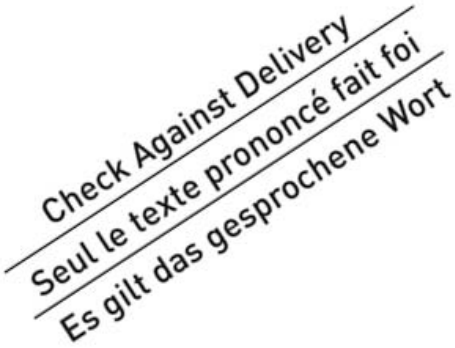
EUROPEAN COMMISSION

Neelie Kroes
Vice-President of the European Commission responsible for the Digital Agenda

Data isn't a four-letter word



IAPP Europe Data Protection Congress/Brussels
11 December 2013

Spokespersons' Service
Service des Porte-parole

SPEECH/13/1059

To add your comment to this speech, see the social version of the speech here

You have been talking intensively about data; and how to protect it.

I want to talk about data too: the opportunity as well as the threat.

Making data the engine of the European economy: safeguarding fundamental rights capturing the data boost, and strengthening our defences.

Data is at a cross-roads. We have opportunities; open data, big data, datamining, cloud computing.

Tim Berners Lee, creator of the world wide web, saw the massive potential of open data. As he put it, if you put that data online, it will be used by other people to do wonderful things, in ways that you could never imagine.

On the other hand, we have threats: to our privacy and our values, and to the openness that makes it possible to innovate, trade and exchange.

Get it right and we can safeguard a better economic future. Get it wrong, and we cut competitiveness without protecting privacy. So we remain dependent on the digital developments of others: and just as vulnerable to them.

How do we find that balance? Not with hysteria; nor by paralysis. Not by stopping the wonderful things, simply to prevent the not-so-wonderful. Not by seeing data as a dirty word.

We are seeing a whole economy develop around data and cloud computing. Businesses using them, whole industries depending on them, data volumes are increasing exponentially. Data is not just an economic sideshow, it is a whole new asset class; requiring new skills and creating new jobs.

And with a huge range of applications. From decoding human genes to predicting the traffic, and even the economy. Whatever you're doing these days, chances are you're using big data (like translation, search, apps, etc).

There is increasing recognition of the data boost on offer. For example, open data can make public administrations more transparent and stimulate a rich innovative market. That is what the G8 Leaders recognised in June, with their Open Data Charter. For scientists too, open data and open access offer new ways to research and progress.

That is a philosophy the Commission has shared for some time. And that is what our 'Open Data' package of December 2011 is all about. With new EU laws to open up public administrations, and a new EU Open Data Portal. And all EU-funded scientific publications available under open access.

Now not just the G8 and the Commission are seeing this data opportunity: but the European Council too. Last October, they recognised the potential of big data innovation, the need for a single market in cloud computing; and the urgency of Europe capitalising on both.

We will be acting on that. Next spring, I plan a strategic agenda for research on data. Working with private partners and national research funders to shape that agenda, and get the most bang for our research euro.

And, beyond research, there is much we can do to align our work and support secure big data. From training skilled workers, to modernising copyright for data and text mining, to different actors in the value chain working together: for example through a public-private partnership.

For some, the instinctive reaction is to be worried by these trends. They see the rise of big data, mobile and cloud as meaning a paradigm shift for privacy, with endless data being mixed and meshed, leading to outcomes that may be intrusive, annoying, or just plain wrong.

I agree we should not ignore those risks: we should understand them.

We need to ensure that new technologies are designed to respect privacy, without the law becoming a strait-jacket to innovation.

Attending to fundamental rights does not mean preventing possibilities, and losing this opportunity. On the contrary: mastering big data means mastering privacy.

Because we need to recognise that tomorrow's world will be digital. In that digital world, Europe can either lead or follow. We can either be at the table - or on the menu. So let's remember the opportunities on offer, and not be afraid to capture them.

With the economy where it is, we can't be afraid of new opportunity.

The fact is, many online services rely on data, and are free only because of the information people supply. In some ways data has become currency and it has proven to be a valid business model.

And most people can make those decisions themselves; whether to exchange data for a service. Informed, empowered adults with fair and transparent options can be in in control of their own privacy. In a competitive market they can make that trade-off; our data policies should be equally grown up. Indeed building that competitive market offers a big economic opportunity.

Empowering people is not always easy in this complex online world. I want to see technical solutions emerge that can do that, give users control over their desired level of privacy, how their data will be used, and making it easier to verify online rights are respected.

How can we do that? How can we ensure systems that are empowering, transparent, and secure? There are a number of subtleties in play. Here's my take.

First, companies engaged in big data will need to start thinking about privacy protection at every stage: and from system development, to procedures and practices.

This is the principle of "privacy by design", set out clearly in the proposed Data Protection Regulation. In other words, from now on new business ideas have two purposes: delivering a service and protecting privacy at the right level.

Second, also under the regulation, big data applications that might put fundamental rights at risk would require the company to carry out a "Privacy Impact Assessment". This is another good way to combine innovation and privacy: ensuring you think about any risks from the start.

Third, sometimes, particularly for personal data, a company might realise they need user consent. Consent is a cornerstone of data protection rules, and should stay that way.

But we need to get smart, and apply common sense to consent. Users can't be expected to know everything. Nor asked to consent to what they cannot realistically understand. Nor presented with false dilemmas, a black-and-white choice between consenting or getting shut out of services.

Fourth, we can also get smart when it comes to anonymisation. Sometimes, full anonymisation means losing important information, so you can no longer make the links between data. That could make the difference between progress or paralysis. But using pseudonyms can let you to analyse large amounts of data: to spot, for example, that people with genetic pattern X also respond well to therapy Y.

So it is understandable why the European Parliament has proposed a more flexible data protection regime for this type of data. Companies would be able to process the data on grounds of legitimate interest, rather than consent. That could make all the positive difference to big data: without endangering privacy.

Of course, in those cases, companies still to minimise privacy risks. Their internal processes and risk assessments must show how they comply with the guiding principles of data protection law. And – if something does go wrong - the company remains accountable.

Indeed company accountability is another key element of our proposal. And here again we welcome the European Parliament's efforts to reinforce that. Clearly, you might assure accountability in different ways for different companies. But standards for compliance and processes could make a real difference.

A single data protection law for Europe would be a big step forward. National fortresses and single market barriers just make it harder for Europe to lead in digital, harder for Europe to become the natural home of secure online services. Data protection cannot mean data protectionism. Rather, it means safeguarding privacy does not come at the expense of innovation: with laws both flexible and future proof, pragmatic and proportionate, for a changing world.

Of course, laws aren't always enough; they need to be properly implemented. So I strongly support industry driven initiatives to ensure that. Lots of good work has already happened, for example on the data protection code of conduct for cloud providers; a joint undertaking by the industry with national data protection authorities fully involved. And I am looking forward to the final version of that plan early next year, as endorsed by the Article 29 Working Party.

But data protection rules are really just the start.

They are only part of our response to the Snowden revelations.

Because, let's be honest: spying has been going on for some time; perhaps it's the world's second oldest profession. It uses whatever tools lie to hand; today it uses digital ones.

So let's not be naïve. However well drafted and carefully negotiated, the risk of breaking EU law will not deter your average hacker or spy. When your house is broken into – you don't need a lawyer, you need a lock.

That response must involve many elements beyond data protection. And it will.

We will also invest in security solutions - through our research and innovation programme, Horizon 2020. We have proposed legal safeguards – obliging public and private actors to keep networks and systems resilient and secure, protected from hacking and spying, through a Directive on network and information security.

And we can ensure secure and transparent cloud computing: so ordinary users get contracts crystal clear about what happens to their data, and when it might ever leave Europe. And with governments working together to stimulate solutions that meet the highest security standards: getting the European Cloud to cruising altitude.

On their own, data protection is not about putting barriers in the way of well-meaning businesses, or limiting the options of innovators; it is about safeguarding fundamental rights, building trust, and ensuring a system built on fairness, transparency and user control.

Ultimately our goal should be clear: to stimulate European leadership, and make our continent the world's natural home for secure online services.

That is what our Digital Agenda is all about: ensuring Europe can capture the rich and rewarding benefits of the online age; growth, opportunities, jobs. Let's find the solution that lets openness, innovation and fundamental rights go hand in hand.