Opening presentation (via skype) at the Autumn School 2016 on the EU

Les données personnelles: entre protection et exploitation

Université de Laval, Québec

[9am ET] 4 November 2016

Giovanni Buttarelli

[Introduction]

Mesdames et Messieurs, bonjour à tous et à toutes.

Je voudrais tout d'abord remercier Monsieur Delas et la Chaire Jean Monnet en intégration européenne de l'université Laval de m'avoir invité à participer à cette édition de l'école d'automne, édition consacrée à la protection des données.

Avec l'aimable autorisation des organisateurs, je propose de m'adresser à vous en anglais.

I know that you have had a very intense week of engagement with Europe's approach to data protection.

So first of all I would like to congratulate you on your stamina and dedication, and assure you that there is not much longer to wait for the *cocktail de cloture* - so richly deserved!

I am delighted to open this final session, "Les Ateliers Schuman", which aims to examine broader issues of data protection in North America and Europe.

Jean Monnet and Robert Schuman were visionaries for a new Europe after decades of almost perpetual crisis, war and tyranny. They laid the foundations for the Common Market as a means for securing a long-lasting peace across the continent, based on the four freedoms – of goods, capital, services, and people.

It is now 66 years since the Schuman Declaration, which came a few months before the signature of the opening of the European Convention on Human Rights.

In the intervening years, the means for automated processing of data have become universally available. In the 1970s and 80s we recognised that the Internal Market required an additional freedom, that is, the free movement of data according to certain rules which protected the rights and interests of the individual.

Since then, globalisation has disrupted and transformed economies around the world, leading to political and social uncertainty on a scale unknown since the time of Monnet and Schuman, at the end of the Second World War.

Individuals and even states feel disempowered by the breakneck speed of economic and technological change - witness the delays to the signing of CETA, as a result of the concerns of the Belgian state of Wallonia.

I want to argue this morning that what we need is a new vision for trans-Atlantic cooperation in the digital age – a vision broader and even more ambitious than that of Monnet and Schuman.

This new common approach must embrace how individuals are respected online as well as offline. That means a common approach to safeguards for handling personal information, as well as ensuring privacy for communications.

Your work this week is a step towards to defining this vision.

I would like to posit three ways for achieving this:

1. Firstly, we need a shared understanding of the digital challenge

2. Secondly, we need a shared concept of what human dignity means in the online environment and how to translate this into effective laws and regulation, taking into account what the courts of have said in Québec and the rest of Canada and in Europe.

3. Thirdly, we need more joint action which starts to apply these shared values

[1. The common digital challenge]

Web 2.0, big data, Internet of Things and Artificial Intelligence are bringing about a paradigm shift in the way we perceive ourselves and act as a society.

This applies to economic and state activities alike.

The digital revolution offers extraordinary benefits. But like its industrial predecessor, this latest revolution brings externalities, unintended consequences.

So the epicentre of our policy response must be individual and ensure that the 'digital dividend' is enjoyed by society as a whole.

The problem with the way most people experience web-based services is that covert tracking is the norm.

The problem is also that people are generally unable to understand and, even less, to contest, the inferences which are made about them on the basis of this massive data gathering.

We need, therefore, effective data protection rules, fit for the global digital arena covering the next generation.

Jurisdictions are national while the challenges and the benefits are global. In the legal-jargon of rights and obligations we may find a lot of differences in our legal orders. We also find cultural differences.

Yet, to address the challenges, more than ever we need a shared data protection identity, based on plural identities and cultural diversity.

Also inside the EU we deal with this challenge and the EU is committed to respect the cultural differences in the Member States, and yet we have adopted one data protection law applying to all Member States.

In Europe we have just opened a new rulebook.

This was necessary because of the entry into force of the Lisbon Treaty in 2009 which established the Charter within primary law of the EU (article 6.1 TEU). The Charter thus became binding for

the EU institutions and bodies, and for the Member States when they are acting within the scope of EU law.

Meanwhile Article 16 TFEU formulated a positive obligation of the EU to lay down data protection rules for the processing of personal data. This is perhaps unique: I do not know any other constitutional rule providing for such an obligation.

After four years of hard negotiations and unprecedented lobbying, the EU has adopted its new data protection framework – a regulation and a directive, applying to the activities of the private and public sectors, including law enforcement.

I do not need to repeat for you the details of this new framework. But its important innovations include:

- Greater control for individuals over their data by streamlining the notion of consent, the right to portability, the right to be forgotten and the right not to be subject to an automated processing or profiling.

- The notion of accountability, which requires companies and public authorities to comply with and to demonstrate compliance with the data protection rules. This implies a shift from a retroactive to a proactive protection, from a merely bureaucratic compliance exercise, and will require a culture change in the organisation.

- Data protection by design requiring privacy-conscious engineering from the conception phase of the data processing throughout its life-cycle. A concept which was born in Canada with the work in the late 1990s by then Information and Privacy Commissioner of Ontario, Dr. Ann Cavoukian

- Strong enforcement powers for the supervisory authorities.

- Cooperation and consistent application of the Regulation by the supervisory authorities through the European Data Protection Board

Professor Greenleaf of the University of New South Wales has been following the globalisation of data protection. This year, he

reported 111 countries which now have data privacy rules. And generally there is a tendency to emulate and to adapt the standards applied in Europe.

A single legal instrument for the whole planet is unfeasible and probably undesirable. But we need to work urgently towards common principles in the same way that nations around the world worked towards the human rights framework of the UDHR.

[2. Shared concept of dignity and legal protections]

The EU is founded on the value of respect of human dignity (art. 2 TEU) and the Charter of Fundamental Rights recognises dignity as an inviolable right (art. 1).

The notion of dignity and its role for the notion of privacy in Europe, in its modern context, goes back to the 18th century as James Whitman describes.[1]

[1] James WHITMAN, The Two Western Cultures of Privacy: Dignity Versus Liberty, The Yale Law Journal, Vol. 113, 2004, p. 1151

Indeed some newer research points out the role played by dignity, more specifically by honour, also in the southern US in shaping the notion of image and privacy.[2]

Privacy may also be expressed differently around the world.

As has been recently highlighted in a paper by my colleague, Daniel Therrien, the Privacy Commissioner of Canada, in the 1988 judgment on *R v Dyment*, Canadian Supreme Court Justice Gérard La Forest pronounced privacy to be "at the heart of liberty in a modern state…Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual".[3]

The vast majority of countries protect privacy either in their constitutions, or their courts recognise implicit constitutional rights to privacy.[4]

[2] Alessandro MANTELERO, Book Review, Laws of Image, Privacy and Publicity in America, by Samantha Barbas, 2015, EDPL 1/2016, p. 141

[3] 7R v Dyment, [1988] 2 SCR 417 at para 17. Online at https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/375/index.do in: Office of the Privacy Commissioner of Canada, Consent and privacy - A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act, 2016, p

[4] Daniel SOLOVE, Understanding Privacy, Harvard University Press, May 2008

Thus, as the Supreme Court stated in *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers*, data protection legislation has a quasi-constitutional status given the important interests it protects.[5]

Equally, the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR) and national courts in the Member States clarified that data protection is not an optional extra.

The courts have applied these rules strictly, interpreting them in the light of the primary law and favouring the rights and interests of the individual above corporate or state aims, however reasonable and legitimate.

There is a constant dialogue, even cross-fertilisation, between the CJEU and the ECtHR and between the Member States' courts by referring the cases to the CJEU for a preliminary ruling.

[5] *Local 401, 2013 SCC 62,* para. 22

The CJEU settled case-law states, in essence, that the fundamental rights guaranteed in the legal order of the EU are applicable in all situations governed by EU law. Derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary[6].

We may briefly consider a few landmark judgments of the CJEU and the ECtHR.

The CJEU judgments on the annulment of the data retention Directive and of the Commission's Decision on the adequacy of Safe Harbour (Schrems) ruling concern the processing of personal data by commercial entities, either because these are obliged by statutory law to retain these data for the purpose of subsequent access by law enforcement authorities or to disclose data to national intelligence services.

[6] See Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke* and *Eifert*, paragraph 77; Case C-473/12 *IPI,* paragraph 39; Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* and *Seitlinger and Others*, paragraph 52; Case C-212/13 *Rynes,* paragraph 28 and Case C-362/14 *Schrems,* paragraph 92

The ECtHR judgments in *Zakharov v. Russia*[7] and *Szabo and Vissy v. Hungary*[8], relate to the law enforcement and national intelligence services' activities.

But in each case the courts showed how privacy and personal data protection should be treated even when the objective is of public interest, i.e. to combat crime and terrorism. They found generalised storage and subsequent access by public authorities, without any objective criteria limiting the access in terms of persons concerned, to be unacceptable interferences with the rights to privacy and (in the CJEU's case) personal data protection.

In two other pending cases before the CJEU, the Opinions of the Advocates General maintain the conclusions of the aforementioned CJEU and ECtHR judgements.

The one case concerns the issue of the retention of communications data provided the criteria for access by public

[7] ECtHR, Roman Zakarov v. Russia, 4 December 2015
[8] ECtHR, Szabo and Vissy v. Hungary, 12 January 2016

authorities comply with the CJEU judgement on the data retention Directive[9] and the second case the EU-Canada PNR agreement.[10]

In the PNR case the Advocate General held that some provisions, such as the processing of data outside the objective of fighting terrorism and serious transnational crime and the processing of sensitive data are incompatible with the Charter.

These judgments are of paramount importance for the discussions on the transatlantic data flows and on cooperation in the fight against crime and terrorism.

Serving as judge in my country I handled complex cases concerning the intelligence, mafia and organised crime.

I know the importance for law enforcement of quick access to all relevant information. But we need to look at the actual needs of our intelligence agencies and what is the cost for our rights and freedoms and the society as a whole by massive and intrusive surveillance methods.

[9] CJEU, Joined cases C-203/15 and C-698/15, Opinion of Advocate General, 19 July 2016
[10] CJEU, Opinion 1/15, Opinion of Advocate General, 8 September 2016

The problem is not the lack of relevant information, the problem rather lies on the lack of sharing and adequate analysis of existing information.

What is needed is a global consensus around human dignity and data.

[3. Joint action]

How do we begin to build a consensus?

My third proposition is that consensus can be built through joint action by enforcement authorities.

Canadian privacy regulatory enforcement, at both Federal and provincial level, is one of the most active in the world, with rigorous investigations into global multinationals, including some joint international investigations.

Regulators have also issued forward looking guidance and research on a range of emerging privacy issues.

I am a passionate supporter of cooperation and concerted actions between the data protection authorities.

In my Strategy as the European Data Protection Supervisor I committed to build global partnerships inside and outside the EU with fellow experts, authorities and international organisations.

In 2007, OECD governments adopted a Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy.

Two years ago, the 36th International Privacy Conference meeting in Mauritius adopted the Global Crossborder Enforcement Cooperation Agreement.

Last month, the 38th International Conference in Marrakech adopted a Resolution on International Enforcement Cooperation and mandated a new working group to develop a set of key principles in legislation that facilitates greater enforcement cooperation.

This year, within the Global Privacy Enforcement Network (GPEN) some 25 data protection authorities participated in a coordinated review of more than 300 devices connected to the Internet of Things, such as fitness trackers, thermometers, heart rate

monitors, smart TVs, smart meters, connected cars and connected toys, to find out how users are kept informed.

The commitment and structures are in place.

The challenge now is to make international enforcement cooperation the norm, not the exception.

And we must go beyond the silos of regulatory jurisdictions.

I see a big potential in global partnerships with enforcers in the area of competition and consumer protection, whose ultimate goals are very close to those of privacy and data protection laws.

Both sides of the Atlantic are worried about excessive market powers, concentration of data in too few hands and unfair terms and conditions. We, enforcers, can learn from each other, and create synergies, at the end allocate our resources efficiently.

That is why EDPS has launched a Digital Clearing House for digital market regulators of all shapes and sizes to discuss common concerns and potential violations of more than one framework.

[Conclusion]

Ladies and gentlemen,

This is a moment of economic and political tension across the globe.

We need to define a new vision for transatlantic cooperation which includes safeguards based on shared values.

Europe and Canada are natural allies in building a new consensus, not only on the rules governing international data flows, but also on the wider ethics of behaviour by states and corporations in the digital environment.

Data protection authorities can act as facilitators of open-minded, unpolarised dialogue with different stakeholders and build partnerships with other enforcement authorities.

Thank you for listening. I would be very pleased to hear your comments and questions.