Adequacy, Localisation and Cultural Determinism

Keynote Speech at 38th International Privacy Conference, Marrakesh, 19 October 2016

Giovanni Buttarelli

Ladies and gentlemen

Thank you to Marty for that introduction.

Thank you to the Moroccan data protection authority for inviting me to offer some introductory reflections.

The topic of this debate is an inspired choice from this Conference. And I would like to applaud our Moroccan hosts for their vision and ambition on this session and on the rest of the programme.

Because, in my view, adequacy, localisation and cultural determinism is a topic with truly global resonance; it is a topic that matters to businesses and governments as well as to ordinary citizens, workers and households, and to their advocates in civil society.

It exposes one of the most important faultlines of globalisation.

As such, the issue presents to this Conference a big open goal.

This Conference brings together a unique and rich diversity of expertise and expertise from around the world.

This is the best equipped forum to tackle these issues.

At the heart of the matter is the following question:

How do we, as privacy regulators, secure in the digital, globalised age the rights to privacy and data protection - along with related rights and freedoms?

The media tend to focus on alleged divisions, disagreements and controversies.

But if you ignore legal jargon of 'rights' and 'obligations' and consider instead our underlying values, then the world has much more in common that would at first appear.

I want put forward three propositions, to which the panel may wish to react.

First, that there is no room for relativism when it comes to respect of individuals and human dignity.

Second, we need to free up flows of data around the world; but this is not for purely economic reasons, its rather to ensure everyone is able to enjoy the digital dividend of technological change and globalisation.

Third, we need a common framework of reference for ethics in the digital age.

[No compromise on human dignity]

Privacy is a widely recognised universal human right.

There now is an increasingly intense debate on the confidentiality of electronic communications in the digital age.

We live in a time of worrying tendencies all over the world towards interfering with confidentiality of communications and the freedom of expression on line.

We live in a time where the norm is for private communications via web-based services to be routinely, trivially, parsed by machines and monetised for profit motives.

If you process data, then that must be done legally, and for clear purposes.

But, on top of that, if you are using a service to communicate with another person you should be able to do this in confidence no-one else is going to snoop on that communication.

That should hold true regardless of the means that you choose to communicate.

And those means of course are proliferating in variety and in number with Web 2.0: traditional telephony is just one means of many.

So it doesn't matter whether personal information processing is involved, the right to privacy is sacrosanct.

[Data protection and the free flow of data]

So, privacy is a widely recognised universal human right.

Data protection isn't – at least, not yet.

But, I would argue, it is fast becoming that way.

I think lawyers - myself included - can sometimes become too fixated with terminology instead of focusing on real outcomes for ordinary women and men.

The terminology of rights can sometime become a barrier to dialogue about ensuring that individuals are actually protected against harmful behaviour; about ensuring that they are empowered to take control over their online lives, and to understand to and to determine what happens to information about them.

Many countries now have a data protection law, setting out the rules for handling personal information. But they don't necessarily use the terminology of rights.

And there is a growing number of countries that realise the need to regulate data processing - regardless of privacy implications.

Data protection was conceived as a means of facilitating personal data to flow freely between freely trading countries.

Among pioneers in the 1970s and 1980s were international organisations - the Organisation for Cooperation and Development and the Council of Europe - and, at a national level, the United States, Sweden and the German Federal State of Hesse.

These trailblazers recognised that such a free flow of data was only permissible if each country enforced an acceptable standard of respect for the individual whenever personal information was processed.

It is curious - and instructive - to note how, in Europe, we have come full circle in our analysis of when transfers of personal data to another jurisdiction should be permitted.

In 1981, the Council of Europe, in its Convention 108, prohibited restrictions on transfer of specific categories of data to another Party whose laws offered 'equivalent protection' (Article 12.3.a).

The European Union, when it adopted the Data Protection Directive many years later in 1995, followed the OECD in referring to 'adequacy' of protections.

Now with the Schrems judgment of October 2015, the European Court of Justice has interpreted adequacy as meaning 'essential equivalence' of standards and safeguards.

[Building a global consensus]

In the past, your rights have been determined by the colour of your passport.

Now, at last, rights are being unshackled from citizenship: if you are a human being, you should be treated with respect and dignity.

And in today's hyper-connected reality, respect and dignity require preserving confidentiality of communications and lawful processing of personal information.

Exercises like the adequacy decision-making process, Safe Harbor and the Privacy Shield should help to build a consensus on what is right.

It has been said that rights are 'not a limit but an effect of politics'*.

There are now 111 countries which have privacy and data protection laws and studies.

More and more countries in all continents are seeing the global picture; they are seeing data protection as an integral part of good administration and reasonable regulation.

According to the International Telecommunications Union, there is still more than half of the world's population who don't use the Internet.

So, where Internet coverage is still limited, countries see data protection as an essential measure for building or restoring trust in how people are treated in the digital space.

In such parts of the world, there is a great opportunity to ensure mass use of technologically on the basis of trust and accountability.

By contrast, in the more economically developed regions of the world, it is already a decade ago that the majority of the population were reported to be Internet users. This is where trust has been lost, and where we face a much bigger challenge of restoring trust.

* Martti Koskenniemi, The Politics of International Law, 2011.

All regions of the world, therefore, have a long-term strategic interest in the question of data flows, localism and determinism.

All regions of the world have an interest in pushing for global partnerships.

All regions of the world have an interest in local laws being compatible with one another - 'interoperability' to use the jargon.

This means mutual recognition where appropriate, and respect for the diverse legal and cultural DNA which prevail from country to country.

[The EU approach]

For us in the EU, we need to refresh our legal apparatus for the Big Data age. We need a new generation - a third generation - of forward-looking, generally applicable data protection rules.

This is not a mere political aspiration; it is a legal obligation under the 2009 Lisbon Treaty, which includes the positive obligation (according to ECHR case law) to uphold the rights to privacy and to data protection in the Charter of Fundamental Rights.

And the Treaty also obliges the EU (Article 6) to accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms.

This is crucial for mutual understanding when the EU enters negotiations with our friends and partners around the world on international agreements, for example, on trade - take TTIP and TISA - and law enforcement cooperation - take bilateral agreements on passenger name records or the EU US 'Umbrella Agreement'.

We as data protection authorities understand the importance of free flow of data around the world. At a time of global economic uncertainty, we appreciate the weight of expectation for a potential boom in digital trade.

But trade is not only an economic issue.

That is why Commission President Juncker said on his appointment two years ago that data protection was not a bargaining chip. And that is why, more recently in his 2016 state of the Union speech, he said, 'Europeans do not like drones overhead recording their every move, or companies stockpiling their every mouse click. In Europe, privacy matters. This is a question of human dignity.'

Ladies and Gentlemen,

[Consensus]

I believe we need a new consensus, a global political consensus, on the ethics of data processing.

Yes, we face big obstacles.

Since 2013 this Conference has been calling for an additional protocol to Article 17 of the International Covenant on Civil and Political Rights. This would ensure a common international standard on privacy and the constraints on surveillance to be respected by all governments.

The UN Special Rapporteur on the right to privacy has acknowledged this stakeholder consensus (in his report this year to the Human Rights Council). His ten-point plan includes the development of international law in the area of privacy and Internet Governance, and achieving a better universal understanding of what the core values in privacy are or may be.

I would argue that there are values and areas of public life which offer fertile ground for this new consensus.

Ethics is one area.

Accountability is another.

The concept of accountability goes beyond compliance with the rules, it implies a cultural change.

The new GDPR includes a direct reference to the "accountability principle" in Article 5.2 and will require, under Article 24, the implementation by controllers of appropriate technical and organisational measures.

It is an essentially practical principle. For instance, it means: up-to-date documentation; registers for international transfers including the legal basis and the instrument used; and records of where there has been an exception to the rights of information or the right of access.

This is relevant to checking compliance when we conduct and inspection or when we have to carry out "indirect access" in the context of a complaint.

We are applying this now to the European Union institutions, bodies, agencies and offices that we supervise as EDPS.

I am also discussing data protection accountability at the very highest level, for example with the President of the CJEU, with the President of the European Central Bank, the Secretary General of the Council of the EU and the Director of Fundamental Rights.

We as Privacy and Data Protection Commissioners in the world need to take a sound, pragmatic approach.

We need more flexibility: in our recent experience in the EU of data protection reform, we managed to reduce by two-thirds the number of separate implementing and delegated legal acts which were required.

DPAs in the EU and the EEA are able to cooperate with other Privacy and Data Protection Commissioners outside the European Union to develop together flexible guidance, to share best practice and to cooperate on enforcement.

We already have similar rules on binding corporate rules applied by the Article 29 Working Party and by APEC; this is an excellent precedent upon which to build.

And as courts assume a more assertive role in enforcing privacy protections, there is more scope than ever for judicial dialogue also.

We need an in-depth discussion of how to ensure privacy is not dependent on wealth or knowledge.

Such a discussion requires openness about, and respect for, cultural differences.

We should resist the temptation to find and rely on 'quick fixes', which will not stand the test of time, and which cannot hold up to scrutiny of the independent courts.

I hope the discussion today will enable us to step forward in this journey for a global consensus.

[Conclusion]

Ladies and Gentlemen,

In June 1980 the Member States of what was then known as the European Economic Community gathered in Venice – when the world was still divided along Cold War lines and Lebanon was in the middle of a brutal civil war that was in many ways a proxy for the Arab-Israeli conflict.

These governments meeting in Venice set out principles for initiating a Middle East peace process -including an affirmation of the right to self-determination of nations.

This was controversial at the time. But thirteen years later Israel recognised the PLO as its negotiating partner in the Declaration of Principles of 1993.

And the Venice Declaration of 1980 proved to be ahead of its time, anticipating the prevailing international consensus on the principles to resolving a decades-long conflict.

Twenty years later there was another meeting in Venice, this time it was this Conference of Commissioners. Our slogan then, in 2000, was One World, One Privacy.

As I have previously said in Montreux and Mexico City, that slogan has never been more relevant.

This Conference is the new pioneering effort to apply safeguards to the fast-evolving technologies of a globalising economy and society.

I believe our deliberations and resolutions, however controversial or contested, will stand the test of time.

One world one privacy: let's revive that rallying call today, we seek to define principles for personal data sharing for the next generation.