Transparency International Leadership Integrity Forum

Privacy Commissioner John Edwards

27 September 2016

Office of the Auditor General, Wellington

SUMMARY:

Address to public sector chief executives: Privacy Commissioner's perspective on prevention of corruption, such as training in incorporating tools to identify and address corruption, the ways to build stronger integrity systems and/or the benefits from having a public sector that is trusted.

INTRODUCTION

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

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

That phrase is attributed to Justice Louis Brandeis, among other things, the first Jewish judge to be appointed to the US Supreme Court.

Before being appointed to the Bench, Brandeis taught at Harvard Law School.

In 1890, he and his colleague Samuel Warren published the seminal article "A Right to Privacy" in the Harvard Law Review and in so doing, established the right in US law.

Brandeis and Warren described the right to privacy as an already existing common law right which embodied protections for each individual's 'inviolate personality'.

In my brief comments I will discuss the relationship between privacy and transparency, and how a wide and principled understanding of the nature of privacy

is essential for the maintenance of public trust, which is also the aim of initiatives designed to enhance transparency.

You'll find more connections between the topics, which at first glance might seem to be in opposition, than you might have first thought.

There are many instruments of transparency, such as the Public Finance Act, but one of the most important, the OIA, was the topic of an earlier talk at this forum.

In addition to providing for the principle of availability of official information, that Act in 1982 established as a legal right the right of an individual to find out what information a government agency has about them.

That right, in 1993, was transferred into the Privacy Act.

It is difficult to overstate the importance of a right of access to one's own information as a means of enforcing transparency on an agency of the state.

The Court of Appeal here has described it as being of "constitutional significance".

My counterparts in Latin American jurisdictions call the right "habeas data" - "bring up the data" - recalling that most fundamental human rights writ and instrument of the rule of law: habeas corpus or "bring up the body".

That right, combined with the right to have the reasons for decisions affecting the individual - which has remained in s.23 of the OIA in relation to public sector agencies - is a check which ensures that government is accountable for its actions which affect the rights of individuals.

It is a check against corruption, an essential aspect of our system of accountability, and needs to be done better in some parts of the public sector.

PRIVACY

When many in the public think of privacy, they think of the right of individuals to keep things out of view – or within your own control or determination.

And that's an important dimension.

But when we at the OPC apply the Privacy Act, we are looking to a much wider expression of privacy rights.

Information privacy principle 3, for example, imposes an obligation on agencies - on your agencies - to ensure people are aware of the reasons you are collecting personal information, who will have it, and what it will be used for.

In other words, to be transparent about your information management practices.

We see the same obligation in the law relating to information matching.

Rule number one in the information matching rules is:

> *Agencies involved in an authorised information matching programme shall take all reasonable steps (which may consist of or include public notification) to ensure that the individuals who will be affected by the programme are notified of the programme.*

One of the most common corrupt practices undertaken by public officials in New Zealand is the corrupt use of official information.

Public servants who are trusted with access to citizens' personal information use that information for their own benefit.

When detected, this practice is punished with termination of employment, and even prosecution.

But how do you know whether it is happening?

We need to have far better systems for auditing access to data bases.

Employee "browsing" is one of the most common complaints (after access) we come across – the inappropriate accessing of official records.

This kind of activity undermines trust in Government.

At the recent OECD Ministerial Meeting on the Digital Economy in Cancun, the participating Ministers, including the Hon Amy Adams, 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 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;*

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

There is no small coincidence with Better Public Services result areas 9 and 10:

> ***9.*** *New Zealand businesses have a one-stop online shop for all government advice and support they need to run and grow their business.*
>
> ***10.*** *New Zealanders can complete their transactions with the Government easily in a digital environment.*

In order to have trust and confidence in an online environment, Government needs to provide assurance to the public and to business that they can interact with it online safely.

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

TRUST

New Zealand was one of the first countries to establish a Privacy Commissioner by law – doing so in 1976.

Those were pre-internet days, the days of the Wanganui Computer Centre, and the newly-established Commissioner was given jurisdiction over law enforcement data.

Forty years later, public concerns about security and privacy remain, but for different reasons.

Revelations of data breaches, concerns about mass surveillance without due process, secret courts established to oversee secret processes for authorising access to information.

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”.

In terms of privacy, my role is to be the electric light.

It’s important we understand and help support how we in New Zealand will respond to the challenges faced by many countries in an uncertain geopolitical climate, with tremendous advances in technology and data collection.

Transparency in our way of government is a key part in checking the abuse of power and protecting our reputation as being one of the least corrupt places in the world to do business.

The equation is simple – privacy supports trust and confidence.

Transparency also supports trust and confidence.

Privacy plus transparency equals increased trust.

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 also has big cost implications for government agencies.

There’s an increased cost to collecting personal information because it becomes encumbered with the cost of checking the accuracy of that information.

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

TRANSPARENCY

Wikileaks, the Snowden revelations, intelligence and security botch ups and law reform have made surveillance a household word.

You could make a strong argument that non-state actors and partially informed commentators have emerged to fill a vacuum and that vacuum was created by a lack of transparency.

There's also been a growing unease at the growing power of big companies, Facebook, Google, Amazon, and others.

But there is also the argument used by some that we will assume everything is known about each of us and give up - the 'privacy is dead: get over it' approach.

I believe the reverse is true.

People are becoming more aware and concerned about their privacy and the fate of their information.

Our latest biennial tracking survey – carried out earlier this year – showed approximately two-thirds of New Zealanders continue to be concerned about privacy.

Nearly half of New Zealanders have become more concerned about individual privacy issues over the last few years.

Our surveys show there is clearly a higher level of trust when a government agency collects a person's data, and less if it is done by a commercial organisation.

But whether it is a public or private sector agency, one of the expectations under the law is that agencies are transparent about what they do with it.

As the unease about mass surveillance or mass collection of personal information grows, privacy advocates are expecting greater transparency from the organisations that amass and dissect our information – more electric light.

TRANSPARENCY REPORTING

There are of course limits on confidentiality. A person or organisation giving financial support to terrorists should not expect their transaction details to remain private.

Many in society are unaware of the limits on confidentiality, so when Police access a year's worth of banking records about a journalist in the course of an investigation into an illegal hack, that can cause alarm.

In my view it would be consistent with the principles of transparency underlying the Official Information Act, for Government agencies to make public the number of instances in which they access private data. For a variety of reasons that is not happening.

To fill this vacuum, my office has taken a position in support of commercial entities engaging in transparency reporting, that is, being transparent about how many requests for personal information they receive from government enforcement agencies, and how they respond to them.

We undertook a pilot on this last year. We worked with 10 companies from a the utilities, telecommunications and financial services sectors between August and October last year.

Our goal was to produce a report on how businesses generally responded to requests for information.

The results: 11,799 requests for personal information, of which 11,349 were complied with and 449 declined.

We are currently doing another transparency pilot with different organisations – keep an eye on our website to see the results.

Transparency reporting like this has been endorsed by the International Conference of Data Protection and Privacy Commissioners in a 2015 resolution.

ALGORITHMIC TRANSPARENCY

Elsewhere in Government, we see a growing enthusiasm for "big data".

Regardless of your level of confidence in what I have taken to calling the ‘new alchemy’, of data scientists over-selling the potential of their algorithm’s ability to turn base metal of raw administrative data into the gold of improved public policy outcomes, everyone in this room is operating under clear instructions to use data better.

This is going to throw up increasingly complex problems, that may entrench, rather than assist to resolve, social inequities and misallocated resources.

One emerging threat in this area 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. We’ve seen 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.

If you don’t allow this transparency, and instead rely on the data without questioning it, then you could miss opportunities, or end up breaking laws against discrimination.

This issue was flagged in the White House Report on Big Data, which was released in May of this year.

Algorithmic transparency isn’t enough on its own, though.

Using an algorithm to assess a person’s suitability for a loan is one thing. Getting it wrong could lead to an inconvenience, or even tangible harm from the denial of credit. Think about the potential for harm in the use of predictive risk modelling algorithms to make and act on assessments about the life outcomes of children.

CONCLUSION

I support Transparency International's vision of a world with trusted integrity systems in which governments, politics, business, civil society and the daily lives of people are free of corruption.

New Zealand's continuing reputation as a high trust, high integrity society depends on transparency and the right to privacy.

Transparency and privacy are not mutually exclusive.

New Zealanders are entitled to have both.