OUR PRIVACY ACT: 30 YEARS AND 25 YEARS REFLECTIONS

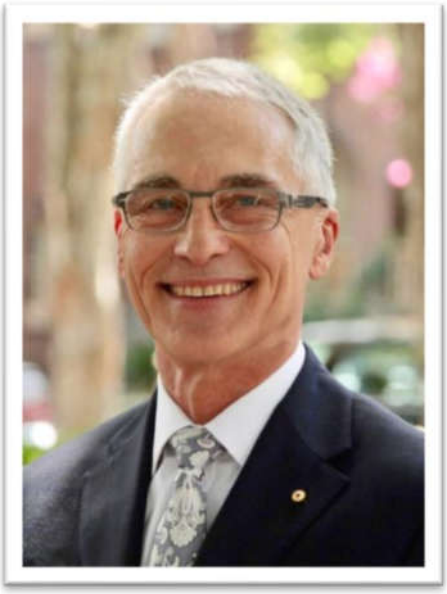
By: Malcolm Crompton, Anna Johnston, Marie Shroff, Tim McBride and Dr Paul Roth

Celebrating milestone birthdays for our Privacy Legislation

As Australia's Privacy Act turns 30, and New Zealand's Privacy Act turns 25 we asked a number of respected privacy practitioners to turn their minds back to the introduction of the legislation and forward to our world today and provide us with their insights on how the legislation has stood the test of time and hopes for future privacy reform.

We are privileged to be able to share with you the reflections of Malcolm Crompton, Anna Johnston, Marie Shroff, Tim McBride and Dr Paul Roth.

Malcolm Crompton, IIS



Malcolm Crompton is the Founder, Lead Privacy Advisor and former Managing Director of Information Integrity Solutions Pty Ltd (IIS), a global consultancy based in Asia Pacific, specializing in data protection and privacy Strategies.

As Australia's Privacy Commissioner from 1999 to 2004, Malcolm led the implementation of the nation's private sector privacy law. He hosted the 25th International Conference of Data Protection and Privacy Commissioners in Sydney in 2003.

Malcolm was the founding President of iappANZ

Can you share, anonymously, a privacy debacle you were involved in any way with in your career that has burned itself in your memory?

Perhaps both a privacy debacle and a privacy success.

A few years ago, we worked with an Australian small to medium, family owned and run business. The news media suddenly proclaimed that it had suffered a huge data breach. The media claimed that the personal information of hundreds of thousands of individuals had been stolen and eventually posted on the Net (not even the Dark Web) for all to see.

We were invited in to assess the situation and to advise on what to do.

We put together a data breach team for the business. The team included forensic experts, security experts and issues management experts. One of our rules from the very beginning was that the Privacy Commissioner should be 'first to know' on any developments as we analysed the situation.

Our forensic partner on the team did an incredible job of discovering just who had actually been affected. In the end, we concluded that the personal information of less than half a dozen individuals had been compromised. The team ensured that each of those individuals was looked after meticulously and while it was stressful for the affected individuals along the way, no actual harm was done.

The team also assisted the client's business partners to improve their security even though none of them were actually affected either.

As a result, instead of a small business going to the wall through crippling costs that could have included large scale, very expensive and unnecessary data breach notification, the business survived, had much better data security and was able to begin the process of rebuilding trust with its business partners and client base.

We wrote up this data breach as a case study which is available on the IIS website at: https://www.iispartners.com/s/Case-study-Successfully-navigating-a-data-breach.pdf.

Is there one special professional achievement you would like to share with us?

The highlight of my career was the invitation to become the Privacy Commissioner of Australia. I was the third to hold the position after Kevin O'Connor and then Moira Scollay. My term ran from 1999 to 2004.

I came into the role just as the Privacy Act was extended from its initial federal government coverage to apply to much of the private sector.

In the five years of my term, with a very small increase in funding from the government and considerable anxiety in parts of the private sector, we ensured that the extension came into effect smoothly.

We wrote guidelines and information sheets, consulted widely on their development and gave untold presentations.

We had no advertising budget but made good use of the media to get the message out to business as well as to individuals whose privacy the law was intended to protect. Controversy over some aspects of our work helped a lot. It meant we were newsworthy! The events in the USA on 11 September 2001 often added to the controversy. We developed and used four 'punchlines', some of which have lasted to this day:

- "good privacy good business"
- "privacy partners privacy solutions"
- "my privacy my choice"
- "respecting privacy"

There is no doubt that we met the old adage of 'punching above our weight'.

It was an exhilarating, team effort. Indeed, the staff in the Office of the Federal Privacy Commissioner, as it was then, were probably the best team with whom I have ever worked. They were dedicated, high calibre and worked very hard.

In fact, there are two special professional achievements that I would like to share. The other was working with a small group of people to build support for and eventually establish iappANZ and becoming its founding President in 2008.

Do you have a "connected" home? Why/Why not? What would change your mind?

No way. Not yet. There are clearly advantages in many of the concepts such as remote energy management or remote security management.

But at the moment the market is breathtakingly immature when it comes to security let alone privacy. Too many small start-ups rush to market on miniscule budgets and cut corners all along the way. Almost none have robust security or privacy by design processes let alone any independent assurance that they are actually meeting any of the vague claims that they may make about security and privacy. In fact, for many of them the value proposition is not the service provided but the personal information that they collect and monetise.

Maybe this will change as the market matures or maybe it won't. Maybe it will only change when the law catches up and decrees appropriate standards and enforces compliance.

To put it another way: your home is your castle. Your digital home should still be your digital castle, not something with the front door wide-open, inviting all kinds of unknown threats and unwanted surveillance.

What is your hope for the next round of reform?

The big missing link in privacy law is a framework that genuinely holds organisations to account for their handling of personal information. Privacy law in Australia and most of the world (including Europe under the EU General Data Protection Regulation) is still excessively reliant on an approach based on 'catch me if you can', complaints-based enforcement. This is coupled with embarrassingly underfunded compliance and enforcement.

For the last ten years, leading privacy thinkers, especially people in the US such as Marty Abrams at the Information Accountability Foundation, have sought to put into place a more effective accountability framework. This has been partially successful. For example, it led to Australian Privacy Principle 1.2 that has been in place since 2014. More recently, this effort has also directly contributed to a stronger accountability framework being written into the EU GDPR.

However, there is still a long way to go.

The simplest way of demonstrating this is to look at the vast sums of money spent on financial information accountability worldwide: corporations law everywhere requires firms to spend billions of dollars on financial accountability, as illustrated by the size of the Big Four accounting firms alone. Compare this with the spend on personal information accountability: it is trivial by comparison. The spend will remain trivial until privacy law or other law puts obligations in place for personal information that more closely matches the obligations for financial information.

Then again, perhaps this kind of change won't even come from the legislature. Instead, it may come about if the accounting profession catches up and recognises that information is an asset class that must be brought to account on the balance sheet. It will show that information is the most valuable asset in most organisations. Leadership will respond accordingly.

One way or another, if 'personal information is the new oil' then the current weak accountability framework cannot

continue. Change will come. The only question is how long do we have to wait.

Where do you see the privacy profession heading in the next 30 years?

The privacy profession is likely to become part of a wider, more deeply appreciated information governance profession. It will have stronger links to the professionals who deliver risk management, asset management and audit.

Privacy will no longer be treated as a second-class compliance issue.

Instead leaders in both public and private sector organisations will realise how much customer or citizen trust depends on respect for individuals and the information about them combined with credible audit, assurance, accountability and redress systems. The profession will evolve accordingly.