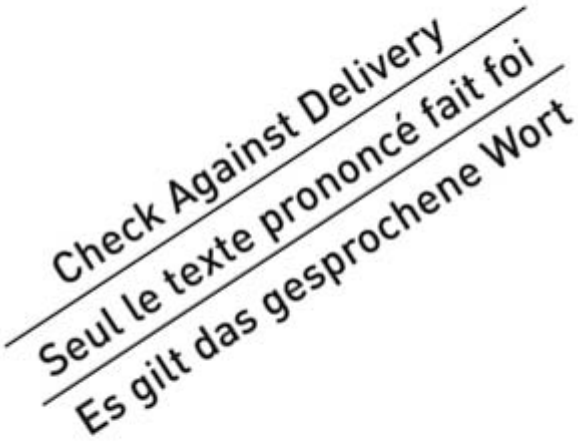
EUROPEAN COMMISSION

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

Data protection reform: restoring trust and building the digital single market



4th Annual European Data Protection Conference /Brussels
17 September 2013

Spokespersons' Service
Service des Porte-parole

SPEECH/13/720

I. MAIN MESSAGES

- Data is the new currency: the value of EU citizens' data was €315 billion in 2011. It has the potential to grow to nearly €1 trillion annually in 2020. But trust in the data-driven economy, already in need of a boost, has been damaged. 92% of Europeans are concerned about mobile apps collecting their data without their consent. 89% of people say they want to know when the data on their smartphone is being shared with a third party.

- The Data Protection Regulation is the Union's response to fear of surveillance. By adopting the Data Protection Regulation, the Union will equip it itself with a set of rules fit for the 21st century. Rules that will empower the very people whose data fuels the digital economy. Rules that will ensure the digital economy's growth can be sustained.

- The data protection reform proposals have been on the table for nearly two years. The anti-Data Protection regulation lobbyists have run out of arguments. Experts have dissected the texts this way and that. Discussions in the European Parliament and in the Council are mature. It is time to drive the institutions towards an agreement. It's time for political leaders to show determination. Europe's citizens deserve nothing less.

II. FULL SPEECH

Introduction

Ladies and Gentlemen,

The headlines over the past months have been dominated by stories about surveillance. Claims and counter-claims have been made at a dizzying speed. In my dialogues with citizens across the Union, the sense of shock is palpable and the reaction is clear. The revelations over the past months have acted as a wake-up call. People have been reminded of why data protection is important; of why a strong framework for the protection of personal data is a necessity, not a luxury.

Trust in the data-driven economy, already in need of a boost, has been damaged. This is a source of concern because of the potential impact on growth. Collected, analysed and moved, personal data has acquired enormous economic significance. According to the Boston Consulting Group, the value of EU citizens' data was €315 billion in 2011. It has the potential to grow to nearly €1 trillion annually in 2020.

Restoring trust and boosting growth. Two imperatives. Both can be delivered at the same time – through the EU's data protection reform.

How?

- First, the data protection reform will restore the trust of European citizens by putting them back in control of their data;
- Second, the reform will boost growth by opening the EU's market in data. It is a key building block of the Digital Single Market.

I. Restoring Trust

Trust has been lost in all these spying revelations. They are particularly damaging for the digital economy because they involve companies whose services we all use on a daily basis. But trust in the data driven economy began to fall long before the first NSA slides were published. The data protection reform proposed by the Commission in January 2012 provides a response to both these issues: to Europeans' concerns about PRISM as well as the underlying lack of trust.

A. Data Protection Reform and PRISM

Surveillance under Section 702 of Foreign Intelligence Surveillance Act (FISA) involves the access of national security authorities to data held in the U.S. by companies active in the EU's Single Market. This brings four components of the Data Protection Regulation into play:

First, territorial scope. The Regulation makes clear that non-European companies, when offering goods and services to European consumers, will have to apply the EU data protection law in full. European rules should apply from the moment of collection to the moment of deletion of the data.

Second, international transfers. The Regulation establishes the conditions under which data can be transferred from a server in the EU to a server in the U.S. It is the transfer of data outside the EU which brings it within the reach of the NSA.

Third, enforcement. The new rules provide for tough sanctions (up to 2% of a company's annual global turnover) to make sure that companies comply with EU law. At the moment, when confronted by a conflict between EU and foreign law, foreign companies have no reason to hesitate. In future, they will think twice.

Fourth, processors. The Regulation includes clear rules on the obligations and liabilities of cloud providers who are processors of data. As PRISM has shown, they present an avenue for those who want to access data.

In a short, as the data is collected in the Union, the Union can establish safeguards. The Data Protection Regulation is the Union's response to fear of surveillance. It is the answer to the impression that nothing can be done.

B. Trust in the Digital Single Market

Trust in the way private enterprise processes data is also low. 92% of Europeans are concerned about mobile apps collecting their data without their consent. 89% of people say they want to know when the data on their smartphone is being shared with a third party.

Why are the figures so poor?

In part because the number of high-profile security and data breaches is on the rise.

Data protection has an important part to play in addressing this problem. By minimising the data you store, you minimise the damage that can be caused by a successful attack.

It is in this spirit that the Commission, in the Data Protection Regulation, has introduced new concepts such as data protection by design and data protection impact assessments. Modern principles that respond to today's problems. The goal is to make sure that businesses and national administrations do not collect and use more personal data than they need. This will help restore trust.

The second explanation is that citizens know that companies, many of which you work for, use their personal data in ways that they cannot control or influence.

Some say that this is a question of individuals' knowledge being overtaken by technological change. But what does a citizen do when he or she understands, disagrees but cannot act? That's when trust evaporates. I believe that this is a question of individuals' rights being overridden by technological change.

That's why it's important to put individuals back in control by updating their rights. The right to be forgotten, the right to data portability and the right to be informed of personal data breaches are important elements. They will help close the growing rift between citizens and the companies with which they share their data. Empowerment will lead to a return of trust and therefore – to use the proper business vocabulary – a "return on investment". Let's believe in giving people meaningful rights.

By adopting the Data Protection Regulation, the Union will equip it itself with a set of rules fit for the 21st century. Rules that will empower the very people whose data fuels the digital economy. Rules that will ensure the digital economy's growth can be sustained.

II. Completing the Digital Single Market

A. One continent, one law

The second way in which data protection reform will boost growth is by completing the Digital Single Market.

Take a look at Europe's current regulatory framework from a business perspective. It is no longer fit for purpose. It is fragmented and it is complicated.

I say fragmented: A business operating in all 28 Member States has to comply with a different set of rules in each country. It has to deal with a different Data Protection authority in each country. The reality is 28 different laws and 28 different interlocutors.

I say complicated: the current rules, a Directive which dates back to 1995, are 12 pages long. But they are implemented differently in 28 countries. In Germany, for example, the current federal data protection law is 60 pages long. Take those 60 pages and multiply by 28 Member States. Then you'll get an idea of what the term "regulatory complexity" means in practice. A mountain of red-tape which has an enormous cost.

The Commission wants to replace this mountain by one law that is 91 articles long and valid in all of Europe. **One continent, one law.**

Within a single market for data, identical rules on paper won't be enough. We have to ensure that the rules are interpreted and applied in the same way everywhere. That's why the Data Protection Regulation introduces a consistency mechanism. Individual decisions will still be taken by national Data Protection authorities. But we need to streamline cooperation on issues with implications for all of Europe. The consistency mechanism will ensure that peer pressure on Data Protection authorities will be much stronger than it is currently. Problems of understaffing or lack of resources will be more visible. The powers of Data Protection authorities will be the same across Europe. Standards will be equally high everywhere.

Our data protection reform is a building block of the Digital Single Market. A single set of rules in a crucial sector, consistently applied.

B. A competitive Digital Single Market

Maintaining Europe's high standards of data protection is good for business.

I explained why minimising the amount of data processed was good for individuals. It is also good for business. Compare and contrast two cases. Experts believe that the hacker attack on Sony, in which the data of 77 million people was compromised, cost the firm between 1 and 2 billion US dollars plus reputational costs. That's what I call the cost of non-compliance. It is both high and avoidable. Compare this with the city of Hamburg in Germany, a place with a thriving gaming industry. Hamburg counts 155 gaming companies with more than 3000 employees. SMEs that are generating growth and wealth. This is a data-sensitive industry developing in an area where data protection standards are high, possibly the highest in the world.

High standards of data protection will also give Europe's cloud providers a competitive advantage. Trust is bankable. A survey carried out by the Cloud Security Alliance after the recent surveillance revelations found that 56% of respondents were hesitant to work with any US-based cloud service providers. Perhaps they had heard the warning given by Ladar Levison when he closed down his Lavabit email service: "I would strongly recommend against anyone entrusting their private data to a company with physical ties to the United States".

The economic impact of these doubts has now been quantified. The Information Technology and Innovation Foundation estimates that the surveillance revelations will cost the US cloud computing industry $22 to $35 billion in lost revenues over the next three years. This provides an opportunity for cloud providers who are able to deliver a higher standard of safety and security for data. Data protection will be the selling point: a competitive advantage.

I am aware that the goal of stimulating economic growth would be frustrated were the Regulation to impose an additional burden on European business. That is why I have proposed to scrap notifications, for example. Notifications to supervisory authorities are a formality and red tape which has little added value from a data protection point of view. A bureaucratic formality that represents a cost for business of 130 million euro every year. So yes, let's get rid of it.

The rules will also be flexible. We want to build an approach into the legislation that adequately and correctly takes into account risk. In a number of cases, the obligations of data controllers and processors are calibrated to the size of the business (SMEs should be made exempt from a number of requirements) and to the nature of the data being processed. We want to make sure that obligations are not imposed except where they are necessary to protect personal data.

The data protection reform will establish a modern, balanced and flexible set of data protection rules. A set of rules that will create a dynamic market within the European Union and a basis for international cooperation.

C. The EU-US Relationship

The Commission's Data Protection proposals triggered a debate on privacy in the US. In March last year, immediately after the proposals were made, the White House said that it would work with Congress to produce "a privacy bill of rights". The recent discussions in Congress testify to the growing importance attached to privacy in the U.S as well. The creation of a bipartisan privacy working group has given some impetus to the process.

The problems the working group will confront are similar to those I have mentioned in Europe.

An IPSOS poll released in January says that 45% of U.S. adults feel they have little or no control over their personal data online. In addition, there is also no single U.S. Federal law on data protection. Instead, a maze of State laws offers varying degrees of security and certainty. In Florida, not a single law lays down a definition of "personal information". In Arizona there are five. The same goes for rules on security breaches. Some States have them, others don't.

Given the significance of personal data for transatlantic trade, legislative progress on the U.S. side is important for Europe. The privacy bill of rights will form the basis of future transatlantic regulatory dialogue and cooperation.

Data protection is a fundamental right. It is different in nature to the tariff of a good or to the schedule of a service. That's why a discussion on standards of data protection should be kept separate from the give and take of a trade negotiation. I am grateful to my colleague Karel de Gucht for saying that data protection is outside the scope of Transatlantic Trust and Investment Partnership (TTIP).

Once a single, coherent set of rules is in place in Europe, we will expect the same from the U.S. To create a stable basis for personal data flows between the EU and the U.S., we can do better than a system of self-regulation which has often been criticised by European industry and questioned by its citizens. The data protection reform will be the foundation on the European side of a solid data bridge that will link the U.S. and Europe. It is better to have steady footing on a bridge than to worry about the tide in a "Safe" harbour.

Conclusion

It is time to restore trust in digital services. It is time to complete the digital single market. President Barroso recognised the significance of the reform in last week's State of the Union address: "Both with respect to internal and external developments, adopting the proposed legislation on data protection is of utmost importance to the European Commission." This is an example of Europe's value added. Of Europe "being big on big things".

The data protection reform proposals have been on the table for nearly two years. The anti-Data Protection regulation lobbyists have run out of arguments. Experts have dissected the texts this way and that. Discussions in the European Parliament and in the Council are mature. It is time to drive the institutions towards an agreement. It's time for political leaders to show determination. Europe's citizens deserve nothing less.