LSE European Institute-APCO Worldwide Perspectives on Europe series in association with the Law Department

The importance of strong data protection rules for growth and competitiveness

Viviane Reding
Vice-president of the European Commission, EU Justice Commissioner

London School of Economics and Political Science

Thursday 1 March 2012

Check against delivery
http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/171&format=HTML&aged=0&language=EN&guiLanguage=en

---

Ladies and gentlemen,

I would like to thank the London School of Economics European Institute and Department of Law for their invitation to come to London to deliver this lecture.

Today I would like to present and discuss with you the data protection reform proposals that the European Commission adopted at the end of January. I know that many of you have been following developments on this important subject very closely.

My starting point is to state the obvious. The world has been turned upside down since the existing EU data protection framework was adopted in 1995. We now live in a world of immense communication possibilities. We can update our friends and family with what we are doing the moment something happens, sending photos and information at the tap of a finger. We can access infinite knowledge through highly refined search engines that trawl the Internet. Or we can entrust our private data to a cloud service provider without having to worry about storage space.

And this revolution is not over. It is just beginning. Smartphone applications will soon be able to constantly monitor our health though, for example, blood pressure. We can already see the potential for car positioning systems which report traffic jams and communicate with cameras to direct drivers onto optimised routes, saving time and fuel. Then there are the smart grids, which will combine with smart meters and smart appliances to help us save energy.

The prospect of an increase in growth and competitiveness that flows from these changes is enormous. These technological developments are welcome drivers of innovation, growth and job creation. They also mean that we live increasingly in a "global village". Thanks to IT 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 a huge potential for growth; we in Europe must harness this potential.

The currency of this new digital economy is the free flow of data. The Internet, cloud computing, and mobile devices allow us to access our data on the go wherever we are in the world. In 1993, the Internet carried only 1% of all telecommunicated information. Today, the figure has risen to

more than 97%, and this is only the beginning. Personal data has become a highly valuable asset. The market for analysis of large sets of data is growing by 40% per year worldwide.

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, buy online, and accept new product developments and services.

For us policy makers, this is a real challenge. How to ensure the protection of data, and thereby to nurture consumer confidence, in a world of total connectivity and exploding data volumes? The challenge for data protection and privacy is sizeable. To tackle it, the public and private sector must work together. Why? Because we are no longer talking about individual devices but about very complex and interconnected public and private systems.

And let's face it, the way we have so far addressed privacy in this totally connected environment is not fully satisfactory. As policymakers, we have taken too fragmented an approach.

At a lecture in Brussels last month, Samuel Palmisano, the CEO of IBM said that "the data explosion combined with a new level of data integration is a revolution". I agree with him. Mister Palmisano made a point that I share:

The new level of integration we have now thanks to cheap communication, cheap sensors and mobile devices, **can only work with higher standards, and with more expertise infused into public policies**. Without this expertise, neither political nor technological integration can work, and the benefits will be fragmented.

But all of this presupposes that people care about data protection. So, are people concerned about how their data is used? Do people mind if their data is sold on to third parties? Do people even care whether their data is protected?

The answer is simple: Both in the UK and all across Europe, people do care.

80 percent of British citizens are concerned that their personal data held by **companies** may be used for a **purpose other than that for which it was collected**. The European average is 70 percent. And almost half of British Internet users are concerned about falling victim to online fraud or identity theft.

This is not surprising given the long list of recent data breach scandals in the UK.

The Internet economy will continue to grow exponentially under one pre-condition: that people's trust in the Internet prevails. And that will be quite an achievement: 79 percent of British Internet users buy goods and services online (EU average: 60 percent). Yet a quarter of British online shoppers feel they have no control at all over the data they disclose when shopping on the Internet.

These figures explain why the European Commission's data protection reform is an important part of our long-term growth strategy, Europe 2020: it can unleash the potential of the Digital Single Market. How?

In the first place, I've proposed a Regulation, meaning one single law, one single set of rules, applicable to all businesses and public authorities in the whole of Europe. The existing Directive has brought with it 27 different, and often contradictory, regimes. A Regulation will bring an end to the fragmented application of the rules. This fragmentation not only imposes extra costs, it also holds back economic growth and innovation.

I have also taken the decision to set up a **one stop shop** for data protection – instead of having to deal with authorities in all Member States in which it is active, a business will now have a single contact point. The national Data Protection Authority where the business has its main establishment.

This is of course a major simplification for businesses. It is also important from the perspective of the data subject or consumer, who still can turn to his local body to get a problem solved wherever it has arisen in Europe. All data protection authorities have a common interest to see that the Regulation is applied in a **coherent and consistent manner**. There will be mechanisms

to ensure that data protection authorities in Europe will work closely together to tackle cross border cases, as already happens in competition law or in the telecoms sector. Each national authority must have sufficient resources. And each will get a set of strong sanctions powers to deter non-compliance.

Finally, the new rules will **cut red tape for businesses**. Under the current rules, companies face cumbersome and costly general notification requirements for processing data. We will scrap these and make companies integrate a responsible risk assessment and data protection culture.

In order to help start-ups and SMEs to concentrate on their core business, I integrated the "**think small first**" principle into the proposal. That means that Small and Medium Enterprises will not be subject to heavy requirements.

Overall, the Commission estimates **net savings** for businesses amounting to about **€ 2.3 billion per year – around £1.9 billion** – in administrative burdens.

Stimulating growth is not only about completing our internal market. It is also about making our internal market standards a global benchmark. How will these rules strengthen the position of Europe in the global village?

With clearer rules and better enforcement, we can be confident that our data is protected inside the EU's borders. But what if the data goes out of Europe?

The new rules will apply to **all** controllers established in the European Union. They will also apply to all those offering services and products to individuals in the European Union, whether they are established here or not. Europe represents a huge market for foreign companies: our new rules will make that market borderless. **One set of rules for one continent**.

International transfers of data should be easy and they should be safe. For this reason, the new rules allow a company based in the European Union but with subsidiaries across the globe to establish so-called "binding corporate rules". Binding Corporate Rules are a corporate code set up within an organisation or group of organisations, which allows data to be transferred worldwide with full legal certainty. It also means that their customers' personal data is fully protected, and that redress is available if there is a problem.

How can a change in data protection rules give people more confidence in Europe's digital single market?

First, the reform will reinforce transparency requirements. People need to be **informed** about the processing of their data in simple and clear language. Today, hundreds of pages of technical jargon make many privacy policies unreadable – and that is not acceptable. In the future, internet users must be told which data is collected, for what purposes and how long it will be stored. 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. People need to be able to make an informed decision about what to disclose, when and to whom.

Second, whenever users give their agreement to the processing of their data, it has to be meaningful. In short, their **consent** needs to be specific and given explicitly.

Thirdly, individuals must be swiftly **informed** when their personal data is lost, stolen or hacked. Whether user data gets stolen from an online gaming service, or credit card details are hacked on a firms' website: these security breaches affect millions of users around the world. We all remember last year when it took weeks for users to learn that their credit card information had been compromised following a data breach in an online video game. Serious incidents like these highlight why companies need to reinforce the security of the information they hold. Frequent data security breaches risk undermining consumers' trust in the digital economy. I will therefore introduce a **general obligation for data controllers to notify of data breaches**. Companies that suffer a data leak must inform the data protection authorities and the individuals concerned, and they must do so without undue delay. That normally should mean "within 24 hours".

Finally, the reform will give individuals **better control** over their own data. I will include **easier access** to one's own data in the new rules.

The new rules will provide for **data portability**. If a user wants to take her holiday pictures off a photo-sharing website and upload them somewhere else she should be able to do so. Consumer choice is key to effective competition.

Another important way to give people control over their data: **the right to be forgotten**.

The Internet has an almost unlimited search and memory capacity. So even tiny scraps of personal information can have a huge impact, even years after they were shared or made public. The right to be forgotten is not new. It builds on already existing rules which are unfortunately not clear, nor adapted to the internet age. It is the individual who should be in a position to protect the privacy of his data by choosing whether or not to share it. Under the new rules, people will have the right – and not only the 'possibility' – to withdraw their consent to the processing of the personal data they have given out themselves. This is what we call "A right to be forgotten".

The available figures speak for themselves: almost three quarters of British internet users would like to have the possibility to have their personal data deleted from a website whenever they decide to do so. If an individual no longer wants their personal data to be processed or stored on a website or a server, and if there is no legitimate reason for keeping it, the data should be removed from the system.

The right to be forgotten is, of course, not an absolute right. There are cases where there is a legitimate and legally justified interest to keep data in a database. The archives of a newspaper are a good example. It is clear that the right to be forgotten cannot amount to a complete erasure of history. Neither must the right to be forgotten take precedence over the right to freedom of expression. The independence of the press and freedom of expression are cherished rights in Europe. Let me say it very clearly: the right to be forgotten is not a right to censorship.

That is why the new data protection rules are carefully drafted to make sure that the balance is right. They include **explicit provisions on the freedom of expression** and information. Data protection is a fundamental right, but it's not the only one that must be protected.

Ladies and gentlemen,

I am not alone in identifying the need to give internet users a right to control how their personal data is used. The same observations are being made on the other side of the Atlantic. Last week the Obama Administration unveiled a "Consumer Privacy Bill of Rights" as part of a first outline to protect individual privacy rights and give users more control over how their information is handled. It shows that the USA is now following our path.

In the totally connected world of exploding data flows, we need to set a high standard for data protection. The data protection reform that is now on the table will secure Europe's place as a standard setter in the digital age. Standards that protect citizens, but that also help businesses to navigate the exciting new potential of the digital economy.

Thank you.

END