Speech to Brussels Matters 21.5.2015

I

Introduction

Thank you to the Conor and Brussels Matters for organising this discussion.

And there's certainly lots to discuss at the moment. It follows two weeks after the publication of the new Commission's ideas - some old, some new - for rebooting the EU's digital economy.

And we are now about a month away from the anticipated agreement by the Council on a common position for reform of the EU's data protection framework, a move which will immediately trigger the trilogue negotiations with the European Parliament and Commission – the home straight of a marathon process.

At the same time, we are in the middle of a number of tracks for determining rules and standards for personal data flows between the EU and other countries, notably the US - the Safe Harbor agreement by no means the only example.

II

For discussion

I would like to talk to you about five things before we get into discussion.

1. A short introduction to my role as EDPS
2. A word or two about the context of the legal changes taking place

3. Big data and ethics
4. The need for global partnerships
5. And what the EU should be doing to get its own house in order

III

About EDPS (I)

I am almost six months into my mandate as the EDPS, together with the assistant EDPS Wojciech Wiewiórowski. The EDPS was established by Regulation 45/2001 which sets the specific rules for personal data processing by EU institutions and bodies - at the latest count there were 62 of them. My role is firstly to supervise these bodies and ensure they handle personal information lawfully, and secondly to advise them on policies which are relevant for fundamental rights, in particular the rights to privacy and to data protection. For that second task I work very closely with the Parliament, Council and Commission to improve the quality of existing and prospective laws.

So we basically share the DNA of the data protection and privacy enforcement authorities in European and around the world. Accordingly a third task for EDPS is to cooperate with national DPAs in the EU, particularly through the Article 29 Working Party.

IV

About EDPS (II)

Wojciech and I were appointed the European Parliament and Council with a clear mandate to develop a vision for

EU as a global leader on questions of privacy and data protection.

That's why after publishing our strategy I spent a week in Washington DC to start to build up a dialogue beyond the usual data protection community.

V

1995

Let's rewind the clock to when the Data Protection Directive became law.

In 1994 there was allegedly the first online transaction - it was for a pizza from Pizza Hut. In May 1994 Mark Butler published a book called How to Use the Internet which included advice like:

On “Surfing” the Internet: “Surfing the Internet is a lot like channel surfing on your cable television. You have no idea what is on or even what you want to watch.”

But also tips which remain relevant today:

“Never forget that electronic mail is like a postcard. Many people can read it easily without your ever knowing it. In other words, do not say anything in an e-mail message which you would not say in public.”

1995 was a watershed year for technology:

- the removal of the last restrictions on the use of the Internet to carry commercial traffic (NSFNET decommissioned and replaced by backbones operated by several commercial ISPs)

- 10,000 websites and two million computers connected to the Internet
- The 'second generation' mobile phone systems was still emerging, using using digital instead of analog transmission. And more people starting using mobile phones thanks to the advent of prepaid services.

If you read the recitals of 1995 Directive, the EU legislators knew something big was happening in how we communicate.

VI

2015

Fast forward twenty years. Today there are 45 billion web pages and roughly three billion web users.

We find ourselves in the 'global village' predicted by Canadian philosopher of communications Marshall McLuhan: the globe contracted into a village by electric technology and the instantaneous movement of information from everywhere to everywhere all the time

Data moves around via mobile devices – phones mainly – but increasingly with other things that can be worn on your person: watches, SmartBand, glasses...

Our data is an asset for big tech companies, monetised - WhatsApp with its nearly 1bn user (a company with about the size and budget of EDPS!) was valued at 18bn USD by Facebook when they merged last year.

There are imbalances in the market, with questions of fairness of competition and consumer protection.

The Snowden revelations of 2013 indicated that the internet has been exploited to create a global surveillance state.

VII

Leading by Example: The EDPS Strategy 2015-2019

I would like to offer you a strategic, holistic response to these trends and developments.

So what can we do to work better together?

First, we need to empower the individual to take control of their own information in the digital age.

There are many battles raging around 'Big Data' at the moment, whether it's antitrust and search engines, application of Artificial Intelligence, or surveillance and social media. But the common theme is the imbalance of power between corporations and governments on the one hand, and the individual on the other.

The industrial revolution moved from a concentration of machinery in the hands of the producer, to putting the power of machines in the hands of consumers - cars, fridges, televisions, computers, mobile devices.

True data portability – allowing the individual to decide what happens to their data – could bring about a similar paradigm shift in the digital revolution.

That is why EDPS has been at the forefront of the discussion for a more coherent application of rules on data protection, consumer protection and antitrust.

Second, we need global bridges to protect the personal data and privacy of the individuals facing borderless challenges.

There are initiatives for data protection reform all over the world: in Brazil, in Japan, the review of Convention 108 and the OECD Guidelines.

In fact, there are now 109 countries with data privacy laws, and for the first time European countries are in the minority.[1]

That means the EU must focus with its partners on common values - we can see the purpose of privacy as the freedom of the individual to control how his or her personal information is handled and by whom, which could look appealing to both EU and US audiences.

Third, we need a modern, easy-to-understand regulatory framework for handling personal information which applies consistently to everyone, and which is properly enforced.

VIII

Nihil novum sub sole?

Let me ask you to read this quote from a well-respected newspaper.

Can anyone guess when it was published?

Poured into huge computers, swapped with mountains of other data from other sources, tapped at the touch of an electronic code button, these vast reservoirs of personal information make it possible for government to collect

[1] Graham Greenleaf, 'Global data privacy laws 2015: DPAs and their organisations'

taxes, for banks and schools and hospitals to serve millions of customers and students and patients, for restaurants and airlines and stores to extend immediate credit to people they've never seen before. But somewhere in the roil of expanding population, vast economy, foliating technology and chronic world crisis, individual Americans have begun to surrender both the sense and the reality of their own right to privacy— and their reaction to their loss has been slow and piecemeal. "The individual is being informationally raped," says Dr. Arthur Miller, a University of Michigan law professor whose career has been given over to the defense of privacy. "The government, credit bureaus, the police and others have their fangs in this guy. They each have their piece of information about this guy, and he doesn't have access to the information

The quote comes from Newsweek, the cover article entitled 'Is Privacy Dead?' in 1970.

Big Data, in qualitative terms, is not new.

Without going into the various definitions of Big Data, let me just say that most of them highlight the growing capability of new software and hardware devices to capture, transfer, merge and extrapolate potentially unlimited volumes of information, in multiple ways and faster than ever. It will soon become difficult to process this data by using standard management tools or traditional processing operations.

The challenge of Big Data for those who care about individual data rights is similar to the move from manual to automated processing, from analogue to digital networks, from the pioneering development of e-

commerce to the Information Society, from silos to interconnected large-scale data systems.

IX

Objective 1: Data protection goes digital

When I say Data Protection must go digital, what do I mean?

I mean that we need to find new ways for applying data protection principles to the latest technologies, be they big data, the internet of things, cloud computing, artificial intelligence, drones or robotics.

We need to place the individual more firmly at the heart of technological development, through transparency, user control and accountability.

By way of illustration, much newsprint has been devoted to the so called 'new right to be forgotten'. In fact, this expression is catchy but also perhaps misleading.

In its judgment on Google Spain in May last year, the European Court of Justice did not invent a new right. It rather confirmed that if you process personal data (and, it ruled, search engines certainly do process and make decisions on processing personal data) then you have a responsibility to treat those data in a way that respects the rights and interests of the individual. Part of that responsibility is enabling the individual to challenge what you do with the information which relates to him or her.

In the headlong rush for innovation, we cannot forget the human element – that was the message of Stephen Hawking and the Future of Life Institute in their open

letter in January – and I see our strategy as a challenge to the EU to respond that call.

X

Big Data Accountability

So that's why want to promote big data accountability.

We are offering to work with data controllers to find ways of addressing the concerns that individuals.

There is no simple answer. But the remedy must be a blend of greater transparency, responsibility and user control.

XI

Objective 2: Forging global partnerships

We need global partnerships on the big questions posed by these technologies, and by the social and economic changes which accompany them.

Let me say that I believe in interoperability– a fashionable term, and a fashionably vague term – between different approaches to privacy and data protection, if such interoperability is genuinely two-way, and both sides in the discussion respect the other's values in practice, not just in words.

This must be borne in mind for international agreements like Safe Harbor and TTIP, and law enforcement like PNR and TFTP.

Bilateral agreements even with our closest strategic partners cannot be a back door for weakening the protection of the rights for which generations have fought.

As Bruce Schneier said in his book this year on surveillance: this is the cyber sovereignty moment. We want to build bridges for individual freedom to avoid the Balkanisation of the internet.

A word at this point on Safe Harbor.

The 1995 Data Protection Directive caught most US businesses by surprise. Safe Harbor was flawed attempt, with US businesses' intimate involvement, at bridge-building between the EU and US.

It was a panicky rescue mission on the part of the EU and US policymakers to preserve the close trading ties between the EU and the US.

Let's also be frank on another point. Abolishing Safe Harbor will not stop infringements of fundamental rights, and it will not stop surveillance or intelligence activities. Just like the annulment of the Data Retention Directive has not stopped data retention. You could even argue that the contrary has occurred: look at the decision of the French Assemblée nationale this week, the proposal from the German government in April, last years' 'emergency' data retention act in the UK.

Proper and transparent rules and controls on surveillance are needed – and that is a separate exercise.

But as far as data flows between the EU and its trading partners are concerned, we now have a unique opportunity to put in place, on the basis of shared values with the US, a robust precedent to serve as a model for the rest of the world

I have been very critical about safe harbor, but what I do like it about it, is that it was creativity. The problem was that it lacked a thorough application of key principles. It lacked a proper reflection on what we really mean by 'adequacy', and what the interests of the individual are.

Now is a chance to put a better arrangement in place

XII

Strong bridges are built from solid pillars on both sides…

If you look at the history of the most beautiful and strongest bridges in the world, you'll notice that their construction begins with solid pillars from both sides.

The US in its Constitution, and the EU in its Charter of Fundamental Rights, have each laid down the foundations of these pillars. The EU put it into law with the Data Protection Directive, now under revision.

An unambiguous and coherent Consumer Privacy Bill of Rights in the US would be the most powerful signal of reciprocity.

The internet has connected the whole planet. In the same way, we need similar constructions which protect the interests of the individual between all regions, not just the US and Europe

XIII

Objective 3: Opening a new chapter for EU data protection

Third, we need a new deal on data protection in the EU and we need it fast. The new data protection regulation is just the beginning: we need to mainstream the rights of the individual throughout all policies, whether on law and

order, financial services regulation, exchange of health data, or competition and consumer law.

The Revision of Regulation 45/2001 gives us an opportunity for future oriented rules for the EUI.

On each of these fronts the EDPS will engage proactively and honestly. And we will broaden the debate beyond politicians, privacy lawyers and regulators.

XIV

In the mix

There is still a lot to play for in the EU data protection reform.

- Definitions
- Scope
- Individual rights eg RTBF and data portability
- Purpose limitation
- OSS
- Data transfers
- Red tape and burdens
- Sanctions

But time is running out.

In a few weeks, the Council is likely to adopt a common position, and they will begin formal negotiations with the Parliament.

As advisor to the institutions, the EDPS will shortly afterwards publish a position paper, highlighting the main

issues from a fundamental rights perspective, but moreover offering pragmatic suggestions for resolving the differences between the institutions.

Suggestions for making the rules simpler and easier to comply with.

XV

2019?

Our mandate runs to 2019. Technology is not going to wait for the EU

You may have heard about smart cars - that's just one example of the internet of things, devices talking to each other and transmitting personal data about us, usually without the user being aware of it.

As EDPS, as we say in the strategy, we will continue to work with EU institutions, companies and all experts in the field to exploit these possibilities in line with the rules and principles of data protection which, in my opinion have served us well.

Thank you