ICDPPC

International Conference of Data Protection & Privacy Commissioners

Executive Committee

Keynote address to International Telecommunications Union
World Telecommunications Standardization Assembly (ITU – WTSA16)

Global Standards Symposium, Hammamet, Tunisia

24 October 2016

Regulatory principles for security, privacy and trust

I am very grateful to the ITU for the invitation to address you and to introduce you to the International Conference of Data Protection and Privacy Commissioners and to update you on our 38th annual conference which concluded in Marrakech, Morocco, just last week.

For many years when I practised law in the field of technology and privacy, the term "convergence" was in vogue. I can't even remember what was going to converge: telephony and computing; broadcasting and the internet? It was one of those terms that expanded to meet any number of needs. Convergence seemed always to be just around the corner, and what ever it was, we don't seem to hear much about it anymore, so maybe that indicates it has been achieved.

There seems to be another convergence occurring – the gradual but accelerating consensus among previously disparate organisations that privacy is becoming one of the defining issues of our age.

The UN General Assembly, during its 68th Session (2013), adopted a Resolution titled: *The right to privacy in the digital age,* calling on all UN Member States to *"respect and protect the right to privacy, including in the context of digital communication"*.[1]

The international technology and market research company Forresters, declared that 2015 would be the year privacy and security became competitive differentiators. We saw that happen and saw the trend continue into 2016. We have seen Apple, Facebook and Microsoft in the courts to stand up for their customers'

[1] UNGA Resolution 68/167, http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167

rights to privacy. We have seen Google and Facebook and many others subject to the high profile regulatory attention of European data protection regulators.

In May this year, the World Bank issued a World Development Report entitled "Digital Dividends" which highlighted, among other things, the need for consistent reliable regulation for data protection as an a key factor in reducing inefficiencies, and promoting consumer confidence in the online world.

In June this year at the OECD Ministerial on the Digital Economy in Cancun participating Ministers declared the importance of building and strengthening trust in order to maximise the benefits of the digital economy.

The participating OECD Ministers recognised that trust, privacy and transparency are essential elements of civic and digital engagement.

Ministers agreed that they would:

> "Develop privacy and data protection strategies at the highest level of government that incorporate a whole-of-society perspective while providing the flexibility needed to take advantage of digital technologies for the benefit of all; and support the development of international arrangements that promote effective privacy and data protection across jurisdictions, including through interoperability among frameworks"

The OECD has earlier declared the importance of a "multi stakeholder" approach. The ITU, it seems to me, is very much a "multi stakeholder" organisation, and it has clearly recognised the importance of privacy and security to its membership by organising this conference, and in so doing, converges with the work of the World Bank, the OECD, and the International Conference of Data Protection and Privacy Commissioners (ICDPPC) which I am representing here today.

In my brief comments, I would like to give you a bit of the history of my organisation, mention some of the work that we and member authorities have undertaken in areas of common interest to your membership, and outline some areas of possible future collaboration.

History of the conference

The first conference of privacy commissioners was held in 1979. In 2001 the Conference first adopted membership criteria. Fifty-four authorities formed the foundation membership, and by 2010 the conference had grown to 89. The coverage grew to include agencies with a solely private sector mandate, including the Korean Internet Security Agency (KISA) in 2004, and the US Federal Trade Commission (FTC) in 2010.

The Conference rules and procedures adopted in 2010 set out five substantive membership criteria:

1. A public entity, created by an appropriate legal instrument.
2. Has the supervision of the implementation of data protection or privacy law as one of its principal regulatory mandates.
3. The law under which it operates is compatible with the principal international data protection or privacy instruments.
4. An appropriate range of legal powers to perform its functions.
5. Appropriate autonomy and independence.

Conference size

In the 14 years since 2002, when membership was first established, the Conference has grown from 54 to 115 members. In other words it has more than doubled in size, reflecting an expansion in data protection laws around the world.

While that may be encouraging for anyone that values the idea of more universal data protection law, the growth should be seen in perspective. Note, for example:

- Only about 1/3 of the 193 UN member states are represented in the Conference.
- Only 3 of the 20 most populous countries have authorities that are members of the Conference.
- Some 2/3 of the Conference membership is from one region.

Berlin Group

From time to time the Conference convenes working groups to undertake research or develop policy on particular issues. One working group of particular relevance to the ITU is the International Working Group on Data Protection in Telecommunications (“the Berlin Group”). The Berlin Group has met twice a year since the early 1980s and consists of 55 participants representing 36 delegations.

Last week in Marrakech the Berlin Group reported back on its activities in the last year, including issuing working papers on:

- Location Tracking from Communications of Mobile Devices
- Intelligent Video Analytics
- Update on Privacy and Security Issues in Internet Telephony (Voice over IP – VoIP) and Related Communication Technologies.

In this last paper, available on the group’s website, the Berlin Group calls upon legislators and regulators to ensure that the provisions for telecommunications secrecy, as foreseen in many national constitutions and regional and global regulatory instruments, also fully cover VoIP and other multi-media communication services. In addition, the paper contains recommendations on privacy and security for VoIP providers, software developers, hardware manufacturers, and for users.

The Group has also led an ongoing discussion about the **Use of Biometrics in Electronic Authentication**. You will appreciate the significance of this issue, given that you can change your password, or cell phone number, but it is not so easy to change your retina, or voiceprint!

https://datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt

Challenges and opportunities

One of the reasons we are so focused on privacy, particularly in telecommunications at the moment, is because of the disclosures of former NSA contractor, Edward Snowden.

I don't need to remind you of all the details, but the Snowden revelations sent shockwaves through the privacy, telecommunications and IT worlds. The allegations that intelligence agencies routinely received access to vast amounts of data both in transmission, or on the servers of online platforms ignited conversations and debates (as well as inquiries, court cases, and law reform) in many countries around the world.

The allegations had potential to undermine what the OECD has identified as that necessary precondition for the effective operation of the digital economy - trust.

The responses were immediate, and wide-ranging. The UN moved that same year to appoint a special rapporteur on the question. He is today making a report to the General Assembly.

I add without comment that our conference first passed a declaration in 2005 at Montreux, Switzerland, calling on the United Nations to prepare a legal binding instrument which clearly sets out the rights to data protection and privacy as enforceable human rights. We are yet to see such an instrument, but perhaps when the Special Rapporteur completes his mandate the UN will have a sound basis to do that work.

https://icdppc.org/wp-content/uploads/2015/02/Montreux-Declaration.pdf

If the Snowden revelations eroded trust, so too does the seemingly endless parade of leaks and breaches, criminal and state sponsored, that compromise networks, databases, and consumer and business confidence in the digital infrastructure.

The question then, for the many agencies and interest groups converged on this problem is how to build and maintain that trust?

The ICDPPC has undertaken some work in this area, but it will take the kind of multi-stakeholder approach sought by the OECD, and represented by the ITU to ensure a comprehensive and coherent response to these issues as the digital world continues to expand, and more and more economies begin to rightfully demand their digital dividends.

Here are some ideas for shoring up that confidence and trust by applying privacy principles and perhaps developing standards in the telecommunications sector.

- Promote and deploy Privacy-by-Design, Privacy Impact Assessment and Privacy Enhancing Technologies.

There is no tradeoff to be made between innovation, enterprise and privacy. Good privacy and security practices, when designed in to new technologies, become a selling point and improve the whole network.

- Ensure that access to networks, systems, content, communications and metadata by agents of the State is undertaken only in accordance with lawful authority, and only when that access is necessary, and proportionate.

Privacy is a fundamental human right. But like many other rights, it is not absolute. Just as I cannot exercise my right to freedom of expression in this room to shout "fire", nor can I exercise my right to privacy to prevent the detection of a trade in child pornography. Access to communications by law enforcement, security or intelligence agencies should be according to consistent legal standards, regardless of the jurisdiction.

- Promote transparency in relation to access to or use of personal data for purposes other than those for which the data subject has consented.

What shocked many about the Snowden allegations was that online platforms many of us use on a daily basis were allegedly freely available to agencies for intelligence purposes. Several of the most prominent online platforms responded with regular "transparency reports", in which they revealed to their customers, and the world, the nature and extent of official calls on their customer data. In 2015, The Berlin Group and the ICDPPC passed resolutions supporting and promoting transparency reporting.

- Develop and promote appropriate standards and safeguards for the de-identification of personal data, and for the prevention of re-identification of individuals from de-identified datasets.

Industry and governments alike are clamouring to reap the benefits of so called "big data". The ability of data scientists to derive public benefits from analysing large datasets is undeniable. Telecommunications companies have vast volumes of data with which much good can be done. With location data, for example, NGOs and aid agencies can track the movement of refugees after political and upheaval, or natural disaster, or trace the spread of disease. The UN Global Pulse has developed a set of privacy principles to try and facilitate this kind of work.

To get the societal benefit of such data, it is not necessary to identify individual mobile phone users, and to do so would in many cases breach privacy principles, but how do we know that a given measure to de-identify a data set will be effective?

DPAs and PCs heard at our "Internet of Things" session in Mauritius in 2014, that researchers had proven the ease with which individuals could be extracted from a supposedly "de-identified dataset. They found that if they had a dataset including all the location details of 1.5M mobile phone users over a year, and they knew where one individual had been only four times in that year, they could extract that individuals full location history, with an 85% accuracy.

- Ensure citizens and consumers continue to have transparency about the basis on which automated decisions affecting them have been made.

We heard in Marrakech last week that even though it is still quite undeveloped and not widely understood, the concept of "algorithmic transparency" is facing considerable challenges in the light of artificial intelligence, machine learning, and "unpredictability by design."

- Data portability

Just as number portability has proved crucial in promoting competition in the mobile phone industry, so is data portability an important concept in promoting consumers' rights, and facilitating the ease of access to, and exit from, telecommunications, online, and other services. Data portability is part of the European General Data Protection Regulation; due to come into effect in 2018, and will need to be provided for beyond Europe.

Future collaboration between ITU and ICDPPC

I hope that there will be further opportunities for our organisations to work together, and look forward to a continued exchange of speakers for our respective conferences. I would welcome, for example, a proposal for the ITU to attend our 39th Conference in Hong Kong in some capacity, either as observer, or host of a side event.

One thing that has become very clear to our Conference is that data protection authorities and privacy commissioners cannot resolve the challenges on our own. We must work with industry, governments, NGOs, academia and organisations such as yours, to ensure that all can participate safely in the digital economy.