Privacy Commissioner
Te Mana Matapono Matatapu

ASIAN PRIVACY SCHOLARS NETWORK

KEYNOTE ADDRESS BY PRIVACY COMMISSIONER JOHN EDWARDS

TUESDAY 13 DECEMBER 2016 | UNIVERSITY OF AUCKLAND BUSINESS SCHOOL

Kia Ora Tatou. Nga mihi kia kotou e tene wa.

Language

When we come here together, representing many different countries, languages, cultural and legal traditions to talk about "privacy", how can we be sure we share a common understanding of the concept? Are we all talking about the same thing, or do we each have slightly different concept in mind when we use the term?

I have to admit, sometimes when I am in an international forum, I wonder if there aren't quite a range of different understandings.

If you look at legal writing, I think we can agree that the most general definition is freedom from interference or intrusion, or the right "to be let alone".

But privacy means different things to different people, to different cultures, to different communities.

At the same time, we live in an increasingly connected, global world, in which it is often said, information or data knows no borders and information originating from an apparently simple domestic transaction might pass through three or more countries.

So there's a tension, and arriving at a common definition or meaning of the concept of privacy is one of the challenges privacy regulators and the international privacy community face.

In the recent Hollywood film *Arrival*, the actor Amy Adams plays a linguist who is recruited by the US government to communicate with newly arrived extra-terrestrial visitors.

The main conflict in the film comes from the humans trying to learn the aliens' language. The aliens, for example, talk about a "weapon." Debate rages in the film about whether they mean a weapon, or a tool. Both terms are quite similar, but the slight differences in meaning bring dramatically different consequences.

'Tool' as a word builds trust while the word 'weapon' instigates fear and mistrust.

When we debate the term 'privacy,' we are also trying to find common ground between different cultures' definitions of (ostensibly) the same thing.

In a world with human languages numbering between six- and seven-thousand, the word 'privacy' can mean different things. These meanings are often nuanced and shaped by culture, society and history.

Privacy in history

In our early human history, privacy was a lesser priority, in conditions of subsistence existence.

Living in small, rural communities, most humans had little concept of privacy until fairly recently. Sex, breastfeeding, domestic quarrels, toileting and bathing were usually performed in front of other members of the small communities that were the cradle of humankind.

The anthropologist Jared Diamond observed that "*because hunter-gatherer children sleep with their parents, either in the same bed or in the same hut, there is no privacy. Children see their parents having sex*". In one tribal society, parents took no special precautions to prevent their children from watching them having sex: they just scolded the child and told it to cover its head with a mat.

In the 1951 book *Patterns of Sexual Behaviour*, the American researchers Clellan Ford and Frank Beach, studied the sexual behaviour of 191 cultures and found that the preference for privacy was instinctive. In nine of 12 societies where homes have separate bedrooms, people preferred to have sex indoors. In those cultures without homes with separate rooms, sex is more often preferred outdoors.

Often the desire for privacy was overridden by the need to survive. The anthropologist Jean Briggs found herself being ostracised by her native North American Utku host family after daring to explore the wilderness alone for a day. She made the observation "how forlorn I would be in the wildness if they forsook me. Far, far, better to suffer loss of privacy".

The concept of universal individual privacy is usually associated with Western culture and as you can see it was a concept foreign to some cultures until recent times.

There's also the subtle distinction between privacy and secrecy. Ontologically, the word privacy has been described as an example of an untranslatable lexeme with many languages – there is simply no specific word for it.

In Russian, the words for solitude, secrecy and private life combine to capture the essence of what we mean by the term privacy.

Other languages adopt privacy as a loan word – *privasi* (pron: PREE-vah-SEE) in Bahasa Indonesia or *la privacy* (pron: PRAI-VA-SI) in Italian.

In Mandarin Chinese, privacy means secrecy, solitude, and seclusion – all or each of these things.

Meanwhile, in Islamic cultures, the notion of privacy has no conceptual autonomy in legal literature. Rather, it has to do with a cluster of attitudes and norms.

A famous line in the Qur'an says "do not enter houses other than your own unless you have asked permission and greeted the inhabitants!"

The Qur'an also includes a general injunction against prying and spying on people.

In New Zealand, Western concepts of privacy, especially legal concepts, are centred on the individual - Western intellectual ideas have for many centuries developed along the lines of the rights of the individual.

However many indigenous peoples, including New Zealand Maori, have a different focus that is more likely to emphasise the good of the collective, the rights of the collective and solutions for the collective.

The Maori word *tapu* perhaps provides us with the best analogy to aspects of European concept of privacy with its several overlapping shades of meaning - including sacred, prohibited or unclean.

New Zealand Maori legal academic Khylee Quince described *tapu* as: “A status that exists when a person, place or thing is placed under restriction or dedicated for a particular purpose. She says in a legal sense, this relates to the inviolability of the human person – to be free from physical assault and interference.

A related concept is that of *mana* which Khylee Quince describes as “my reputation and my self-esteem – both how others think of me and how I think of myself”.

Mana and tapu combine in many settings to produce ideas and reactions which closely parallel European responses to privacy invasions.

In a Law Commission review of this country’s Privacy Act, the reviewers observed that in the State’s drive to collect health information, if Maori are confident that their information will be used in a way that is empowering or mana-enhancing, they will be more willing to agree to the collection and use of that information.

But if Maori believe that information will be used in a way that is derogatory to Maori and which diminishes mana, then they will be reluctant to share information.

Steps toward a common understanding

Robert C Post of Yale Law School wrote in 2001 that “*privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all*”.

People are different and our ideas of privacy are shaped by culture, religion, language, history and architecture.

Through the ages, there has been no single unifying concept of privacy, but that’s changing.

These different perspectives that existed have slowed the establishment of a set of internationally accepted principles on privacy.

The constitutions of many countries do not explicitly mention privacy and an individual’s right to privacy.

In Indonesia, for example, the Constitution does not explicitly mention privacy. However, Article 28(g) protects the right to dignity and “to feel secure”, concepts that are often related to the right to privacy in the national constitutions of other countries.

In Kenya, the constitution specifically protects the right to privacy. It states "every person has the right to privacy, which includes the right not to have:

- their person, home or property searched
- their possessions seized
- information relating to their family or private affairs unnecessarily required or revealed
- or the privacy of their communications infringed."

But according to *Privacy International*, civil society groups in Kenya report it is difficult to work on privacy and surveillance in that country as the issue is not widely deemed important by society in general.

This is in part because the increased number of security threats has enabled a strong national security discourse to overshadow concerns about individuals' privacy. *Privacy International* notes that privacy is often subsumed by other human rights issues.

A universal acceptance of a singular definition of privacy is not going to happen because it would be impossible to get agreement.

How do we get the United States, China, the Republic of Korea, and Ghana, for instance, to agree upon a universal set of privacy expectations? More importantly, should we even try? Do we need a global standard of privacy? Is it possible to abstract what are described as privacy values to a level that receives acceptance across the entire global community?

One of the abstractions is “data protection”, which I see as a subset of a wider group of privacy values, but which is a term used interchangeably with “privacy”, which can add to the confusion.

For example, we see an increasing diversity of countries in the Asia Pacific region, in Africa adopting data protection laws, but the underlying values and social and cultural traditions on which these laws are based may represent a quite divergent approaches to the concept of privacy in those communities, from that which informs the similar looking laws in countries in Western Europe or North America, which themselves begin from quite different points when it comes to recording the respective rights and obligations on data processers/generators or users, and data subjects.

There’s a view among some technologists as well as some governments, that accommodating privacy concerns and safeguards is a curb on technological innovation or on the aspiration of building a better model citizen, more efficient cities and safer societies.

For example, China’s government is exploring plans for a social credit system which utilises big data to hold citizens to account for their financial decisions. To do so, the government is enlisting some of the country’s best-known companies to help create it.

According to the *Wall Street Journal*, Alibaba's Alipay payment system is one of eight companies involved in the first experiments around China's social credit scoring system.

Alipay will compile scores based upon a user's smartphone brand and what they buy online, before offering users perks for high scores. The information helps the government monitor and reward citizens with higher credit scores.

The scores will not only be based on a user's lending and spending numbers but also on what the money is spent on. "If friends have a poor lending reputation, this reflects badly on the person, just as prolonged playing of video games," one report explained. "Buying diapers indicates responsibility and scores therefore well."

China's government says it wants to roll out the social credit score program nationwide by 2020.

Meanwhile in the UK, the British financial regulator, FCA, has warned that insurance companies could use available data to identify customers who shop around and those who do not, and could differentiate their pricing accordingly.

The warning comes as the availability of more personal information on social media and devices such as "telematics boxes," that monitor driving habits, mean the insurance industry is moving towards quotes based on observed behaviour of individuals.

One telematics provider, Octo, launched an app this year that shared customers' driving data with insurers so that they could bid for custom. It claimed that the safest drivers would get the lowest premiums.

Also earlier this year, the British insurer Admiral announced it planned to use Facebook status updates and "likes" to help establish which customers were safe drivers and therefore entitled to a discount.

Privacy advocates called the proposal intrusive and it was blocked by Facebook hours before it was due to launch.

Privacy and government surveillance

Due to Edward Snowden, one of the hottest privacy debates of recent times has been about the relationship between security and intelligence agencies and the community - how those agencies derive their legitimacy, and how that legitimacy can be harmed, or enhanced.

So how does society engage in the conversation with government and big business when it lacks the information necessary to make a fully informed choice about the "balances" and trade-offs?

Can accountability mechanisms keep pace with change, and not get left behind and be rendered obsolete?

These are questions which roil around the public discourse in many countries or hang unspoken but are of no less concern in others.

I want to take a slightly different tack from one which you might expect a privacy commissioner to take, in discussing the Snowden revelations. A lot of people both within, and outside the countries directly implicated in the material he leaked, simply didn't care. Or they expected the Governments to be doing exactly what was reported. In some countries there is a very high level of comfort for agents of the state having access to whatever information they need to keep people safe and to stop terrorists.

We saw outrage and shock from some NGOs, and we saw righteous indignation from some countries, which within a few months of the NSA/GCHQ interception activities being revealed were exposed as being involved in exactly the same kind of activity.

The fact that those revelations coincided with an explosion in the data ecosystem has lead to a complex and interrelated series of responses, which do not necessarily as a whole, demonstrate a consistency of values and imperatives.

In April 2015, the UN Human Rights Council adopted a resolution to appoint a Special Rapporteur on the right to privacy. The resolution directed the Special Rapporteur, amongst other responsibilities, to report on alleged violations of the right to privacy including in connection with the challenges arising from new technologies.

Those developments are reactive responses to perceived abuses.

At the same time Governments are trying to capture for their populations, the benefits of the digital economy.

A consensus seems to have developed that increasing participation in the digital economy is a good thing, that there are enormous quantifiable benefits to be had from investing in online infrastructure to deliver a range of social and economic services.

A precondition to that engagement, to the realisation of the benefits of technology is that the users must have trust in the system, and that without trust that personal information will be kept and transmitted safely and securely, those benefits will not be realised. When privacy is a prerequisite for Governments and businesses benefitting from technology, the value proposition for agreeing on some common and consistent approach to privacy, or data protection, call it what you will, becomes evident.

We saw this at the OECD Ministerial in June in Cancun. It was entitled The Digital Economy: Innovation, Growth and Social Prosperity.

Paragraph 5 of the Ministerial Declaration recorded Ministers' commitment to:

> *Promote digital security risk management and the protection of privacy at the highest level of leadership to strengthen trust, and develop to this effect collaborative strategies that recognise these issues as critical for economic and social prosperity, support implementation of coherent digital security and privacy risk management practices, with particular attention to the freedom of expression and the needs of small and medium enterprises and individuals, foster research and innovation and promote a general policy of accountability and transparency;*

If we abstract privacy to a level of trust in personal information, then it doesn't necessarily matter whether one country regards "privacy as a fundamental human right" and another finds that concept so vague as to be unmanageable. It avoids a primacy of rights, for example setting freedom of expression against individual privacy.

If you ask the question, "what is required to maintain trust in our management of personal information" you can move past prescriptive rules and absolutism, and address the underlying question of how competing needs from personal data can be accommodated with a single framework.

Take the security and intelligence element for example. Few if any people would deny the legitimacy of the state to act to protect its population. Most of us would regard it as a duty. We entrust agencies with powers in order to allow them to do so. We expect that trust to be respected.

The fact that in certain prescribed circumstances, an agency of a state will need to access and use personal information other than for the purpose it was provided, should surprise no one. If we can agree on a set of principles governing how that access should be granted, and have some transparency to ensure that those principles are respected; we should be able to meet the apparently competing needs.

There is as yet no internationally agreed standard for the conduct of intelligence and security activity. In my view efforts should be made to develop and articulate some. If that sounds like naïve folly, then let me remind you that even the conduct of war is subject to internationally enforceable agreements.

That need was starkly demonstrated to me at a recent International Intelligence Oversight Forum in Bucharest. I was struck by the lack of agreement on the meanings of basic terms. The same activity (for example a requirement of telecommunications companies to retain content and or metadata for a certain period) was described as "mass surveillance" by some observers, a term strenuously rejected by many.

The same observers might regard as "mass surveillance" a warehousing of communications data accessible by search terms which had to be individual approved by an overseeing judge. The architects and administrators of that scheme argued that it was entirely consistent with international norms requiring "lawful and proportionate" access to private communications.

But until we have an international conversation about the parameters of that legitimate activity, and the elements required to maintain trust (such as independent oversight, transparency reporting, a sound basis in the rule of law) we are destined to continue the cycle of criticising the activities of some countries, while maintaining a blind spot in respect of our own.

Regulatory models

Governments have three broad options on how they choose to regulate privacy and data protection. They follow the three economic models that range from laissez faire to a more prescriptive command-type economy.

The first is an environment where governments and organisations can do anything with personal data. There are no safeguards and no rules except for what can be negotiated as a private contract. The individual is basically powerless to influence or even to know the information which organisations hold about them and the Government has few if any privacy statutes that protect personal information. This is the most permissive model.

At the other end of the spectrum is a quite prescriptive model, under which clear legal authority is required to make use of personal information beyond that which has been expressly consented by the data subject.

In the middle, there is the mixed model of market forces and government intervention. This regulatory approach introduces friction into the processes by which organisations collect, store, and disclose personal information. Individuals also have access to information about them and have measures of redress if their personal information is being used unlawfully. This regulatory model puts the onus on an affected individual to enforce their rights, and creates litigation risk for an agency that decides it can do what ever it wants with personal data

This is the approach we have adopted in New Zealand – a law based on OECD privacy principles that are flexible enough to foster economic growth and technological innovation while also giving individuals the right to exert some level of control over their personal information.

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

The World Bank is no cheerleader for privacy or data protection, and didn't express a preference about what the correct model might be, however it did note that inconsistent approaches add friction and inefficiency into international trade and could be an impediment to realising digital dividends.

Promote and deploy Privacy-by-Design, Privacy Impact Assessment and privacy enhancing technologies

It would be overly simplistic and plain wrong to think that the actions of security and intelligence agencies are the sole drivers of the international conversation on data privacy.

We are seeing in increasing trend in consumer demand for privacy protective products, whether in hardware, like the iPhone, or in software such as encrypted messaging services such as WhatsApp, or temporary media like Snapchat.

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 in 2016. We have seen Apple, Facebook and Microsoft in the courts to stand up for their customers' rights to privacy. We have seen Google and Facebook and many others subject to the high profile regulatory attention of European data protection regulators.

So rather than framing privacy regulation as a drag, perhaps we can reframe it as a market leading response to consumer demand.

It is another trick of language to establish false dichotomies. We've all heard the false argument that you can have privacy or security. Similarly, it is in the interests of some to argue that strong privacy regulation is incompatible with innovation.

In my view, there is no trade-off 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.

Nor does privacy only mean secrecy, notice and consent, or a number of other limited and culturally specific manifestations of individual autonomy. New concepts are emerging within the family of privacy related rights, which don't fit with a limited linguistic construction of the term.

Think of the concept of data portability, the right to receive your data in a machine-readable format so you can take it to another provider of the service that originally collected it from you.

Just as number portability has proved crucial in promoting competition in the mobile phone sector, 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. It's a concept we are looking at closely here.

Control

In concluding, despite the difficulties in reaching a universal understanding about the nature of privacy, a common understanding of the elements of privacy is emerging, in New Zealand and in many other countries.

Our laws reflect this need to be able to protect and control information about ourselves and our need to withdraw - physically or mentally - from society, or to exercise some autonomy over our information, or at least be informed about it.

Privacy, as defined by this common understanding, is important to ensure that we feel secure. If we are unable to control who knows information about us, we will feel insecure - at least in part because the boundaries of our relationships become uncertain.

We started with language – what we need is a deep discussion about what we mean when we talk internationally about concepts like privacy, and data protection, about trust. We need to understand not only what we have in common in these understandings, but also to make a greater effort to question our assumptions about how other jurisdictions approach these questions and values, and if we see difference, to make a genuine effort to understand that difference, rather than to assert a cultural and or legal superiority.

This is the ideal forum for that conversation and it is my great pleasure to welcome you and to open that discussion.

ENDS