80's Icon Set

Photo credits: Illustrations by Vecteezy
## Contents

1. / **VICE PRESIDENT’S FOREWORD**  
   Veronica Scott  
   page 4

2. / **EDITORS’ PREAMBLE**  
   Lyn Nicholson and Katherine Gibson  
   page 5

3. / **A WORD FROM THE NEW AUSTRALIAN PRIVACY COMMISSIONER**  
   Angelene Falk, Australian Privacy Commissioner  
   page 6

4. / **PRIVACY ACT’S 25TH ANNIVERSARY – CHANGES AND CHALLENGES OF THE PRIVACY PROFESSIONAL**  
   John Edwards, New Zealand Privacy Commissioner  
   page 9

5. / **OUR PRIVACY ACT: 30 YEARS AND 25 YEARS REFLECTIONS**  
   Malcolm Crompton, Anna Johnston, Marie Shroff, Tim McBride and Dr Paul Roth  
   page 11

6. / **THE “TECH CONFERENCE” CIRCUIT: WHERE ARE THE PRIVACY PROFESSIONALS?**  
   Alan Mihalic  
   page 21

7. / **GDPR IS NOT A REGULATION**  
   Dr. Andrey Ivanov  
   page 23

8. / **BOARD TALK – DEALING WITH DATA PRIVACY AND THE KEY DATA RELATED ISSUES FACING BOARDS TODAY**  
   Kelly Henney and Alisha Malhotra  
   page 26

9. / **LEGISLATION CORNER: AN UPDATE ON THE PROPOSED CONSUMER DATA RIGHT**  
   Peter Leonard  
   page 29

10. / **THE GDPR STARTS TO BITE – TOP 5 TAKEAWAYS FROM THE FIRST ENFORCEMENT NOTICE**  
    Frith Tweedie and William Fussey  
    page 33

11. / **UPCOMING EVENTS**  
    page 35
**Author Guidelines - subject to the discretion of the editor**

**Criteria for articles**

1. An original article – one that is different and reworded from any article that you have published to a broad audience on this topic AND has a different heading than any article you have published on this topic, but may be based on an earlier published article.

2. Generally, between approximately 600-2500 words. This broad range notes that subject matter may vary from technical and complex to short and topical.

3. For a longer, more technical article, we may publish by instalments.

4. For articles that have been broadly published, we may publish a summary and link to full text.

5. We cannot accept images sourced from the internet due to copyright. Images from ATMOSS or ADDS will be accepted.

**Copyright and Licence**

1. Copyright in the article at all times remains with the author.

2. No fees are payable by iappANZ.

3. Author grants to iappANZ a world-wide royalty-free non-exclusive licence to publish the article in material form and online to reproduce the article for those purposes and to edit as is reasonably required by iappANZ for publication purposes.

4. The author may republish the article elsewhere once it has been published in the journal.

**Acknowledgement**

1. iappANZ will use all reasonable endeavours to ensure that the author’s name is published with the article.

---

**Our contact details**

Privacy Unbound is the journal of the International Association of Privacy Professionals, Australia-New Zealand (iappANZ), PO Box 576, Crows Nest, NSW 1585, Australia (https://www.iappanz.org/)

If you have content that you would like to submit for publication, please contact the 2018 Editors: Lyn Nicholson (Lyn.Nicholson@holdingredlich.com) and Katherine Gibson (katherine@gibsonslaw.co.nz) the co-chairs, covering both AU and NZ together with Veronica Scott, Nicole Stephensen and David Templeton.

If you have an idea for the journal please share it with us. We are keen to broaden content and scope to all things privacy related and all aspects of the privacy profession.

Please note that none of the content published in the Journal should be taken as legal or any other professional advice.
Here’s a bit of personal information: I am an 80s tragic. Unashamedly so. And so it gives me great pleasure to introduce our jam pack edition that reflects on where we have come from since then, following 30 and 25 years respectively since the Australian and New Zealand Privacy Acts became law. For privacy professionals the key take aways are: the globalisation of privacy regulation and dealing with security risks and the impact technology.

We are delighted to have interviews from both the recently appointed Australian Information Commissioner, Angelene Falk and the New Zealand Privacy Commissioner John Edwards, as they reflect on the changes we have seen in privacy through the technology revolution in particular (which are showing no signs of slowing down) and how our privacy and data protection frameworks have been able to respond, as well as looking forward to the work their Offices are focussing on. We also bring you the shared reflections of some of our most experienced and respected privacy practitioners, Malcolm Crompton (former President of iappANZ and former Privacy Commissioner), Anna Johnston, Marie Shroff (former New Zealand Privacy Commissioner), Tim McBride and Dr Paul Roth. Their passion for privacy has not waned – they discuss the changes they have observed and what can be done better and also do some crystal ball gazing. We also have an interesting review from Alan Mihalic about the how the (jam packed) technology focussed conference circuit lacks a proper focus on privacy and cyber security which is often an afterthought.

And then of course there is the GDPR which effectively marks the 30th anniversary of the Privacy Act in Australia. Dr Andrey Ivanov reports on his research which found that GDPR compliance does not have to be painful if your data governance is in order. He reminds us that GDPR is a customer-centric issue. He cites Air New Zealand as a great example of an organisation that has taken a customer-centric approach to GDPR (led by iappANZ’s very own Jacqueline Peace). Picking up on the theme of good governance, a great piece from Kelly Henney and Alisha Malhotra from KPMG discussing the key data related issues facing boards today. Good governance as well as trust, security and a data strategy means organisations don’t have to compromise on tech innovation.

The veritable Peter Leonard (newly appointed Professor of Practice at UNSW Business School) explains the new Australian Consumer Data Right that is set to be introduced next year which he says heralds a new approach to competition regulation through data access and sharing. And hot off the press from Frith Tweedie at EY Law is a report on the takeaways from the first formal GDPR enforcement notice (that was quietly issued to a Canadian firm back in July).

And finally, a quick plug for our final iappANZ national Privacy Summit which is taking place on 1 November in Melbourne followed the next day by two workshops – (both of which are now sold out). We will be holding our AGM early in the morning before the Summit too and we look forward to seeing you all there. Thanks to all our members for their support this year and your response to and vote on the resolutions passed at our recent EGM. We are now putting in place a plan for a smooth transition to IAPP over the coming months. As always, if you have any questions or queries please do not hesitate to reach out to any of the board members.
In this edition your editors are reflecting some nostalgia. In privacy things are ever changing and it often seems that people are looking always forward to the next big thing and new developments.

In this issue we invite some long term practitioners to pause and reflect on the changes they have seen as we celebrate 30 years of the Privacy Act in Australia and 25 years in New Zealand.

We are delighted that both regulators have been able to contribute.

We also introduce some forward looking content that may offer you a different perspective, illustrating the challenge of managing privacy in the modern world that is a continually evolving.

Finally, as we prepare this edition we are mindful this journal is not part of the standard iapp offering, being unique to iappANZ and may not continue into 2019. If so, we will make arrangements for iappANZ members to have access to the archive of rich journal material.

We also note that the final 2018 edition will be the Summit wrap up edition for those of you unable to make it and for those who attended, but are looking for some insights from others.

Enjoy.

Lyn & Katherine

Lyn Nicholson is an iappANZ board director and a General Counsel in the corporate and commercial group of Holding Redlich. Lyn’s specialist areas include data & privacy, Government and corporate & commercial law.
https://www.holdingredlich.com/people/lyn-nicholson

Katherine Gibson is the Director of Gibsons Law Limited and is co-Chair of the iappANZ Journal Committee. Katherine has significant experience in providing legal advice on a broad spectrum of business issues across a range of industries for large and small organisations. She also has expertise in advising businesses on privacy issues.
This month, Privacy Unbound talked to the newly appointed Australian Information Commissioner and Privacy Commissioner, Angelene Falk. Angelene was previously acting Commissioner and prior to that Deputy Commissioner at the Office of the Australian Information Commissioner (OAIC).

1. When did you join the OAIC?
I joined the Office more than ten years ago when it was the Privacy Commissioner’s office, the first iPhone had just been announced, Twitter had just celebrated its first birthday and Facebook had only been open to the general public for a few months.

Before that I worked in other statutory authorities in equal opportunity and anti-discrimination. It was at the Anti-Discrimination Board of NSW that I had the opportunity to build the protection of rights into economic frameworks, leading interventions in ten test cases that embedded principles aimed at ensuring non-discriminatory employment terms in NSW.

Protecting rights and interests and achieving positive economic outcomes has been a central feature of my approach. The digital global economy depends upon the trust that comes from a strong foundation in privacy and data protection.

Early in my time with the Office, there was significant community concern about the Google Street View cars and one of the first written undertakings that I worked on was with Google, aimed at building privacy into product design. This followed our investigation into Google’s collection of unsecured WiFi payload data in Australia. We were also focused on pixilation of faces and number plates and ensuring that the safety of people using refuges was protected while filming was happening around the country.

A decade later, another digital platform, Facebook, is at the centre of one of the largest data protection and privacy incidents the world has experienced. It’s a matter I’m investigating and conferring about with international authorities, including the UK Information Commissioner’s Office.

So 30 years on from the introduction of the Privacy Act, and a decade since I joined the Office, the technology landscape has certainly changed but many of the central privacy issues remain constant.

2. What does the changing landscape mean for privacy professionals?
When I started in this position in an acting capacity in late March this year, there was a significant shift occurring in the privacy landscape. The Facebook issue had arisen and the Notifiable Data Breaches Scheme had just commenced. The government also announced that it would introduce a Consumer Data Right, establish a National Data Commissioner and the Australian Competition and Consumer Commission started seeking views on its Digital Platforms Inquiry. The Royal Commission into the financial sector was underway, and APRA had released its report into the Commonwealth Bank. And that was all before Privacy Awareness Week and the GDPR in May!

All of these events mean that privacy and data protection are high order issues for both government agencies and business. It has also been elevated to the fore as a community issue.

The heightened awareness of these issues is driving a change in community expectations around transparency and accountability. This presents a challenge and an opportunity for privacy professionals, to ensure personal information is handled in a way that aligns with community expectations and increases trust and consumer confidence.
3. How is it affecting the regulator’s role?

The issues within our remit — information privacy, access to information and information policy — have never been more relevant.

In this changing landscape we are also seeing more scrutiny of regulators, not just in the privacy area but in general. The community expects greater transparency and accountability – and they are looking to all regulators to be efficient and constructive and to use the full scope of our powers where appropriate. The OAIC is focused on meeting these expectations and our approach will be proportionate, evidence and risk-based.

We are also working closely with other domestic and international regulators, peak bodies and government agencies that are central to the issues we are dealing with. An integrated approach is essential to get the best outcomes in the public interest.

4. Looking forward, where do you see the privacy profession heading over the next 30 years?

The biggest change will be in relation to technologies that we can only imagine. Building in privacy by design will increasingly require a multi-disciplined approach. This is particularly apt in relation to securing personal information. The Notifiable Data Breaches scheme is a key transparency and accountability measure, and our quarterly statistical reports are providing important information on causes and how to mitigate them. This creates an opportunity to elevate the security posture across the economy.

Privacy professionals will increasingly need to engage on security risks, prevention and response strategies across technologies. Global practitioners also need to develop their approach to meet the requirements not only of the Australian NDB scheme, but also the GDPR.

I also see increasing international cooperation between data protection regulators continuing – as we know, data has no borders and the privacy landscape is digital. We saw that in our joint investigation with Canada into the Ashley Madison data breach, which set a precedent for global cooperation.

It will be important for practitioners to be experts in regulatory approaches around the world, and to be able to traverse both data protection and consumer protection regimes.

5. As you said, the new privacy landscape is digital - can the current Privacy Act keep up?

While the technology has changed significantly over the years, the issues remain, essentially the same. The Privacy Act requires that personal information collected by an entity must be reasonably necessary for its functions and activities; for collecting sensitive information generally there is an additional requirement for consent. Collection must also be by lawful and fair means. Secondary uses need to be limited to those that are reasonably expected, or else consent which is fully informed, freely given, current and specific needs to be given. So these are some of the foundational principles that must be considered, and they are technology-neutral.

The Privacy Act is also about ensuring transparency in how entities handle personal information, and ensuring they are accountable to their customers, to the community, and to the regulator.

I want to see business bring some innovation to these challenges, from how they communicate with customers to embracing good privacy practice as a market differentiator. I am also giving some thought to the role of certifications, seals and marks as an accountability mechanism into the future.

6. What are some of your key priorities for your term as Privacy Commissioner?

As Commissioner I’m very much focused on ensuring the OAIC is an effective regulator, connected and informed by our international and domestic landscape; that we engage constructively with other regulators, organisations, agencies and the community; and that we take proportionate regulatory action to meet the objectives of the Privacy Act.

Over the past year we’ve provided more advice to government, business and the community than ever before. Part of that is our work to implement and administer the NDB scheme, and we will continue our focus on elevating awareness and understanding of the scheme and encouraging a proactive approach to preventing data breaches.

I’m working with the ACCC to develop the framework for the new Consumer Data Right and preparing to implement additional regulatory functions under that scheme. I’m also engaging with the interim National Data Commissioner on the new data sharing and release framework. These are significant new initiatives that will require close attention over the next three years.

Since the introduction of the Privacy Code for government agencies on 1 July 2018, we have been helping agencies to implement the Code and develop capability and governance measures.

We will continue to build on our early resolution and conciliation model to resolve complaints, and to undertake complaint and Commissioner Initiated investigations. Privacy assessments (audits) are an ongoing priority, as part of our proactive approach to identifying and mitigating privacy risks.

What runs across these issues is our strong commitment to deliver on our core purpose: to promote and uphold the protection of privacy, together with information access rights. Enhancing awareness and understanding of privacy issues is at the core of that purpose, along with our regulatory and enforcement role.
I’ll be leading the OAIC to meet those community expectations, and to drive better practice and a mature approach to privacy by design across government and business.

7. And, finally, when you do get some time off what do you most enjoy?
Spending time with my family, gardening, singing and watching Grand Designs!
The same year the Privacy Act was enacted, American technology company Intel introduced its first Pentium microprocessor as the microchip-of-choice for the manufacturing of personal computers. The original Pentium contained 3.1 million transistors. Two years later it was surpassed by the Pentium Pro with its 5.5 million transistors. (The latest iPhone has 4.3 billion transistors.)

What does this mean? Let’s look at the company Intel. Intel makes microprocessors for computer systems companies like Apple, Lenovo, HP and Dell. These microprocessors have been driving an information technology revolution – with computers increasing in speed and portability.

In 1965, computer scientist Gordon Moore made the observation that the number of computing power appeared to double every two years in what has become known as Moore’s Law. Let’s relate that to privacy. In the 25 years since the Privacy Act was enacted, computing power has grown exponentially by roughly the power of 12.

When the Privacy Act became law, the World Wide Web and the internet were in their infancy. We didn’t have portable pocket computers which collected extraordinary amounts of personal information, including our location, conversations and shopping habits. We didn’t have email and there was no Facebook. Back then, data breaches were harder to cause and easier to contain. This was the era that I started working in informational privacy law.

Since then, our Privacy Act has withstood substantial challenges by providing a workable framework for addressing existing and emerging privacy issues. It is a tribute to the lawmakers of the time that this technology-neutral legislation, with a principle-based approach, has proved so durable.

However, the scale of digital information being created, collected, transferred, shared and disclosed is now off any chart conceived in 1993. Over four billion people use the internet today. Over three billion people use social media – something that wasn’t a thing until 2004 with Bebo, MySpace and, subsequently, Facebook (anyone remember ICQ?). By one estimate, we produce 2.5 quintillion bytes of data every day - and that’s with the Internet of Things yet to get into a full stride.


This is a dramatically different environment than the one in which I began my professional career. Back then, I could name the other privacy lawyers on one hand. A common privacy concern was the amount of information about citizens being collected and stored by law enforcement agencies. It was a legacy of the anti-establishment 1960s and 1970s when people were increasingly concerned about privacy against a backdrop of the anti-Vietnam war protests, Cold War anxieties, and large mainframe databanks.

Informational privacy is much more than a single issue in New Zealand today. The latest results in our biennial tracking survey show that people are more concerned about privacy issues. While trust in government has improved, increasingly it has become the collection of personal information by business that is cause for concern, among other things. New Zealanders are also deeply concerned about the amount of information children post about themselves on social media and the privacy threats posed by drones and surveillance cameras.
While the privacy concerns of the 1990s have grown and diversified into a multitude of challenges, it’s an encouraging sign there’s been an even further awakening in this digital age of privacy awareness among the public and organisations that hold their information.

A big part of this has been driven by the meteoric emergence of Silicon Valley technology companies. Individually, many of these global companies are now valued at sums greater than the GDP of most nation states. Facebook has a market valuation of over three times New Zealand’s GDP. It handles the personal information of nearly half of the New Zealand population. Also in the digital jungle are Google, Yahoo, Amazon, Twitter, Snapchat, Trivago, Uber and others.

This year, in response to a complaint my Office was investigating, Facebook refused to engage with my office and comply with our Privacy Act. We notified the New Zealand public that Facebook was a non-compliant agency. Under the current Act, it was all I could do. The big question today for privacy regulators and the public to grapple with is how to change this power imbalance, to give individuals greater control over their personal information.

In the international data protection and privacy meetings that New Zealand participates in, what’s emerging is a consensus for cooperation. Privacy regulators are showing a willingness to share information and work together. Data flows across borders, and in the Ashley Madison breach, we saw a cooperative enforcement effort between American, Canadian and Australian regulators to investigate.

We will continue to need adaptable international and domestic frameworks for dealing with privacy issues. We’ve seen that technology changes very quickly and privacy regulators need the most updated enforcement tools to keep pace. There’s been an upscaling of privacy protection frameworks in many of the OECD countries that New Zealand compares itself against. As we look to modernise our Privacy Act, changes have already been made in Australia, Singapore, United Kingdom, Canada, and the European Union.

In Europe, the General Data Protection Regulation which took effect in May gives consumers more rights and EU regulators more powers. Data portability, rights of erasure, mandatory data breach notification and significant fines for non-compliant organisations are some of the tools we’re arguing should be included in the Privacy Bill currently before the New Zealand Parliament.

This cursory stocktake reveals the breathtaking scope and pace of change of the past 25 years. The next 25 years will also present us with new privacy threats, opportunities and challenges. Some of these will be predictable and others unforeseen. A modern and up-to-date Privacy Act is necessary to give New Zealanders greater control over their information and to afford more robust privacy protections. Imagine how we’d feel if those first Pentium microprocessors had remained unchanged.
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

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:

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
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.
Is privacy now passe; overtaken by data and IoT?

Hell no! I have never swallowed that defeatist ‘privacy is dead’ line. If anything, the past year has seen a resurgence in privacy concerns and activity. The Facebook / Cambridge Analytica revelations have opened the eyes of so many people, and they are starting to push back against surveillance capitalism. Meanwhile the GDPR has started a global conversation about how best to balance privacy with other interests.

Privacy is front-page news all the time now, and getting stronger all the time. I knew we had gone mainstream when earlier this year I was asked to do an interview about privacy risks with The Australian Women’s Weekly.

I like to contrast these two quotes:

- Privacy is “no longer a social norm”.
- “The number one thing that people care about is privacy and the handling of their data.”

That was Mark Zuckerberg in 2010, and Mark Zuckerberg in 2018.

One of these days I am going to cross-stitch that last quote onto a pillow, so that every night as I lay down my weary head, I can enjoy just a little bit of schadenfreude.

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

I am obviously proud of having built Salinger Privacy into a trusted provider of privacy consulting, training and guidance materials. But for a single achievement I would nominate a two-year-long piece of volunteer work, which was running the successful ‘NoID’ campaign against the proposed Access Card in 2005-07. I co-ordinated the campaign on behalf of the Australian Privacy Foundation, along with a number of other NGOs. As I look back now, I realise what a very female experience it was: Robin Banks headed up the Public Interest Advocacy Centre which was our primary campaign partner, and the three most influential politicians we worked with to oppose the proposal were Senator Natasha Stott Despoja (Democrats), Senator Kerry Nettle (Greens), and the then Shadow Minister for Human Services, Tanya Plibersek (Labor).

Each worked tirelessly to hold the government of the day to account for Joe Hockey’s national ID card thought bubble. This was before social media, so it was lots of phone calls and meetings and driving to and from Canberra and making speeches and writing op-eds. Mind you, we never had the chance to celebrate our campaign victory, as within a few days of the Howard Government finally dropping the Access Card proposal I went into labour (the latter stages of the campaign had involved me waddling around Canberra haranguing politicians in an alarmingly pregnant state), while the others were shortly thrown into a federal election. There was no victory party or magnum of champagne, let alone time to either reflect or pat each other on the back.

While I have taken a back seat on formal privacy advocacy campaigns since becoming a parent, the work of privacy advocates goes on. It is all volunteer work, and mostly thankless, but incredibly rewarding. I engage in armchair advocacy these days, firing off grumpy tweets and watching with amazement as my monthly blog occasionally goes viral.

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

I was about to say another “hell no” but then I remembered I have smart electricity metering. Oh, and a lovely connected sound system. Um, does Netflix count?

But I studiously avoid any digital personal assistants (no, not even Siri or Cortana), let alone connected lightbulbs or doors, for the many reasons outlined in my blog about IoT. I like my devices dumb: no need for the toothbrush, toaster or toilet to talk.
How have businesses changed in the way they respond to the law in the last 30 years.

There has been a really positive shift in thinking. In the early days of Privacy Impact Assessments, I had a few clients which were reluctantly dragged to the process under the eye of the Privacy Commissioner. Every opportunity was taken to try to wriggle out of interpretations of the legislation that didn’t suit their plans. At the time I would joke to colleagues that PIA apparently stood for ‘Pay to Ignore my Advice’.

Now it is completely different. The clients who come to us already get it: privacy is about respect and restraint, common sense and good manners, and if they get it wrong their reputation is doomed. Legislative compliance is just a given, a baseline; the discussions are much more around ‘what do our customers expect from us?’

What is your hope for the next round of reform?

If I had a magical privacy wand (or the Attorney General’s job), I would:

• Tighten the Privacy Act to match GDPR standards including higher penalties, a right to algorithmic transparency, and a right to human review of automated decisions; abolish the exemptions for political parties, small business and the media; and tighten the ‘directly related secondary purpose’ test that has been interpreted as allowing a Minister to publicly release personal information about a welfare recipient just because she wrote a blog critical of her experiences.

• Reform the complaints and access to justice process under the Privacy Act, so that complainants can go directly from OAIC to the AAT for cheap, effective review and meaningful remedies, as happens under NSW and Victorian state privacy laws. (There have been 400 cases decided under NSW privacy law, and less than ten under the Federal Act. Privacy principles mean nothing if they can’t be easily enforced by individuals.)

• Fund the OAIC properly so they can set up a technical expertise unit, to offer advice and robustly investigate cases like Robodebt, Facebook & Cambridge Analytica, and enforce the new Privacy Code.

• Repeal warrantless access to telco/ISP metadata; and convince the Health Minister to turn MyHealthRecord back to opt-in.

• Re-think the Data Sharing & Release Bill, and tell the ABS to stop data-matching using Census data without new, specific legislation.

• Introduce a statutory tort of privacy as recommended by the Australian Law Reform Commission and bi-partisan parliamentary committees.

• Introduce a Bill of Rights such that individuals could challenge legislative and administrative overreach.

• Give privacy advocates wine and chocolate and the occasional hug.
Marie Shroff

Marie Shroff is currently:
• a member of the Consumer NZ Board,
• Chair of the Consumer Foundation,
• member of the Media Council, and
• Chair of the Privacy Foundation

Marie was Privacy Commissioner from late 2003 to early 2014 working closely with the Law Commission on its recommendations to increase privacy protection for New Zealanders.

From 1987 – 2003 Marie held the position of Secretary of the Cabinet and Clerk of the Executive Council, developing reforms of constitutional policy and practices especially about proportional representation and coalition government.

Earlier in her career Marie worked in foreign affairs, teaching, journalism and the public service.

From 1980 – 82 she was seconded to the UK Cabinet Office.

She was awarded an Australia/New Zealand Foundation Fellowship in 1995 and a Chevening Fellowship in 2002. Marie represented New Zealand on the Board of Directors of the Commonwealth Association for Public Administration and Management (CAPAM) from 2005-2009. She was awarded a CVO in 1995 and a CNZM in January 2004.

Marie was the inaugural recipient of the iappANZ Privacy Hall of Fame in 2015.

Is privacy now passe; overtaken by data and IoT?

Far from being out-dated, the Privacy Act is rising to the challenges with intelligent regulation and enforcement. The changes to the Act currently before Parliament will help with that by giving the Commissioner greater powers. Compulsory breach notification will be a wake up call to New Zealand organisations – get it right before you get it wrong. Good data stewardship will have to be part and parcel of how organisations operate into the future.

25 years ago, how hard was it to get senior executives to take privacy seriously?

In the nineties technology was a new and marvellous tool for organisations to deliver services cost effectively; and business and government were just waking up to how they could exploit big databases to their advantage. Is it any wonder, in that environment, that privacy was viewed largely as an obstruction to be got around, or as political correctness gone mad?

You could say that the last 25 years of privacy have really been about organisations painfully and slowly getting their heads around the fact that there is no such thing as a free digital lunch. Controls, checks and balances have to be present, to moderate big business and government power gained through technology and big data. With power comes responsibility.

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

The achievement I am proudest of is getting some shift in attitude to privacy – particularly from the media, and in turn the public.

How have the public and media perceptions of privacy changed?

In 2003 privacy was getting a really bad press. Angered by a threat they (wrongly) perceived from the new Act to freedom of speech, some in the media seemed determined to discredit it, by running endless “privacy horror stories”; for example about parents allegedly denied access to their child’s school report or health records. Without much to lose in the hostile media climate of the early 2000s, we at OPC went all out to show them that these stories were misguided, on at least two counts. The horror stories were almost always based on misunderstandings and mistakes about how the Act really worked, and the real horror stories were actually about injustices to individuals arising from withheld, wrong or misused information; problems which the Privacy Act could be used to fix.
More positively, we managed to get better coverage of one of the biggest stories of the early 21st century – the information technology revolution, and its huge impacts on privacy, people and society. These days media focus has rightly shifted to stories about the power of big data and the benefits and threats it poses to human lives and society. Complaints about political correctness are almost forgotten.

**What is your hope for the next round of reform and the future?**

The Privacy Act was farsighted in tackling ways to control “big data”, long before the phrase had even been thought of. The tough task for the future is carefully to fashion controls which will balance the tech giants’ power, ensure they treat people openly and fairly, and allow individuals to retain some control over their information. The Privacy Commissioner’s Credit Reporting Privacy Code is a great, evolving example of bold but well consulted and designed regulation. It tackles both business needs and how to protect people – demanding accuracy, preventing misuse and allowing us access to our credit records.

**Where do you see the privacy profession heading in the next 25 years?**

The GDPR also puts pressure on New Zealand to be up with the play on information protection in a globalised world. The World Economic Forum has said that global internet bandwidth quadrupled between 2010 and 2014, and cross border internet traffic increased 18-fold from 2005 to 2012. In this climate, privacy professionals can have a bright future, because of the growing demand to protect organisations’ data and to safeguard their customers’ information.
Can you share any privacy debacles you were involved in any way with in your career that has burned itself in your memory?

A memory from over 40 years ago stands out. In September 1977, I became heavily involved in the campaign against the just introduced NZ Security Intelligence Service Amendment Bill. It proposed to give the SIS very broad powers to ‘intercept communications’ between individuals. The bill generated an intense public controversy. Thousands marched the streets in various towns and cities. I still have vivid memories of the 750+ concerned Kiwis I addressed at the Wellington Town Hall.

Despite all the protests, the bill was enacted largely unaltered. It taught me a valuable lesson. In reality there is no such thing as achieving a ‘balance’ between protecting individual privacy and the public interest in safety and security. The latter always wins.

I have been reminded of that whenever there have been bills introduced into parliament to increase the powers of the SIS, or its even-more shadowy ‘cousin’, the Government Communications Security Bureau (GCSB). This has occurred on a number of occasions. Each time, individual privacy has been further diminished in the interests of national security. However, some forms of complaint redress have been enhanced, for example, the role and functions of the Inspector-General of Intelligence and Security.

What is your hope for the current round of reform?

The Privacy Act 1993 made our country a world leader in aspects of data privacy. Since then, our privacy laws have fallen behind aspects of similar laws in comparable jurisdictions. My hope is that New Zealand will regain that status in the near future. Unfortunately, the Privacy Bill currently before parliament does not come close to that. I am in full agreement with the NZ Privacy Foundation’s submission that the bill requires substantial amendment. This includes –

- A right to portability of personal information
- Effective protections against re-identification
- Harmonisation with the requirements of the EU’s General Data Protection Regulation (GDPR), to ensure that NZ safeguards its present ‘adequacy’ status.
- Recognition of an individual’s right to anonymity and pseudonymity in certain circumstances.

Is privacy passe; overtaken by data and IoT?

No. Meaningful protection of individual privacy is more important than ever. It’s an internationally-recognised fundamental human right. Despite that, it is forever under threat. Privacy forms a core component of the concept of individual freedom. To protect that freedom in a meaningful way, something more than ‘mute protest in our bones’ (Orwell, 1984) may be required. Ever-more invasive IT threatens to strip individuals of what little privacy they have left. Proponents of a new form of IT may attempt to sell to decision-makers and an unwitting public, on the basis that the particular development is for the ‘public good’.

All ‘privacy professionals’ have an obligation to be active in exposing and resisting developments and practices that have the potential to erode significantly the privacy of individuals.
I live in hope that the select committee will recommend accordingly.

Tell us about some of the “doom and gloom” predictions made at the time the legislation commenced that were widely off the mark.

Some critics were of the view that ‘it was not worth the paper it was written on’. Similar predictions were made about the NZ Bill of Rights Act 1990. Fortunately, both observations proved wildly inaccurate.

Former PM, David Lange, described the Privacy of Information Bill (ie, the bill that eventually became the Privacy Act 1993), as a “Clayton’s Bill”. By this he meant that the bill purported to protect individual privacy, but in reality was more concerned with legalising certain state sector activities, in particular information matching, that was more likely to erode the privacy of effected individuals. Given that this was a major reason why the national government of the day enacted the 1993 Act, there was some element of truth in Lange’s assertion. However, in practice other aspects of the Act (eg, the seamless application of the IPPs to state/private sector agencies and the handling of personal information in any form being covered), have proved much more significant than was originally contemplated.

The direct marketing industry argued that the law would have a draconian effect on their activities, and that the thousands of Kiwis who depended on that work would be badly affected. The banking, credit and finance industry, also had major concerns. Other than the predictable teething problems, few of these concerns proved of significance. Undoubtedly, the phased implementation of aspects of a number of the IPPs helped ameliorate industry worries.

Has the legislation in the main achieved what you thought it would when it became law back in 1993?

Overall, the Act in practice has exceeded my expectations. I give much of the credit to the three Privacy Commissioners to date and their expert staff. They have produced some excellent practical resources over the years.

During its early years the Act was subject to a concerted campaign by powerful elements of the news media to discredit it. Given that the news media was very largely exempted from the Act’s application, I found this disappointing, to say the least. Making fun of how the Act operated in particular circumstances became a popular form of media entertainment. Many of these stories proved, after investigation, to be highly inaccurate (eg, reporting that the Privacy Act was the cause of ‘the problem’ when in fact the relevant law was the Official Information Act).

Talk about ‘fake news’!

Unfortunately by the time the Privacy Commissioner’s Office put the record right, the damage had usually been done. It was all ‘the fault’ of the Privacy Act. On occasions in the 90s, I wondered whether the Act would survive.

Well, it did. That’s a cause for celebration.
I do not have a connected home. I can’t see how any possible advantages could outweigh the disadvantages. I’m of an age when I can do most things and make most choices for myself. Connected homes are for those who are unmindful of possible data breaches and privacy threats. I just don’t think it is worth the trouble if things go wrong.

Has the legislation in the main achieved what you thought it would when it became law back in 1993?

No, but perhaps that is a good thing. There are many exceptions that provide for flexibility. What is surprising is that many holders of personal information, particularly the box-tickers, tend to use the legislation to deny people information (their own, or the information of others) for little or no reason except to be obstructive. Conversely, the provisions on the collection and sharing of personal information by government agencies has little if anything to do with privacy and more with control.

Where do you see the privacy profession heading in the next 25 years?

The profession will probably become less relevant with time, to be replaced for all intents and purposes by AI and privacy by design. In any event, there will probably be very little privacy left to protect, so there will be no need for privacy professionals, except perhaps for technical experts that can assist individuals or enterprises in case of a damaging data breach or a specific privacy threat.

Paul is a professor of law at the University of Otago, in Dunedin, New Zealand. He has been involved as a lawyer and academic in the freedom of information and privacy law areas since 1990. He is the author of the LexisNexis looseleaf text *Privacy Law and Practice*, which has been updated quarterly since 1994. He has also written a range of articles on privacy law and has taught a course on Information and Data Protection law since the early-2000s. In addition to privacy law, he specialises in labour and employment law.

Is privacy now passe; overtaken by data and IoT?

If it is passé, I’d be very worried. It would not be of our own doing, but something that has been forced on us through lack of real choice and for the convenience of government and business.

25 years ago, how hard was it to get senior executives to take privacy seriously?

It wasn’t difficult if you could sell the idea that it made good business sense, which it did in some industries, but not in others.

Do you have a “connected” home? Why/Why not? What would change your mind?
The problem with conferences

Given the number of conferences and related events covering Smart Cities and Critical Infrastructure, you would think that security and privacy challenges facing the Internet of Things (IoT), Industrial Internet of Things (IIoT) and Operational Technology (OT) streams are well covered in these fora. Unfortunately, this is not the case. Often, the cyber presentations are tacked onto the end of the conference or sidelined to a small room off centre stage. Privacy is lucky to get a look in.

Perhaps privacy and security impinge on the IoT / IIoT "kumbaya possibilities" and raise questions and concerns that are best left for others to address? Or perhaps, it’s an area of little interest and not considered necessary at such prestigious events? After all, who wants to hear about the ethical or privacy implications of these new technologies when you can demonstrate a flashing, beeping, must-have new IoT gadget? Moreover, for the price of your email address and mobile phone number, you could possibly take one home! Stick around folks, the end-of-conference lucky door prize will be drawn soon!

Either way, by the time we reach three o’clock, most of the food has been eaten, medals awarded and the delegates have had their fill of presenters and special offers. It might leave those in the room with an uncomfortable niggle if we utter words like citizen rights, privacy risk or cyber right now...

Cynical? No doubt. Incorrect? I think not. Of course, a great deal of goodness comes from these tech centered conferences: fresh ideas, novel approaches, exciting technologies. However not enough time or consideration is offered to the other side of the coin: that is, the opportunities presented by thinking about privacy and security at the outset.

With increased attention worldwide to privacy laws, extraordinary data breach events and the more seamy side of data driven technologies, the need to ramp up the dialogue at these events is long overdue. Event delegates need to understand the essential interplay between personal data, privacy and security, and then apply this knowledge to their digital strategies, data management controls and, perhaps most importantly, to their interactions with communities, employees and the private citizen.

I would suggest that certain obligations - privacy, security, transparency in decisions that affect the community - are as important as deciding whether to go with the self-driving bus, intelligent bin or self-steering tourist submarine as a city’s first foray into smart technology.

Urban developers, engineers, councilors, critical infrastructure specialists need to be advised on the risks and responsibilities of any solution. Not just the benefits, not just the shiny parts. They have a responsibility to holistically consider the impact of new technologies and, in cases where the tech involves personal data, failing to do so may result in running foul of the law.

Smart Cities, intelligent grids, building services, and an array of other industry sectors are reliant on these new smart technologies to improve cost efficiencies, service delivery, sustainability goals and user convenience. However, at the core of these success stories is the establishment of trust. Without trust, these initiatives will not reach their full potential.

In return for this trust, citizens across the board, across the social and political divide, require their privacy rights
to be upheld and their personal data to be protected in accordance with the law. This is not a case for filling delegate heads with “cyber tech stuff” or “waffling on about privacy” when the people in the room would rather see cool new technologies in action. Rather, I’m suggesting that there is a real benefit in bringing it all together for the best, most considered and, ultimately, most satisfying results.

Some would argue that we have cyber conferences for this sort of thing. Have you attended a cyber-conference lately? Everyone at the event knows what is going on. It serves a different purpose. It updates the faithful, the interested. It serves an incredible purpose, but it meets a different need. It’s like-minded professionals coming together to improve and educate those already converted to the security mindset. You would expect to see a security specialist, privacy officer, cyber advisor, possibly even a CIO present at a cyber conference. How about a hotel precinct investor or smart cities developer? An urban planner, engineer or city councilor? I would say probably not. However, considering current IoT digital eco-systems and their all-pervasive nature, those Smart Cities and Critical Infrastructure conference devotees are the very delegates that would benefit from better understanding privacy, security, their ethical responsibilities and business risk profiles.

Privacy: the elephant (not often) in the room

Those organising Smart Cities and Critical Infrastructure conferences need to think beyond the vendors sponsoring their show and consider a conference of a different kind – one that displays wonderful technological advancements and opportunities, sure, but one that also acknowledges that we can no longer roll out the tech without considering the bigger picture.

Perhaps the most significant challenge in the emerging and evolving IoT eco-system is the overriding and intrinsic imperative that privacy be given meaningful air time. Never has there been a greater need to ensure that individual privacy expectations (and those of the broader community) are managed carefully and in line with the law.

Traditionally, a solution’s “security requirements” were enforced by a series of organisational policies, risk standards, architectural requirements, etc. Rarely was there a privacy expert involved in the solution’s design and deployment. Ethical considerations were handled by someone but not by the technical design team. The privacy focus was primarily on risk mitigation or monetary and brand risk.

We now have a digital economy that cannot afford such indifference to the person whose information is at the heart of the technologies being deployed. The individual is at the core of the digital economy. The individual has never been closer to technology and never more affected by it.

It has become clear that privacy is the end game. The driving force. The measure for individual, community, and state asset protection. Security specialists may utilise an array of tools and processes, however if the privacy controls are not met, what do you really have? What is the point?

Recent legislation within Australia and globally has made privacy a visible priority. Technology and controls for IoT, IIoT and OT must support the requirements of privacy legislation as part of the solution design and its delivery process. Privacy can no longer be tacked on as an afterthought. This strategic shift provides an imperative to bring together the resources needed to meet future cyber security and privacy challenges facing our smart cities and critical infrastructure projects.

Collaboration and inclusion

At the risk of not being invited to speak at a conference within the foreseeable future, I believe the way forward is a dual approach: 1. additional and defined representation of cyber security and privacy at the (traditionally untouched Smart Cities and Critical Infrastructure) conference level, and 2. more client, vendor, security and privacy industry collaboration at the detail level.

It’s time to drive privacy and security speakers up the conference totem pole – these topics are highly relevant across sectors dealing with IoT, IIOT and OT. Recognising that face time at conferences cannot be expected to result in specific privacy and security related outcomes when choosing and deploying technologies, it’s also time (more broadly) to establish engagement models between business/community leaders, urban developers, engineers, service vendors, cyber advisors and privacy and data protection professionals to create a more collaborative and responsible smart technology sector.
Why is everyone finding GDPR a pain? Put differently, why is everyone doing regulatory compliance wrong?

We’re going to be provocative from the start and say that GDPR is neither a legal issue nor a regulatory one—with all the implications from this statement for running a GDPR compliance project.

We’re co-running a GDPR project on behalf of a major corporate client and have visited several privacy events in NZ to understand patterns that befall large organisations in addressing the GDPR compliance. We’ve also undertaken a survey of Data Protection Officers (or similar C-minus-1 positions) of some of the largest organisations in the world on their compliance journey. The one major theme that came out of this research is: organisations that find GDPR compliance painful do not have their data governance under control—meaning that GDPR pain is not privacy-specific but is rather a reflection of not having one’s data house in order. Conversely, organisations that had their data governance under control had a much smoother road to compliance. Below is a GDPR Optimist’s Guide to Compliance—what follows is a set of “correct” (in our opinion) GDPR positions and opportunities.

Remember—we’re trying to help you alleviate the pain and set your organisation for success beyond compliance.

Customer Centricity

First and foremost, GDPR is a customer-centric issue. At the heart of it is a fundamental right of people to be in control of their personal information. This is part of Charter of Fundamental Rights of the European Union—which itself is part of the Constitution of the EU.

Notice the difference to the Silicon Valley’s rather explicit (until recent California Privacy Law, anyway) insistence on a customer’s signing off all their rights over their data—and said data becoming the property of tech companies (Microsoft, Google, Facebook, and the like).

Now compare these two positions:

1. personal information is property of the individuals, and firms are just custodians of their customers’ and staff personal data, and must therefore treat said data with utmost level of care;

   vs

2. firms are the owners of their customers’ personal information on their servers and can monetise this data in every way imaginable (though with anonymisation), without asking customers for permission.

Now let’s ask ourselves this: which type of organisation would win in the long run? The organisation that takes customer trust to the highest level—or the organisation that treats the customers’ data as a source of income maximisation?

In 2018? I’m betting on the former. People like Rob Everett, Jacqueline Peace and many others have taken similar positions on customer centricity.

From this point of view, GDPR is not something that hinders us from doing business—in fact, if we are serious about customer trust as a marketable brand asset and if we want to live the talk of customer centricity, we want to treat our customers’ trust with respect at the highest level.

P.S. There’s one organisation in the region that visibly took a positive, customer-centric approach to GDPR. We all know this organisation is Air NZ. I’m hoping we all can use their example to adopt the right position on how to treat GDPR as an opportunity to uplift our privacy game.

Please, allow me artistic freedom to use laymen meanings behind the concepts of ownership and such—the purpose is a position for the Executive Team, and not a legal article—so the choice of wording is by design.

2 CEO of FMA, in his speech on “Is trust the new currency?” from 6 September 2018

3 Chief Privacy Office of Air NZ, in her presentation titled “The regulation that shows we are Genuinely Devoted to Privacy Responsibility” at a GDPR iappANZ Event from 11 April 2018
Capability Building

Suppose hypothetically we run an organisation that does want to leverage its data to the fullest—data monetisation is a very popular concept, especially by the firms that don’t perceive themselves as currently doing this. This could be selling (anonymised) data to the highest bidder, leveraging big and small data for hyper-targeting on Facebook to drive conversions, personalised marketing—or even leveraging analytics to improve internal operations.

Leaving aside for now the issue of lawful processing reason (from consent through legitimate interest through mandatory compliance and contract fulfilment), how would one do it?

This argument is very straightforward and is highlighted by the Chief Data Officers of the surveyed organisations—you cannot leverage the value from your data, unless you have a robust data governance and are in fact in control of it. And that’s all that GDPR mandates: that you be in control of your own data. Because if you as an organisation are not in control of your data, you cannot satisfy the customer rights. The flip side is easy: if you are in control of your data, if you can manage the full life-cycle of every data element, can trace it, manage access to it, and can destroy it—then you’re already compliant with GDPR.

Priorities!

So, who says “no” to enterprise-wide capability building and treating customers’ trust with respect? We don’t think anyone does.

So, then, what’s the hold-up?

Yes, but we have a lot of conflicting priorities...

Like what?

Revenue growth, cost-out, digital transformation, data monetisation, other regulation, personalisation, etc.

That’s all correct—and all the above are made more difficult if you don’t have your data under control, and also made that much easier if you do.

How difficult? Consider some of the largest EU banks having had to spend 5 years and more than half-a-billion EUR on regulatory compliance with BCBS 239 (ignore for a moment what this is—all one needs to know is that the first 2 bullet points on its Wikipedia page are “overarching governance and infrastructure and risk data architecture”)—and also consider others from the same group of largest EU banks who already had done something similar for other reasons earlier, and having found BCBS 239 not an issue. The latter group of banks also found GDPR not an issue, nor any other regulation that is coming their way—because they already had built awesome data governance and infrastructure.

Because as one of my interviewees said, “you can do it proactive when you can plan strategically, or you can do it reactive—but at the end of the day, you will do it.” They were referring to data governance and infrastructure of the kind mandated by GDPR, and what they meant was this: everything costs less if you can plan for it, and by the way the capability in question is a key one to have for a modern organisation. So, you have a choice—either invest in it strategically, or scramble in a very ad-hoc, tactical minimum-viable product fashion and then duplicate the effort when another crisis hits, or another regulation that mandates pretty much the same comes along.

Because every year, the same priorities remain: revenue in, cost out. They can be helped by strategic investment in data... or they can be hindered by a lack of strategic investment in data, making every single year look the same, and every single initiative costing more than necessary and delivering less than expected, in the long-run.

Approach and skills needed

There is only about one way to do things right:

1. Start at the highest managerial level, and work top-down;
2. Break silos in data governance and infrastructure with single enterprise-wide point of accountability and powers;
3. Find the right people;
4. Execute strategically with incremental deliverables (avoid bigger-than-Ben-Hur projects) that fit into strategic vision with cumulative benefits.

The people part is key. The other steps are a bit easier to explain—the people become a bottle-neck once the top-down buy-in is acquired and direction is set.

And this is exactly where if GDPR is treated as a legal/compliance project, it will fail—or if not fail, then at least will create an inordinate amount of headache. Because in a business-first data governance project, you need 10-20% legal, compliance, and operations understanding, 45-50% business understanding, and 35-40% data infrastructure and governance understanding. Finding those skills in a person is tough, as it takes decades to develop and this combination isn’t typically something that is readily available.

Setting up a project team like this is easier—but you still need to have T-shaped skills that would understand each other’s language. A business & data expert, a compliance & data expert, etc.
The description of a Data Protection Officer mandated by GDPR (articles 37, 38, 39) highlights the needed expertise in data protection practices as well as law.

### Transformation to a 21st century organisation

There are two things that characterise success stories of a modern organisation: focus on customer (service) supported by best-in-market data capability. You can’t focus on “customer” without knowing who that “customer” is, what they do, like, and how they behave... and this is nothing other than having your data in order. It’s really that black & white.

Customer-centric and capability-building focus make the type of transformation discussed here both exciting and important to the bottom line. Nothing in this is inherently GDPR-related—yet sorting those things out will benefit GDPR, among other things.

So, to sum up—GDPR has nothing to do with the regulation, law, or compliance.

It has *everything* to do with becoming a modern organisation—having customer at the heart of what you do, supported by state-of-the-art enterprise-wide data capability.

The regulator wants the same. Because as one key stakeholder likes to say, “regulators regulate after having asked nicely 3 times”.

So, don’t *react* to GDPR—but do use this as an opportunity to uplift your organisation’s game in all things data. The new NZ Privacy Bill is around the corner—and so are many other regulatory undertakings on the same (or similar) topic. Data is at the heart of everything. And proactive, strategic planning beats reactionary, tactical response every time.

### Caveats

Yes, I purposefully painted a very black & white picture. Partly because it is. Partly because of the space constraints. There are, of course, always nuances.

Finally, beware IT “solutions” providers selling you a “GDPR” solution—*to paraphrase somebody from one of the Privacy after Hours events, “GDPR solutions do not exist”*. There are no doubt technological means to assist you with your GDPR compliance, but there is no “out-of-the-box” solution to seamlessly integrate with, and help all (extremely diverse) organisations with their needs, given that most of these needs are process- and culture-related.

That’s where you get the experts to advise.

---

For any questions/comments on the article, please call me on +64 22 0870 394 or email at a.ivanov@ivanov-consulting.co

Andrey holds a PhD in Economics from Universität Mannheim (Germany) and is a member of iappANZ.

Andrey runs Ivanov Consulting Limited, a holistic strategy consultancy comprising economists, chartered accountants, data scientists, risk and marketing professionals.
Data is fast becoming one of the most important intangible assets for organisations. Data use differentiates organisations, enabling better product development, personalised service offerings and is therefore a source of competitive edge.

However, growing commoditisation of data and the advent of serious data breaches across jurisdictions and industries, has called for sweeping regulatory change to codify accountability and transparency.

Regulations such as the Notifiable Data Breaches (NDB) Scheme and General Data Protection Regulation (GDPR) are lifting the standard on security measures, organisation-wide data awareness and restoring trust and ownership of personal data with consumers. These regulations also seek to increase accountability for breaches. Fines are only the beginning of repercussions, with reputational damage having long-term downstream effects for consumer trust and bottom lines.

Boards are increasingly facing data related risks and issues. New regulation, and community expectations, need to be balanced with strategic objectives for digital transformation, reducing operational costs, and retaining competitiveness while delivering on the value proposition. Data lakes and organisation-wide practices need to be understood, and the controls for ethical use and protection of this data need to be monitored and communicated at all levels.

Some of the key data related issues facing Boards today are regulation, governance, consumer trust, security and technology.

**Governance**

Good governance has never been more critical. In an environment of sweeping regulatory change and heightened consumer awareness of data risks, conflicts often arise between data mining mandates, legal requirements and ethical consumer considerations. Asymmetrical dissemination of privacy risk appetite throughout the organisation and disempowered risk governance across delegations of authority usually result in revisiting decisions and potentially higher costs to rectify poor privacy compliance solutions.

Without clear guiding principles regarding how an organisation treats consumer data, there remains risk of grey areas in data uses, and further processing, and generally also reflects a poor data culture.

In relation to consumer data, good governance means:

- Data principles that align with consumer expectations, board risk appetite and organisation values
- Enforcing, monitoring and reporting in relation to data governance and controls
- Mechanisms for monitoring regulatory change
- Clearly defined roles and responsibilities, with empowering delegations of authority
- Managing conflicts with business uses of data, and secondary uses
- Ensuring data principles are instilled throughout the organisation through regular training, enforcement and real consequences

Without good governance, the framework for data management will not be clear and there is likely to be less visibility of data practices, therefore leading to a higher likelihood of breaches.

**Regulation**

Since 22 February this year, notification of eligible data breaches became mandatory in many cases to the OAIC and affected individuals through the Privacy Amendment (Notifiable Data Breaches) Act 2017 (NDB scheme). This is the first time in Australia that all entities who are covered under the Australian Privacy Principles have clear obligations to report on eligible data breaches. A critical part of being able to comply with the NDB scheme is preparation. Entities need to know what information they have, where it is stored, how it is protected, how they’ll know when a data breach has occurred, and then how they’ll respond should a breach occur.

Since 25 May this year, the General Data Protection Regulation (GDPR) came into force with extraterritorial reach that has implications for Australian businesses that offer goods and services to individuals in the EU, and/or monitor EU individuals. This regulation introduced significant requirements for understanding organisation data processing activities (records of processing), providing significant data subject rights such as the right to be...
forgotten, and data breach reporting requirements of 72 hours from the point of awareness. Broadening the brush stroke of this regulation are the fines, which range from €20 million to 2.4% of annual global turnover or whichever is higher. There is significant compliance burden, and risk of reputational and financial loss entailed in meeting these imposing obligations. In raising the bar for transparency and accountability for personal data managed by organisations, these regulations are also a source of many unknowns for non-EU organisations as the enforcement has yet to be tested by privacy regulators.

Upcoming regulation called the Consumer Data Right which will start with Open banking and ultimately be implemented across the entire market, with Energy and Telecommunications industries next cabs off the rank.

Trust

The Australian Community Attitudes to Privacy Survey 2017 found that privacy awareness was growing, however the majority of respondents did not use, or did not know how to use, simple safeguards such as clearing cookies to protect their privacy.

In 2018:

➢ Approximately 150 million customer accounts, including personal emails and hashed passwords, were affected by the myfitnesspal breach of March 2018.
➢ Orbitz, a travel site owned by Expedia, also disclosed a breach that resulted in unauthorised access to 880,000 personal credit card details for customers who booked travel over 2016 and 2017.
➢ Cambridge Analytica used the data of 50 million Facebook customers without consent to build psychological profiles so voters could be targeted with ads and stories.

Such data breaches, and the approaches to resolution for affected individuals, indicate a shift in accountability and transparency.

The NDB scheme and GDPR most notably brought into effect mandated data breach investigation and reporting timeframes. These laws also increased accountability through introducing significant fines, let alone impacts to reputation due to public reporting.

However, regulation alone is not enough. Attitudes of organisations towards their customer’s personal data and consumer expectations about the fair use of their data need to align. Customers expect organisations to fulfil service and product obligations, remain competitive and profitable, while also protecting their privacy interests.

One way organisations can achieve this is through transparency over internal and external data flows, communicated through clear, concise privacy statements. Giving consumers control over how their data is collected, and making the processes for setting such preferences easy and amenable to different customer groups, also need to be considered.

Underpinning this is how serious organisations are about data protection. Organisations must be assured that third party arrangements preserve customer privacy interests. Further, investments in sustainable technology solutions, and automation of manual processes can improve the efficacy of privacy management.

Security

Strategic objectives for technology transformation, use of social media engines and upgrading legacy systems increase exposure to the risk of cyber-attacks. With organisations becoming more interconnected and reliant on complex IT systems, exposure to cyber-attacks has become more sophisticated, frequent, targeted and difficult to detect. As a result, cyber-related crime is one of the highest rated risks facing organisations today.

New regulation seeks to instil requirements for having adequate safeguards that are commensurate with the scale/impact of threats to which an organisation is exposed. Organisations should also have active measures to protect personal information held, while also having measures to ensure data troves are not retained unnecessarily. These requirements are reflected in APP 11, Article 32 of the GDPR and current draft APRA prudential standard CPS234 Information security.

It is incumbent on organisations to take appropriate and proportionate technical and organisational measures to manage security risks. Organisations can achieve this by integrating preventative measures to safeguard, raising awareness of every employee’s role in data protection, and distributing responsibility across all levels of an organisations. To tackle the increasing threat of cyber security, common controls embedded throughout organisations include:

- Pseudonymisation and encryption
- Confidentiality, integrity, availability and resilience of processing systems
- Restoring availability and access to personal data following a cyber-attack
- Monitoring and supervision of technical and organisational measures

Data Strategy and tech innovation

As organisations seek to improve the customer experience and secure the competitive advantage associated with brand trust, it is crucial to leverage customer personal information assets in the most appropriate way. Organisation strategies often lean on the analytics potential of Big Data to drive competitive positioning for operational efficiency and improved product offerings, however this needs to be tempered with the risk of cyber and data breaches, and requirements for data minimisation.
Quality data is at the heart of a strong data strategy which includes automation and AI initiatives to replace and enhance existing business processes. However, large lakes of unstructured data can hinder the ability to access effective insights. Further, Boards are concerned about the mismatch in maturity of organisation-wide data governance practices with the speed of automation deployment. This generally results in organisations taking on more risk than contemplated in project phases. This is where effective Privacy Impact Assessments (PIAs) are critical to ensuring personal data risks are detected and managed.

Further, automation and AI bring new risks, such as potential biases in those writing algorithms, ineffectiveness of existing controls to monitor performance of algorithms, and lack of suitability of existing risk frameworks to extend over analytics practices. Therefore, existing employees will need to invest in training to learn new skills as their roles evolve. Organisations will need to empower their employees to navigate the new risks as their roles and subject matter evolve.

Conclusion

We have explored some key risks facing Boards today. As the pace of automation, investment in new technologies and machine learning solutions accelerates, new regulations and community expectations will need to be navigated to ensure personal data is adequately protected.

However, new regulation and the fear of customer expectations should not be a hindrance to evolving business practices, being courageous in exploring analytics and designing tailored products for consumers that offer price, choice and flexibility competitiveness. While consumer awareness of data privacy is currently at its highest measured levels, organisations need to finely balance these heightened expectations with meeting efficiency and competitiveness objectives. Organisations should not be afraid to use the data they have, as long as they have confidence that it is well protected, backed by lawful processing and anonymised or pseudonymised where appropriate.

Building consumer trust by enforcing strong policies around data governance, protection and consumer control will be the difference between organisations that thrive and those that fall behind the pack.
1. What is the Consumer Data Right and what is the DCR Bill all about?


The Consumer Data Right (CDR) (if enacted, with effect from 1 July 2019) “will provide individuals and businesses with a right to efficiently and conveniently access specified data in relation to them held by businesses; and to authorise secure access to this data by trusted and accredited third parties”.

The CDR will also require businesses to “provide public access to specified information on specified products they have on offer”. So the CDR will also have an element of mandatory product disclosure.

The CDR aims to facilitate ‘apples with apples’ comparison of products and portability of data to facilitate switching between providers. The Government’s stated policy rationale for the CDR is “through requiring service providers to give customers open access to data on their product terms and conditions, transactions and usage, coupled with the ability to direct that their data be shared with other service providers, the Government expects to see better tailoring of services to customers and greater mobility of customers as they find products more suited to their needs”.

Although expressed as a consumer right, the CDR will also be exercisable by businesses of any size.

The responsible Minister (the Australian Treasurer) may designate a sector by specifying information within that sector that is held by specified persons (or a specified class of persons). The Treasury Laws Amendment (Consumer Data Right) Bill 2018) (CDR Bill) (when enacted) will enable the Treasurer to confer the right sector by sector, without limitation as to which sectors may be designated.

Importantly, the draft CDR Bill proposes to enable the Treasurer (when conferring the right in relation to a particular sector) to designate (1) categories of information within that sector that is subject to the right, and (2) particular businesses within that sector holding that information.

There will broadly be three categories of CDR data – CDR data that relates to a CDR consumer or has been provided by the consumer, including CDR data that relates to a person’s transactions; CDR data that relates to a product (such as product information data like that contained in a product disclosure statement); and CDR data that is derived from these ‘primary’ sources.

The CDR Bill does not limit information that may be specified to confer the right sector by sector, without limitation as to categories of data. Although the already developed proposal in relation to the CDR in the retail banking sector lists particular retail banking products and basic transactional data sets in relation to each of those products, the CDR Bill does not restrict the nature of data sets that might be mandated as subject to the CDR to (say) basic customer record data and transaction data sets.

Accordingly, the Treasurer could designate data sets which include value added data and other derivative data including inferred customer attributes, modelled scores, linked data and imputed or inferred data.

Although the Government states “further sectors of the economy may be designated over time, following sectoral assessments by the ACCC in conjunction with the OAIC”, the Treasurer will have broad discretions. The Treasurer may or may not follow the ACCC’s advice. That noted, the Treasurer is required to ‘consult’ with the competition regulator (the ACCC) and the privacy regulator (the OAIC, being the Office of the Australian Information [Privacy] Commissioner) before specifying a sector, information within that sector, or persons to whom the CDR will apply.

The ACCC may also make a recommendation to the Minister to designate a sector of the economy, provided that the ACCC has first undertaken public consultation in relation to the impact and benefits of the CDR to the sector and consumers within the sector.

The ACCC and the OAIC are responsible for implementation rules for each designated sector.

The draft Explanatory Memorandum states:
“The consumer data rule making powers provide substantial scope for the ACCC to make rules about the CDR. This is because it is important to be able to tailor the consumer data rules to sectors and this design feature acknowledges that rules may differ between sectors. Variance between sectors will depend on the niche attributes of the sector and consumer data rules will be developed with sectoral differences in mind in order to ensure existing organisational arrangements, technological capabilities and infrastructure are able to be leveraged and harnessed as appropriate. Regulatory burden will also be managed via this process.

As noted above, it is important that the ACCC be able to make rules that can be tailored to vastly different sectors. While in the initial roll out it is expected that the banking, telecommunications and aspects of the energy sector will become designated and subject to the CDR, in the future it is possible that insurance information or retail loyalty cards, and the value-added data relating to those cards, may be subject to the CDR system.”

A new Data Standards Body is responsible for development of data standards. Data61 is the interim Data Standards Body.

There are also detailed privacy rules included in the draft CDR Bill, designed to overcome any objection that the Australian Privacy Principles (APPs) may not apply to some data subjects (such as businesses, not being individuals protected by the APPs), data recipients or data sets within the scope of operation of the CDR. The interaction of these proposed detailed privacy rules with the APPs raises issues of significant complexity.

The current Federal Government has committed to applying the CDR to the banking, energy and telecommunications sectors.

The CDR related to banking data is commonly referred to as the “Open Banking” initiative and is running to an advanced timetable.

Given political sensitivity as to retail energy prices, the Federal Government is likely to seek to accelerate the timetable for the energy sector to ensure that the Government has politically attractive announcements to make before the next Federal election as to increasing price competition in the retail energy sector.

However, the CDR will not commence in operation in any sector before 1 July 2019.

2. What is the status of the CDR, ‘open banking’ and ‘open data’ reforms?

The current streams are:

Open banking

Categories of banking transactional data to be subject to the right to be as recommended in the (now completed) Scott Farrell Review.

Detail as to data sets, including data standards, now under development by Data 61 as interim Data Standards Body.

ACCC to be empowered to make a recommendation to the Treasurer as to the banking sector, banking transactional data sets, in the case (unlike all other sectors) without any public consultation.

Implementation depends passage of the CDR Bill and action by the Treasurer.

This process is now driven by Treasury, in consultation with ACCC.

Relevant staff within the Department of Prime Minister and Cabinet (PM&C) responsible for CDR policy have been transferred to Treasury.

Open banking data standards

Industry consultations led by Data61 are now underway. The first Data61 workshop minutes were released on 21 August 2018. There is expected to be exposure drafts released by Data61 progressively over the next few months.

The draft Standards are likely to be significantly influenced by UK standards and recent proposals by the Hong Kong Monetary Authority.

Energy sector

No consultations have been announced to date.

Telecommunications sector

No consultations have been announced to date.

CDR Bill

The CDR Bill is the legislative implementation platform for all CDR initiatives.

Passage of the CDR Bill is necessary to effect implementation of the CDR in all sectors, including banking.
New Australian Government Data Sharing and Release Legislation and establishment of the National Data Commissioner

This initiative relates to Federal public sector data and open government data initiatives and is intended to provide a simpler, more efficient data sharing and release framework for data sets held by Federal government departments and agencies.

This is likely to be particularly important in relation to health sector data, but will also require coordination with State and Territory Governments as many health data sets involve both Federal and State regulated data.

A consultation paper as to this initiative released in July 2018 called for input by 1 August 2018. This consultation process is being led by PM&C.

3. More details about declaration of a CDR right for a sector

Prior to making a designation, “the Minister must consider a range of factors in order to inform his or her decision and ensure that the designation of the sector is appropriate. The ACCC will be responsible for advising the Minister on these matters”.

These factors include the likely effect of the instrument on (i) consumers; (ii) the efficiency of relevant markets; (iii) privacy and confidentiality of information about consumers (iv) promoting competition; (v) promoting data driven innovation; and the likely regulatory impact of allowing the consumer data rules to impose requirements on data holders.

The Treasurer must consult with the ACCC and OAIC and commission a report from each of them about the proposed declaration. There is no minimum period prescribed for this consultation.

The ACCC (note: not the Minister, or the OAIC) must conduct a public consultation before finalising the ACCC’s report to the Minister.

The reports of each of the ACCC and OAIC must be published, but not necessarily before the Minister makes her or his declaration. Accordingly, the only assured opportunity for prior public consultation is in response to the ACCC’s call for submissions in relation to development of the ACCC’s report to the Minister.

4. Accredited data recipients

“Accredited data recipients” are entities holding CDR data as a result of that CDR data being disclosed to them at the direction of a CDR consumer under the consumer data rules.

CDR data held by accredited data recipients can also include data derived from consumer CDR data (including de-identified or aggregate data which is derived from CDR data).

In order to have had CDR data relating to a CDR consumer disclosed to it, the entity must hold an accreditation. Accreditation will initially be managed by the ACCC, who will be the Data Recipient Accraller.

Data holders within the CDR system will only be treated as accredited data recipients if they seek to participate in CDR as recipients of CDR data or if the consumer data rules mandate that outcome.

When in possession of a consumer’s CDR data, an accredited entity can also be directed by a consumer to provide that data to other CDR participants. This is referred to as the principle of reciprocity.

A person does not have to be an Australian citizen nor a permanent resident in order to apply for accreditation.

Examples given include:

A UK Fintech offers a budgeting app, which takes into account transaction data available under the UK Open Banking regime. They hold a UK Account Information Service Provider licence in order to do so under that regime. They wish to provide a similar service in Australia utilising account transaction data accessed under the Australian ‘Open Banking’ CDR system.

They must obtain accreditation under the CDR.

Kathryn moves to the USA and wishes to transfer her banking and telecommunications information to Berkeley Bank, an American bank. Berkeley Bank is an accredited recipient under the CDR and offers to help Kathryn find the best telecommunications services in the USA for her needs. Kathryn is able to establish a line of credit in the USA using her Australian banking information, and Berkeley Bank helps her find internet and phone plans that allow her to call home as often as she did in Australia.

CDR consumers may also direct that their CDR data be provided to a non-accredited entity. Data that has been derived from CDR data, such as financial reports compiled from transaction data, may also be transferred by a CDR consumer out of the CDR system: for example, a data transfer to Xero, or to a consumer’s accountant.

5. Key observations

The CDR Bill (if enacted) will in effect be a very substantial expansion in the discretions and powers of both the Australian Treasurer and the ACCC, an independent statutory authority but closely aligned with the Australian Treasury.
The CDR Bill is quite different from existing competition powers of the ACCC. These existing powers are largely after-the-event powers to order remedies for misuse of market power or other demonstrated failures of competition in a particular industry sector. These existing powers do not enable the ACCC to shape supply-side competition in an industry sector (in the case of the CDR Bill, by regulatory mandate of data flows to address what the ACCC regards as information asymmetries that impede switching between service providers).

There is no analogous regulatory power in comparable jurisdictions. In this respect Australia is ‘going it alone’ in both the potential breadth of operation of the CDR and the discretions conferred upon regulators as to whether, how and when the CDR is declared.

The CDR Bill does not limit sectors, entities or categories of information in relation to which the CDR may be declared. The Treasurer could designate data sets which include value added data and other derivative data including inferred customer attributes, modelled scores, linked data and imputed or inferred data. The Australian Treasurer has said that it is not intended to extend the CDR to value added derived data sets, but the draft Bill does not limit exercise of the Treasurer’s discretions in any relevant way. And the requirements for public consultation are minimal.

The CDR Bill may well be enacted, relatively soon, in some form. With a tight timetable the draft CDR Bill could be revised and introduced into Parliament in Q1 2019. Passage of the CDR Bill is necessary to effect implementation of the CDR in all sectors, including banking.

Public comments and submissions on the Exposure Draft CDR Bill closed on 7 September 2018.

Peter Leonard is a data, content and technology business consultant and lawyer and principal of Data Synergies. He was voted by Sydney technology lawyers as ‘Sydney Information Technology Lawyer of the Year’ for 2016 as a warded by Best Lawyers International. He is rated by Best Lawyers International 2017 as leading in the areas of Commercial Law, Information and Technology Law, Privacy and Data Security Law. Peter was a founding partner of Gilbert + Tobin.
A Canadian data analytics firm has received the first formal enforcement notice under Europe’s General Data Protection Regulation (GDPR) from the UK Information Commissioner’s Office (ICO).

While the brevity of the notice may raise more questions than it answers, it is a useful indicator of potential GDPR enforcement focus areas – and that European regulators are prepared to pursue entities anywhere in the world for breaches of the GDPR.

Our research indicates this enforcement notice is not only the first UK order under the GDPR, but also the first in Europe. So it’s somewhat surprising that it only recently came to light, given the notice was issued on 6 July 2018. Included as an easily-missed link at the end of the ICO’s report on its investigation “into the use of data analytics in political campaigns”, there is no mention of it on the ICO enforcement webpage. The fact it was a GDPR notice was only spotted last week by a UK law firm and the media has been surprisingly quiet. Has the GDPR hype cycle moved on?

What does the enforcement notice say?

The ICO has ordered AggregateIQ Data Services Limited (AIQ) - a Canadian data analytics firm alleged to have close links to Cambridge Analytica - to cease processing UK and EU personal data obtained from pro-Brexit political organisations within 30 days of the notice. According to the BBC, AIQ was paid nearly £3.5m by several pro-Brexit organisations to target prospective voters with political ads on social media during the Brexit referendum campaign.

Failure to comply with the notice could result in a penalty notice requiring payment by AIQ of up to €20 million or 4% of total annual worldwide turnover, whichever is higher. AIQ denies any wrongdoing and has appealed.

AIQ was given the names and email addresses of UK individuals under contracts with its political clients. Despite collecting the personal data before the GDPR came into force on 25 May 2018, the ICO states that AIQ’s confirmation that the “personal data regarding UK individuals was still held by them” meant that the GDPR applies.

The notice states that AIQ failed to comply with the GDPR by processing personal data in a way that data subjects were not aware of, for purposes they would not have expected and without a lawful basis. The processing was incompatible with the purposes for which it was originally collected and AIQ also failed to provide data subjects with relevant information about its use of the personal data, typically done using a privacy notice or policy.

Interestingly, the ICO describes AIQ as a “data controller” but then subsequently refers to it as processing personal data “on behalf of UK political organisations” – language usually used to describe a “data processor”, including in the definition in Article 4. Unhelpfully, the notice does not explain why AIQ is considered to be a data controller.

Top 5 Takeaways for Non-European Organisations

1. GDPR regulators are serious about pursuing non-European entities

Serving the enforcement notice on a non-European entity demonstrates both the GDPR’s extra-territorial reach and that European regulators are not afraid to exercise their powers outside Europe.

While the facts of this case are fairly extreme – not many New Zealand or Australian organisations are likely to be involved in political campaigns with the potential to influence the democratic outcomes of other countries - the notice should serve as something of a wake-up call to organisations around the world that process European personal data. Are you prepared to risk €20 million plus fines and significant reputation damage by choosing to believe geographical distance negates any real likelihood of being penalised for GDPR non-compliance?

2. Online “monitoring” could trigger your GDPR exposure

In the absence of an EU establishment, the ICO’s basis for applying the GDPR to AIQ was its “monitoring of behaviour” of EU individuals (Article 3(2)(b)). You will be “monitoring” the behaviour of EU individuals if you track them online (e.g. using cookies), including profiling individuals to analyse or predict “personal preferences, behaviours and attitudes” (Recital 24). This covers a wide range of online marketing...
and personalisation activity.

The enforcement notice does not discuss why AIQ’s activities were considered to be monitoring, the more opaque “third limb” of Article 3’s Territorial Scope provision. But it shows you cannot overlook this trigger for the application of the GDPR, particularly in the borderless world of the internet.

3. You must determine your lawful basis for processing

The processing of personal data is only lawful under the GDPR if one of six grounds applies, including consent and performance of a contract (Article 6). Unhelpfully, the enforcement notice does not detail why none of those grounds applied to AIQ. Compliance with Article 6 requires analysis of your different types of data, a determination of the applicable lawful basis for processing of each, documentation of those decisions to meet your accountability obligations and transparent communication of your lawful grounds to individuals.

4. Transparency is key

Individuals have the right to be informed about the collection and use of their personal data. Most organisations do this with their privacy policy/notice. But where the personal data is obtained from third parties, you must provide individuals with the relevant information within at least a month of collection, subject to certain exceptions (Article 14).

This can be challenging in practice. Have you considered and addressed how to communicate the requisite privacy information to individuals whose data you are using but with whom you don’t have a direct relationship?

5. Fines are not the only risk

There is a growing view that “cease processing orders” could be one of the most powerful tools in EU regulators’ toolkit. Ordering an organisation to stop processing personal data could have a debilitating impact on its ability to conduct business. How would your business fare if you were forced to stop using all personal data of your European customers and/or employees?

Potentially even more damaging than fines or other regulatory orders is the brand and reputational harm associated with GDPR non-compliance. The heightened global privacy debate and the ever-increasing awareness of individuals’ privacy rights makes this a real, tangible risk despite potential questions as to the ability to actually enforce GDPR orders outside Europe.

What should you be going to manage your GDPR risk?

1. Assess whether the GDPR really applies. Do you have a presence in Europe? If not, do your European activities trigger the GDPR, including online monitoring? Conversely, a risk-based analysis determining the GDPR does not in fact apply (or does not apply to certain parts of your business) could save substantial compliance costs.

2. Undertake a GDPR gap analysis to help you prioritise and take a risk-based approach to achieving compliance.

3. Understand the extent of your online monitoring. Online advertising and targeting can involve multiple partners in a complex web of relationships. You need to understand the extent to which you are “monitoring the behaviour” of EU data subjects and conduct a Privacy Impact Assessment to determine the extent of your risk.

4. Establish your lawful bases for processing personal data. Particularly if you are relying on “legitimate interests”, requiring a balancing of your interests against those of data subjects.

5. Build processes to ensure transparency. Agree with third parties collecting personal data on your behalf who will be responsible for communicating the necessary information to individuals and who will conduct privacy policy reviews, updates and approvals.

It remains to be seen what the ultimate outcome of this first enforcement notice issued under the GDPR will be. We can only hope the final decision resulting from AIQ’s appeal will clarify some of its vagaries.
'Privacy: Handling the Seismic Shift'
Managing personal information in the era of disruption

This year, iappANZ will grapple with the SEISMIC SHIFT in privacy and data protection. We’ll explore emerging trends in privacy regulation, media, technology and innovation. We’ll hear from thought leaders from Australia, NZ and around the world.

SUMMIT: Melbourne | 1 November 2018
WORKSHOPS: Melbourne | 2 November 2018

For more info, click below
https://iappanz2018summit.floktu.com/register