibility to have their data deleted, in particular when the processing is

unlawful. I want to explicitly clarify that people shall have the right – and not only the "possibility" – to withdraw their consent to the processing of their personal data.

I know that there has been some concern about this, but I want to emphasise that the right to be forgotten is not intended, or able, to act as a form of censorship. It is simply a safeguard to ensure that when an individual no longer wants their personal data to be processed, and if there is no legitimate reason for an organisation to keep it, it should be removed.

These are the main elements of the data protection reform that I will propose early next year.

I am confident that the new rules will live up to businesses and citizens' expectations: to have a strong, consistent and future-proof framework for data protection. Europe's data protection rules must and will continue to guarantee a high level of protection and provide legal certainty to businesses, public authorities and individuals alike for generations to come.

I have no doubt that the European Union will continue to lead in setting the standards for personal data protection, as it has done for the past 15 years.

Thank you!