Keynote address to ENISA Annual Privacy Forum 2015, Luxembourg

7 October 2015

Giovanni Buttarelli

Thank you to ENISA, DG Connect and the Université de Luxembourg for putting together this excellent programme and for the invitation to open this year's Annual Privacy Forum.

It is a pleasure to be here, and a privilege to address the forum for the second consecutive year.

Let me confess that I am only slightly less apprehensive than last year. As a humble lawyer in the midst of so many brilliant technical brains, I will not dare to lecture anyone here on the cyber security and engineering questions that are the subject of the various sessions today and tomorrow.

I have no pretensions to 'geekdom'.

But would like to offer some wider context in a week where, once again, the EU's approach to data protection and privacy have been at the top of the news.

Just a few metres away, the EU Court of Justice in the past week has handed down a triple bundle of highly significant data protection rulings.

None of these judgments should come as a surprise.

In the Bara case [C-201/14, 1 October 2015], the Court reaffirmed the principle of transparency towards individuals. The case concerned sharing of data between tax and health authorities - for seemingly well-intentioned purposes as the Court admitted. But it was unlawful to process data in this way on the basis of an administrative decision which was hidden from the knowledge of the individuals concerned by the data.

In Weltimmo [C‑230/14, 1 October], we were reminded that notwithstanding the ability of data to flow instaneously across the globe, national jurisdictions still prevail, and that the national data protection authority remains competent for ensuring compliance with applicable laws and investigate complaints about data processing which affects persons within that jurisdictions.

Now, yesterday, the Schrems [C-362/14, 6 October] judgment has left us in no doubt of the Court's rigorous application of the EU's data protection regime and of the invalidity of any loopholes to the safeguards guaranteed by the Charter.

Let me say it again: this should not surprise anyone who has followed the political and legal developments in the last 15 years.

For me two things are already abundantly clear.

First, no law or executive decision - such as the now moribund Safe Harbor agreement - can limit the fundamental rights and freedoms in an indiscriminate or arbitrary manner.

Vague notions such as national security, public interest or law enforcement, even though they point to legitimate objectives, cannot in themselves justify large-scale undifferentiated interference with the rights to privacy and to data protection.

This was true for the Data Retention Directive.

And it is true now for Passenger Name Records. With the proposed PNR directive, I am very worried that the legislator is moving, as with data retention ten years ago, towards another poorly conceived, blunt-edged instrument which will immediately be challenged in the courts.

The waters of Safe Harbor, as I have said many times in the past, have been stagnant for years.

Several deadlines for reform have passed, even though the shortcomings of the agreement have been known to all parties - at least since 2004 when the Commission adopted its first report.

Now we have a situation where, if someone wanted to further abuse the maritime metaphor, 4400 companies find themselves in stormy waters with a flotilla of often brilliant lawyers advancing towards them offering their navigational skills for a ship's ransom.

The second thing that is abundantly clear is this: No act, legal or otherwise, may constrain the independence of data protection authorities.

This follows judgments requiring Germany, Austria and Hungary to ensure full independence of their national authorities.

There is no doubt that privacy and data protection are not sterile abstractions.

These are European values and norms which are in full vigour. Legislators and companies neglect them at their peril.

But at the same time, those companies which have seriously respected the Safe Harbor principles should be in good shape: good shape to offer alternative safeguards for transfers to the US on a temporary basis, until the deep underlying causes of the stormy seas have been quelled.

They are formidable safeguards.

But what do the safeguards mean for the future of data flows, innovation and EU's much anticipated Digital Single Market?

We are all now familiar with the fact - the once startling fact - that 90% of the world's data has been produced in the last two years.

Critics of the judgment will therefore contend that its object and effect are to inhibit the crossborder data flows on which globalised economies depends.

But it is precisely because of the rapid changes in technology and society that we must now put in place a sustainable framework for personal data handling.

My colleagues and I have been thinking deeply about these questions since the start of my mandate as EDPS in December last year.

So, how does Europe respond to the changing legal and technological landscape?

I would like to offer three suggestions.

1. Among businesses and all data controls, we need honesty about the nature and value of personal information in the big data world

2. In the engineering community, we need coding which is driven by values and not vice versa

3. Among society in general, and DPAs have a special, even central, role to play here, we need an open and informed debate about the ethical implications of new forms of data processing and data driven tech innovation.

First of all, then, we need much more honesty in the debate.

Last month I spent a week in the San Francisco Bay Area talking to tech firms, lawyers and computer scientists.

I wanted to understand better the benefits for society and individuals of the extraordinary innovation being generated in Silicon Valley.

And I wanted a better sense of how seriously they really take privacy and data protection.

I have never encountered such an energetic and creative business environment. There is a genuinely impressive diversity of approaches to solving problems as well as maximizing value for shareholders and investors.

Many people I spoke to, including in the business community, had a clear commitment to individual privacy, to data minimization and data security.

But I was also struck by the gap between rhetoric and reality with many business models. Most large companies now have a chief privacy officer, many have crafted elegant privacy policies, some have developed attractive-looking 'dashboards' for users to amend settings.

And yet how much sway do these privacy initiatives really have at board level?

How much influence do these - in my experience - well qualified and committed privacy officers really have when decisions are being taken on products which could put individual's interests at risk?

And there is a notable lack of transparency about what is really happening to personal data once collated. Who is it shared with and for what purposes? How long is it kept? How can I as an individual access it and get it erased if it's no longer relevant?

We don't need beautiful digital dashboards which give the illusion of user control.

Companies need to honest about their processes and the logic of their algorithms.

Second, we need programmers who are able to reflect the values of democratic societies in the software which they develop, the algorithms which make decisions about individuals.

In Lawrence Lessig's famous article in 2000 which declared 'Code is Law', he used an example which today seems to speak of a different age.

He referred to the ‘nosy’ RealJukebox software, which collected personal data from user's hard disks without their knowledge. Once this practice became known, it was swiftly discontinued.

Fifteen years later, tracking online behaviour and raiding data held on mobile devices are now the standard architecture of the internet.

'If these data were deemed the property of the individual,' wrote Lessig, 'then taking them without express permission would be theft.'

But there was a sense among many people I spoke to in the Valley that, with Ashley Maddison hack, we crossed the Rubicon:

Where is now clear that CEOs are in the firing line if there is a serious data breach

That is why I am delighted that this forum will focus on Privacy Enhancing Technologies, privacy by design and by default, particular for processing in the cloud.

As the conference organisers have made clear in the programme, we need an urgent dialogue between lawyers, developers and businesses on how to mainstream Privacy by Design, at a time when more and more devices become connected and data hungry services break into the market.

We have seen data protection move from being an abstract concept on the technical margins to being a concrete issue in the political mainstream.

With this conference, and with initiatives like our own IPEN, I believe we are on a similar threshold for privacy by design. Where it ceases being an inspiring motto, and becomes instead a reality in product design, in driving the value proposition for marketing departments and customers.

Finally, we need to have a big conversation about digital ethics.

That was the purpose of the Opinion I published a month ago.

It's great that my colleague Achim will chair tomorrow, here, a panel on the ethical dimension of new ways of using personal information based on Big Data and the Internet of Things.

DPAs have to play this role, there is no other organization equipped to understand the technical details of data laws and the implications of data processing for individuals.

Marc Andreessen, the co-creator of the Netscape web browser, famously said that in future there will be two kinds of jobs: those that involve telling computers what to do, and those that involve being told what to do by computers.

In the EU, our legal framework requires that 'data-processing systems are designed to serve man'.

This forum is superb opportunity to discuss how we can ensure that this is the case for everyone, women and men of course, as we move further into the digital age.