Global Standards Symposium

Security, privacy and trust in standardisation

ICDPPC Chair John Edwards

24 October 2016

CANCUN DECLARATION

At the OECD Ministerial Meeting on the Digital Economy in Cancun in June this year, the 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.

Among the nine points in the Cancun declaration that the OECD Ministers committed their nations to, three in particular are perhaps most relevant to us here today.

These are to:

- Support the free flow of information
- Increase broadband connectivity and harness the potential of interconnected and converged infrastructures and digital services; and
- Promote digital security risk management and the protection of privacy at the highest level of leadership.

TRUST AND PRIVACY

The OECD and other international institutions help bridge divergent privacy and data protection frameworks across regional differences.

It is imperative that international institutions work together to coordinate the development of privacy and data protection frameworks.

Noting that this session is titled ‘Security, Privacy and Trust in Standardisation’, I particularly want to address the last point - promoting digital security risk management and the protection of privacy.

In my brief comments, I will discuss the relationship between privacy and trust, and how a principled understanding of the nature of privacy is essential for the maintenance of public trust.

This is the aim of initiatives designed to enhance transparency that are supported by the International Conference of Data Protection and Privacy Commissioners.

The International Conference is an important strategic partner.

It has been the premier global forum for data protection authorities for the past three decades.

The ICDPPC provides leadership at the international level by connecting the efforts of 110 privacy and data protection authorities.

Its aim is to establish a single global standard for data protection and privacy regulators to work across regional differences.

In order to have trust and confidence in the digital environment, governments need to apply a standardised approach to provide assurance to the public and to business that they can interact online safely.

This includes assurances that their data will be looked after securely, and used appropriately.

We know that in a high trust environment, the cost of doing business or engaging the public is much lower than in a low trust environment.

A low trust environment has big cost implications for everyone.

When citizens don't trust their government, they are more likely to deliberately give false information.

The same applies for business.

TRANSPARENCY

At the June OECD Ministerial Meeting in Cancun, the participating Ministers declared the importance of building and strengthening trust in order to maximise the benefits of the digital economy.

The declaration included a commitment to promote a general policy of accountability and transparency.

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

The links between privacy and transparency are deep and go back a long way, and have trust as their common touch point.

The aphorism most closely associated with the benefits of transparency is the homily, "sunlight is said to be the best of disinfectants".

That phrase is attributed to US Supreme Court Justice Louis Brandeis who helped develop the 'right to privacy' as a legal concept in the 1890s.

The digital economy has since widened and deepened our concept of privacy, and highlighted a pressing need for the development and management of international data protection and privacy standards.

This is driven by a reflected increase in public concern about security and privacy.

We live in the shadow of revelations of data breaches, mass surveillance without due process, and secret courts established to oversee secret processes for authorising access to information.

It's important we as a global community understand the challenges and help support people respond positively in an uncertain geopolitical climate coupled with tremendous advances in technology and data collection.

Returning to Louis Brandeis – to give you the full quote, he said "sunlight is said to be the best of disinfectants; electric light the most efficient policeman".

It is the role of data protection and privacy commissioners to be the electric light.

OECD PRIVACY PRINCIPLE

Internationally, the most commonly used data protection and privacy framework is the OECD's privacy principles.

The OECD principles align closely to European Union data protection legislation.

It is also used in New Zealand as the basis for our privacy legislation.

One of the OECD privacy principles is the Individual Participation Principle.

Under this principle, an individual should have the right:

- to obtain from a data controller confirmation of whether or not the data controller has data relating to the individual
- to have communicated the data relating to an individual within a reasonable time, in a reasonable manner and in a form that is readily intelligible
- to challenge data relating to individual and have the data erased, rectified, completed or amended.

Latin American jurisdictions call the right to access one's information "habeus data" – or "bring up the data" - recalling that most fundamental human rights writ and instrument of the rule of law: habeus corpus or "bring up the body".

That right, combined with the right to have the reasons for decisions affecting the individual is a check which ensures that governments – and corporates – are accountable for their actions which affect the rights of individuals.

It is a check against corruption and power - an essential aspect of any system of accountability.

TRANSPARENCY REPORTING

At the International Conference of Data Protection and Privacy Commissioners in Amsterdam last year, regulators adopted resolutions supporting transparency reporting.

It is a response to consumer concerns in which corporates report on a regular basis on the number and nature of requests made by law enforcement or intelligence agencies.

We are also urging governments to keep records, and promote transparent practices, and where necessary to remove barriers to corporate reporting.

The OECD has an important programme of work in this area that can lead to a coordinated approach.

Transparency reporting shows customers how companies are handling requests from government agencies for their personal information.

Transparency reporting encourages global growth by giving consumers more information about who they are entrusting with their data

Companies such as Google, Facebook, Microsoft and Twitter are already doing this.

DATA BREACH REPORTING

There is another important trend in transparency and privacy - data breach reporting.

Mandatory breach reporting is important because it puts the individual at the centre of a security failing.

If a company has a privacy breach which compromises customer data, those customers are entitled to know about it so that they can take steps to protect their identity, their credit etc.

In order to build and maintain consumer trust in the digital economy, citizens and consumers need to be assured that there will be consequences for breaches of that trust.

Governments must respond to this demand by giving privacy and data protection authorities effective enforcement tools, such as the power to issue fines, to make declarations of illegality, and to warn consumers by calling out poor practices.

For example, my US colleagues at the Federal Trade Commission have been able to apply these kinds of regulatory tools to force organisations like the taxi company Uber to improve their privacy practices.

ALGORITHMIC TRANSPARENCY

Data protection and privacy regulators around the world are seeing a growing enthusiasm among governments for “big data”.

The use of automated mathematical decision making throws up increasingly complex problems that may entrench rather than assist to resolve social inequities and misallocated resources.

One emerging threat is the use of proprietary algorithms which produce a conclusion based on data, but leave the subject with no understanding as to the basis on which decisions affecting their lives have been made.

For example, there have been trials running a programme over social media connections to allocate a credit score.

Governments experimenting with predictive risk modelling, or the allocation of resources based on big data analytics should be transparent with their algorithms so that people can see how and why decisions that affect them are made – and allow them to challenge those decisions if they think they’re wrong.

If you’re going to make a judgement call about someone based on a data set, then that person has the right to see why you made that call.

LOOKING AHEAD

Data protection and privacy authorities need to be able to respond more rapidly across borders to emerging threats.

We need to cooperate to deliver effective remedies for their citizens, and the International Conference of Data Protection and Privacy Commissioners has taken a number of steps to do so.

With the support of the OECD, we have established the GPEN - the Global Privacy Enforcement Network - and the Mauritius Declaration of 2014 provides for another option for enforcement cooperation between member authorities.

But there is much to do, and it is a constant struggle to match the pace of industry innovation.

One area that has potential to considerably level the playing field between consumers and providers of digital services is “data portability”, the ability of individuals to take their data with them when they choose to exit one service in favour of another.

In a market where one player can very quickly become dominant, there is a potential for innovation to be stifled by monopolistic practices, and a sense for consumers of being “locked in”.

An ability to freely extract one’s data will not only restore power and autonomy to the individuals, but will make it easier for new players to transfer to innovative services that better meet their needs.

Data portability is a part of the European Union’s General Data Protection Regulations that will come into force in 2018, and it is one of many initiatives that OECD members will need to consider to ensure that their laws remain “fit for purpose” in a rapidly developing digital economy.

ROBOTICS/ARTIFICIAL INTELLIGENCE

Member privacy regulators are currently engaging with privacy challenges posed by the internet of things, artificial intelligence and robotics.

The International Conference recognises artificial intelligence and robotics have huge implications for the right to privacy.

The development of artificial intelligence and robotics brings us nearer to a future dominated by automated decision making.

It is an issue deemed sufficiently important to be discussed by the International Conference and it is just one example of how this network can provide policy leadership.

The International Conference is collectively resourced and can be called upon by governments, ministers and agencies to provide guidance in all aspects of data protection and privacy.

Encryption, data portability, biometrics, facial recognition technology, robotics, artificial intelligence, algorithmic decision making, the Internet of Things are all examples of where the future of privacy is going.

Given the technological changes that are bearing down on us, it seems apparent that individuals should have new rights and new access to exert control over their personal information – and even more sunlight and electric light.

ENDS