# Contents

| 1 | VICE PRESIDENT’S FOREWORD  
Veronica Scott | page 4 |
| 2 | 2018 UPDATE FROM OAIC  
Timothy Pilgrim | page 6 |
| 3 | Q&A WITH THE OFFICE OF THE NEW ZEALAND PRIVACY COMMISSIONER | page 8 |
| 4 | PERSPECTIVES ON CYBER RISK IN AUSTRALIA – 2018 CYBER RISK REPORT  
Veronica Scott | page 10 |
| 5 | GDPR AND BEYOND  
Georgia Milne | page 11 |
| 6 | NEW BOARD MEMBER PROFILE  
Daimhin Warner | page 13 |
| 7 | ACCC ISSUES PAPER ON MARKET POWER OF DIGITAL PLATFORMS IN MEDIA AND ADVERTISING  
David Templeton | page 14 |
| 8 | AUSTRALASIAN IMPLICATIONS OF VICARIOUS LIABILITY FOR PRIVACY BREACH  
Olga Ganopolsky | page 16 |
| 9 | LESSONS LEARNED FROM THE STRAVA DATA DEBACLE  
Anna Johnson | page 18 |
| 10 | PRACTITIONER FOCUS - PRIVACY PAUSE: WHY SOME ORGANISATIONS ARE LAGGING BEHIND  
Nicole Stephensen | page 20 |
| 11 | LEGISLATION UPDATE - AUSTRALIA | page 22 |
| 12 | 2018 EVENTS CALENDAR | page 23 |
| 13 | NAID MANDATORY BREACH NOTIFICATION LAW WORKSHOP  
Emma Heath | page 24 |
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 (http://www.iappanz.org/)

If you have content that you would like to submit for publication, please contact the NEW 2018 Editors:

Your new Journal editors are

Lyn Nicholson (Lyn.Nicholson@holdingredlich.com) and Katherine Gibson (katherine@gibsonslaw.co.nz) the co-chairs, covering both AU and NZ and Veronica Scott, has kindly agreed to stay on and our team Nicole Stephenson and David Templeton.

It is a new year and a new team so if you have a fresh 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.

We hope that all contributors to Privacy Unbound over the past few years will continue to support us and look forward to bringing new authors to the journal.

Please note that none of the content published in the Journal should be taken as legal or any other professional advice

2017 Writing Prize

The eligible articles for the 2017 writing prize have been judged by the 2017 Committee and a decision has been made to award the writing prize to Katrine Evans, Senior Associate at Hayman Lawyers in Wellington for her article on The expanding definition of personal information, published in our #77 edition in March/April 2017. It was a hot topic for 2017. Congratulations to Katrine and watch out for her re-published article and profile in our next edition.

Out and about

The Board has been extremely busy over the past few months since the AGM setting down policies and procedures for the ongoing management and governance of the organisation and developing plans with our Committee Co-Chairs (Journal, Events, Membership and Summit). We also enjoyed a recent visit from IAPP’s Director of International Operations Tory Bell who travelled from the USA to meet with the Executive and Board in Australia and New Zealand to discuss IAPP’s resources, and membership benefits and to get to know the region better. I will be travelling with iappANZ President Melanie Marks to IAPP’s Summit in Washington DC in a few weeks to continue our discussions, meet with the IAPP team, attend events and plug in to the global IAPP membership. Watch out for our reports from DC in the next edition.

As members and their organisations finalised preparations for the start of the NDB Scheme last week, many have turned their attention to the commencement of the GDPR at the end of May. iappANZ was delighted to partner with elevenM and MinterEllison to host renowned privacy expert Sheila Fitzpatrick, in a series of talks last month that answered many of our burning questions about GDPR. Georgia Milne from Holding Redlich provides a great overview of the sessions for anyone who missed it.

Thank you Timothy Pilgrim

In other news, we are sorry to see the retirement of the Australian Information Commissioner Timothy Pilgrim who has contributed enormously to the development of the privacy framework in Australia over many years. He leaves the OAIC in great shape and his reflections on 30 years of the Australian Privacy Act for us provide food for thought. The Journal has also valued all of the insights he has given members over the years.

Also in this edition

Thanks as always to New Zealand Privacy Commissioner John Edwards for his Q&A with his predictions for the coming year in and proposed law reforms in New Zealand. Staying across the Tasman, we also get up close and personal with Daimhin Warner, one of our new Board directors who also sits on the IAPP Certification Advisory Board that is developing the CIPP/ANZ exam.

MinterEllison has released its third annual Cyber Risk Report which looks at how cyber resilient Australian organisations are. Staying in Australia, following the recent release of the ACCC issues paper to kick off is Inquiry into the market power of ‘free’ digital platforms which collect our data, Board director David Templeton explains why we should get involved. Former Board director Olga Ganapolsky looks at the issue of vicarious liability for privacy breaches in light of a recent UK decision following the supermarket chain Morrison’s data breach. The unstoppable Anna Johnson of Salinger Privacy has provided us with her thoughts on lessons learned from the ‘debacle’ of the Strava social network. Finally, iappANZ member and Journal Committee member Nicole Stephens gets deep into the privacy professional challenge of why some organisations are lagging behind when there has been so much progress in the operational and legal privacy and data protection frameworks.

Looking ahead

If you haven’t booked your place at our annual Summit which takes place in Melbourne over 1-2 November 2018, then you should do so now (it will be Spring Carnival too!).
Our Events Committee are busy planning events in Australia and New Zealand over the next few months including for ANZ Privacy Awareness Weeks.

Get in touch

As always, please do not hesitate to contact me, Melanie, our any of the iappANZ team, (through Committee chairs and members, our General Manager Julie Krieger or any of our Board) if you have any questions, queries or thoughts about your membership, participating in any of our committees or contributing to the journal. In the meantime, all the best for the year ahead as it races on.

Veronica Scott is iappANZ Vice-President. She is also senior member of MinterEllison’s Media and Communications team and leader of the firm’s National Privacy Group. Her work covers all aspects of content gathering, creation and publication and big data across traditional and new media, including print, broadcasting and digital.
During these three decades, we have seen remarkable changes to the way personal information is managed. When the Privacy Act first came into force, the internet as we know it today did not exist. IoT technologies, smart devices, and the social media applications recognised by billions of people today belonged to the world of science fiction.

Today, products and services that utilise personal information to provide more efficient and personalised experiences are common. We are also increasingly aware of the innovative potential of data sharing and analysis: it can identify gaps in services, enhance policy-making decisions, and fuel beneficial research across industries.

In this environment, the assurance that privacy is protected is vital. As shown in our long-running national community surveys, people continue to value privacy highly — 58 per cent have avoided a business because of privacy concerns. These concerns can also undermine the social licence various projects involving personal information rely on.

Consequently, in the 30th year of the Privacy Act two significant boosts to privacy governance in Australia take effect.

The first is the Notifiable Data Breaches (NDB) scheme, which came into force 22 February 2018. From that date, Australian Government agencies and businesses required to secure personal information have mandatory data breach notification and assessment obligations under the scheme.

These entities must promptly notify individuals affected by a data breach that is likely to result in serious harm. My Office must also be notified about these data breaches, referred to as ‘eligible data breaches’. When an entity is unsure of whether a data breach meets the threshold triggering notification requirements, they are required to undertake an assessment to determine whether this is the case. This assessment must be reasonable and expeditious, and generally be completed within 30 days. However, this timeframe should be treated as a maximum. Entities should endeavour to complete an assessment as soon as practicable, so that individuals are notified shortly after an eligible data breach.

There is a very practical benefit to prompt notification: it provides individuals with an opportunity to reduce their chance of experiencing harm. By taking action, such as re-securing compromised online accounts, individuals may avoid experiencing the fallout of a breach, and this in turn can limit the potential damage of the breach overall.

The NDB scheme also has a longer-term benefit. By reinforcing entities’ accountability for personal information security, the scheme provides assurance that privacy protection is prioritised. Further, the scheme meets long-standing community expectation for transparency when a breach occurs — 94% of Australians believe a business should tell them when their personal information is lost. As a result, the NDB scheme supports greater public trust in personal information management, which is integral to the operation of projects involving personal information.

My Office has published a suite of guidance on the NDB scheme requirements on our website at www.oaic.gov.au/ndb.

This year, we will also see the implementation of the Australian Government Agencies Privacy Code, which commences on 1 July 2018. The Code sets out specific requirements and key practical steps that agencies must take in complying with Australian Privacy Principle (APP) 1.2. These include appointing a Privacy Officer and a senior official as a Privacy Champion, undertaking Privacy Impact Assessments (PIAs) for all ‘high privacy risk’ projects, and taking steps to enhance internal privacy capability through privacy education or training, among other requirements.

“In this environment, the assurance that privacy is protected is vital”
The Code builds greater transparency in personal information handling practices, and fosters a culture of respect for privacy and the value of personal information. Businesses may also look at the Code requirements as examples of how to comply with APP 1.2, which requires entities to take reasonable steps to implement practices, procedures, and systems to comply with the Australian Privacy Principles.

Discussions about the NDB scheme and Code will feature in the OAIC’s upcoming events for Privacy Awareness Week (PAW), where we will focus on the theme of ‘from principles to practice’.

PAW 2018 will be held between 13 and 19 of May. I hope you will join in this occasion to promote privacy awareness. To get involved, sign-up as a PAW partner on the OAIC website.

In 2018, I also acknowledge a personal milestone — 34 years in the Australian Public Service, including 20 years working in the privacy, Freedom of Information (FOI), and information management space.

It was with these anniversaries in mind that I have decided to retire in late March.

It has been a pleasure to work over many years with iappANZ, and I look forward to following the work and achievements of the dedicated and conscientious individuals I have met in the privacy space as the environment of personal information management continues to evolve.
We’ll announce our new privacy trust mark on 19 March 2018, with $3500 going to the winning designer. The public is also looking at the designs and voting for their favourite.

We want the trust mark to become an incentive for organisations and businesses to start thinking proactively about their customers’ privacy. Building privacy protection into products and services is the best way to stop issues from happening.

Organisations will be able to apply to us to have the trust mark on their product or service. We’ll accept applications for privacy-friendly products and services that take data protection seriously. We hope the privacy trust mark will help New Zealanders make quick, informed decisions about who they can trust with their personal information.

Q3. A tip for privacy professionals – what is one area we should focus on in the coming year?

As data becomes more and more valuable for organisations and businesses, privacy professionals should remember that there’s more to privacy than simply complying with the law.

Just because an organisation’s privacy practices tick all the legal boxes does not mean they are the most effective. We highlighted this in a report last year about a government department’s data collection policy that required social services to provide personal information about their clients so they could get funding.

We should take on a holistic view of upholding privacy rights beyond the minimum legal obligations. An active privacy culture is the best way to keep personal information and your organisation’s reputation safe from harm. How you integrate, review and update your approach to privacy will make all the difference.

Q4. Are there any new insights you can share on NZ Privacy Act law reform?

At the moment draft legislation is being prepared to update
the Privacy Act. We’re anticipating a busy year if a Bill begins to work its way through the House.

One reform proposal would follow in Australia’s footsteps by introducing the mandatory reporting of data breaches, and would bring New Zealand into line with its international counterparts.

Overall, the reforms aim to encourage private and public sector agencies to identify risks and prevent incidents that could cause harm. As the regulator of the Privacy Act, we are expecting the Bill will introduce a broader range of enforcement mechanisms.

**Q5. What is your sense of the effect of GDPR on New Zealand businesses?**

The GDPR will affect any New Zealand business handling personal information about EU residents, even if they’re processing the data outside of the EU itself.

We encourage affected business to review their procedures carefully to make sure they comply.

We hope the broad territorial scope of the GDPR will help lift privacy standards around the world, including New Zealand.

**Q6. What is in store internationally this year for the Privacy Commissioner?**

We’re looking forward to hosting our international colleagues at two events this year: the International Working Group on Data Protection in Telecommunications in late November and our APPA colleagues in early December.

“.... As data becomes more and more valuable for organisations and businesses, privacy professionals should remember that there’s more to privacy than simply complying with the law”
Cyber security and resilience - identifying, understanding and planning for cyber risk, is now critical to any organisation’s data security planning and compliance. It is embedded in the Australian mandatory data breach notification scheme which has just commenced.

Understanding supply chain risks and that cyber security is not solely an IT issue but a board and enterprise wide issue, are important steps in a maturing cyber resilience. A well prepared and resilient organisation can properly respond to cyber data security incidents and ensure business continuity and data access.

This is the third year that MinterEllison has conducted its annual cyber security survey which seeks to understand the cyber resilience of Australian organisations, at a time when more are planning to take advantage of cloud services. Some key findings can be derived from the year on year results. They show that while organisations are becoming more educated and informed about cyber security, they are still not prepared – just over half of respondents did not yet have a cyber incident response plan in place. The number that have taken out cyber insurance has doubled in the last year. While not a panacea, cyber insurance is a useful tool in data breach response planning if it offers the right cover and support.

It’s a question of when not if an organisation will suffer a cyber attack.

A full copy of the report can be found here.

Veronica Scott is iappANZ Vice-President. She is also senior member of MinterEllison’s Media and Communications team and leader of the firm’s National Privacy Group. Her work covers all aspects of content gathering, creation and publication and big data across traditional and new media, including print, broadcasting and digital.
Introduction

On the eve of the commencement of Mandatory Data Breach in Australia, iappANZ was already looking ahead to the next milestone that is the EU General Data Protection Regulation, hosting an exclusive presentation series with internationally renowned privacy and data expert Sheila Fitzpatrick. In a well-attended and fast-paced session titled ‘ANZ, GDPR and Beyond: The Global Ripple Effect’, Ms FitzPatrick, a member of the EU Data Protection Advisory Council and privacy expert in over 160 jurisdictions, talked attendees through the key issues to keep in mind while preparing for GDPR in Australia. Ms FitzPatrick was an excellent and engaging speaker and it was evident that the various awards and accolades she has received, including being recognised as one of Silicon Valley’s Women of Influence in 2017, were well deserved.

Content

In a discussion that touched on everything from the evolving privacy landscape and the regulation ripple effect, to how to handle your own data breach, Ms FitzPatrick had three overarching messages for Australian businesses trying to prepare for GDPR:

1. Don’t panic;
2. Lay your privacy foundations; and
3. Don’t confuse ‘security’ with ‘privacy’.

Don’t Panic!

GDPR is one of the most comprehensive overhauls of privacy regulation in recent history, and its sheer size and reach is enough to send most businesses into a tailspin, but the message here was clear – don’t panic.

Many Australian businesses are still unprepared for the 25 May 2018 start date. In Ms Fitzpatrick’s view, the first step is often the hardest - the key is to just start - and the best place to do that is with your privacy fundamentals. Do you know what personal data you’re collecting, and why? Do you know how it’s used, stored and transferred? Do you have a lawful basis for that collection?

Any interaction with EU resident personal data can be enough to bring you within the GDPR scope and if you can’t answer these questions, then you need to revisit the foundations of your existing privacy framework.

Privacy is not Security and vice versa

Another central theme to the event was the temptation to confuse security with privacy. As the May deadline looms, many businesses are looking to technology to solve their compliance issues. In reality, only around 8 of the 99 articles in the GDPR address technology specifically. Whether you’re managing the issue in-house, or engaging external experts, make sure your advisors appreciate the distinction between the security benefits offered by technology, and the distinct requirements imposed by privacy law. Just because you can store data securely, doesn’t mean you’re entitled to collect, store and use it in the first place.

GDPR “takeaways”

Among the other key takeaways from Ms Fitzpatrick’s discussion were the following:

▪ Extraterritorial: The GDPR represents a significant expansion of the territorial scope of EU privacy regulation, capturing international participants who interact with EU resident personal data.
▪ **Plain English terms:** Businesses must ensure that their personal data terms and conditions are clear and comprehensible. A failure to do so could result in invalidation of those terms and leave the business exposed.

▪ **Right to be forgotten:** The right to erasure demonstrates the importance of data lineage and being able to track how, when and why personal data has been used. If you can’t find it, how can you delete it?

▪ **Scope of Personal data:** The GDPR introduces an expanded definition of what constitutes ‘personal data’ to capture any information relating to an identified or identifiable natural person.

▪ **Lawful basis for collection:** Parties subject to the GDPR will need to consider what (if any) lawful basis for collection underpins their privacy collection practices. Where the legitimate interest basis is relied on, participants should ensure that they can substantiate that claim, as this is likely to be a focus for regulators.

▪ **Designated privacy officer:** An entity’s Designated Privacy Officer cannot also be its Chief Information Security Officer. For GDPR purposes, this is considered a conflict, where responsibility for both data management and data compliance are housed within the same role.

In the context of the discussion, Australia’s existing privacy regulation framework (which draws on previous EU directives) was considered relatively well-placed to adapt to the new GDPR, relative to other schemes around the world. The United Kingdom, for example, is understood to have approximately 29 deficiencies when considered against the GDPR.

The overall message from the presentation was encouraging; certainly the GDPR presents challenges and it is unlikely that any entity will ever be fully compliant at all times, but it is forcing businesses around the world to engage with the issue of privacy and fostering a culture of ‘conscious collection’. In an increasingly globalised and data-driven world, the value of that step cannot be underrated.

The event was co-hosted by iappANZ, Minter Ellison and elevenM.
Q. Mark Zuckerberg famously said that “privacy is dead”. What are your thoughts on this?

A. Privacy is absolutely not dead. In fact, ask anyone in Europe, or anyone outside Europe trying to work their way through the GDPR, and they’ll tell you that privacy is a little too alive. Really, privacy is and always has been a fluid and subjective concept. Privacy means different things to different people, depending on their age, gender, cultural background, knowledge or country of residence.

Ultimately privacy is about control. People have always wanted to be able to control the way their information is collected and used, and this is so regardless of the ways we interact online. So, while the 20-something, tech-savvy online socialite might be happy to share the mundane details of their day, this does not mean they are comfortable for their bank or insurance company to use their financial or health information to develop better marketing strategies. While the parameters may continually shift, people will always have their limits.

As we witness the growth and power of big data, in the private and public sectors (think China’s social credit system), we are seeing a level of public disquiet growing at an equal pace. Global privacy regulation is evolving to meet this discomfort. Privacy laws - and the NZ Privacy Act in particular - traditionally focused on flexibility and an assumption that agencies would take a responsible approach to the application of privacy concepts and principles. This is changing. There has been a realisation that agencies will always push the bounds of what is acceptable, and so privacy regulations are moving to redress the imbalance of power between the individual and corporate and state entities.

2018 and beyond, both in NZ and globally, will be about control, transparency and consequences. We will see data subjects taking the power back and agencies competing to show why they can be trusted. So, if privacy was dead when Mark Zuckerberg made his declaration, then it has reincarnated stronger than ever.
ACCC ISSUES PAPER ON MARKET POWER OF DIGITAL PLATFORMS IN MEDIA AND ADVERTISING

By: David Templeton

The Australian Competition & Consumer Commission has commenced an inquiry into the competition issues posed by digital platforms including Google, Facebook, Instagram, Twitter and others.

The ACCC published an Issues Paper on 26 February 2018 and asks for submissions by 3 April 2018.

The Issues Paper raises questions about the collection and use of consumer information, directly exploring the trade-off between privacy consents exchanged for access to “free” digital platform services, and the impact of newsfeeds compiled by algorithms on the quality of news and current affair content served to consumers.

This article contextualises the Inquiry and expands on some of these topics, aiming to help you decide whether to engage with the Inquiry. Cutting to the chase, if you are a stakeholder in the digital platform value chain, you are likely to be keen on getting involved.

Digital Platforms have changed the landscape

As the Issues Paper observes, a small number of social media, search and other digital platforms now dominate markets for online at a time advertising, media content delivery and other services. The platforms derive advertising revenue by a combination of scale and clever use of insights about consumer preferences to target advertising. Platforms source insights from consumers directly and observe or infer insights from consumer activity on the platform.

To maintain audience attention, the platforms offer a range of services to consumers at no monetary cost, including newsfeeds. The platforms personalise content feeds using proprietary algorithms running, one assumes, on similarly derived insights and assumptions about individual consumers.

The platforms have disrupted traditional markets for media and journalism, rendering traditional journalism uneconomic and sending investigative journalism into much the same death spiral that took Kodak and IBM. 3

Australian public policy on privacy: the story so far

It’s nearly 10 years since the ALRC published "For Your Information: Australian Privacy Law and Practice", an extensive review of privacy. Government implemented many of the ALRC’s recommendations in the 2012 reform package¹ and delivered mandatory data breach reporting last year but has left some other recommendations languishing, including creation of a civil action for serious breaches of privacy.

Subsequently, the Productivity Commission explored the potential of more open access to large datasets, public and private². The Productivity Commission’s recommendations were delivered in 2017 and were extensive and important. They call for significantly greater access to data under public (and in more limited instances, private) control, coupled with a new comprehensive privacy right of access, correction and portability. The Productivity Commission recommended that this be regulated by the ACCC, rather than the OAIC. The Government’s response remains a work in progress.

¹ Privacy Amendment (Enhancing Privacy Protection) Act 2012
² See Productivity Commission Inquiry Report No 82, 31 March 2017 “Data Availability and Use”
Key implications for privacy professionals

The key issues of likely relevance to privacy professionals are:

- Terms and conditions of use, compared to other services;
- Level of consumer awareness, whether consumers understand the trade-off between access to platform services and consent to data use, and whether this trade-off is fairly disclosed and ‘priced’;
- Breadth of the typical privacy consent, which the Paper describes as “wide ranging”\(^6\), and how consumers perceive the privacy trade-off;
- How digital platforms have affected price, choice and quality of news, quality representing “the extent to which the content produced exhibits characteristics such as objectivity and accuracy and performs functions such as analysis and investigation”\(^7\) and whether the use of algorithms has affected the diversity of news supply (the ACCC opining that the “pluralistic and high-quality news content benefits society as a whole”\(^8\)). The Issues Paper observes that content selection algorithms bring a risk that individual consumers’ media feeds become limited to particular topics, perspectives and viewpoints creating a “filter bubble”\(^9\); and
- Overall impacts of Digital Platforms on consumers.

Outcomes that may emerge from the inquiry could include:

- Greater consumer control over content selection; transparency of content selection;
- Closer regulatory scrutiny of the width and duration of privacy consents and the use of data relating to consumer preferences and propensities; and
- A greater role for the ACCC in relation to regulation of privacy, possibly aligned to the role recommended by the Productivity Commission in regulating the proposed new comprehensive privacy right.

Implications and actions

Wrapping all this up, we are moving into a new era of public policy around online data collection and use. Policy makers are looking beyond human rights as the case for data and privacy regulation to economic drivers such as market power, consumer protection and the economic and societal benefits from more open data. This is a global shift.

In parallel with this, the role of competition and consumer regulators in privacy is becoming more significant.

If your organisation is in the digital platform value chain, competes with digital platforms or consumes their services, then it is likely that you may wish to contribute to this inquiry.

Once again, submissions in response are due 3 April 2018.

---

3 Impact of digital mass media on traditional journalism is the subject of other inquiries eg Senate Select Committee on the Future of Public Interest Journalism
5 Issues Paper, page 20
6 Issues Paper, page 10
7 Issues Paper, page 6
8 Ibid
9 Issues Paper, page 10
Could your organisation be liable for the rouge actions of an employee?

According to the Morissons’ case, in the UK, yes....

Despite important legal differences between Australia and New Zealand and the UK, and the fact that there may still be an appeal, this case is a useful reminder of the types of matters that must be addressed by organisations handling personal information.

Below are some quick reminders as to why.

The facts

The Morisons’ data breach came to the attention of the public in March 2014 as a sizable data breach involving the 99,998 employee’s data deliberately posted to a file-sharing website by the company’s (now former) IT auditor. The breached data included dates of birth, addresses, national insurance numbers, and bank sort codes and account numbers.

As many will recall, the data breach was perpetrated by Morisons’ internal IT auditor (IT Auditor), who was at the time a disgruntled employee, protesting what he considered was an ‘unfair’ treatment of him by Morisons. The data breach was his very public revenge.

The revenge backfired, as the IT Auditor was arrested and subsequently convicted for eight years for offences under the Computer Misuse Act 1990 and the Data Protection Act 1998 (DPA).

In many respects, the data breach as perpetrated, is reflective of current research that consistently reports that internal threats to personal data are highly relevant and that the behaviour of contractors and employees is a key consideration in any risk management or privacy program.

This case, takes this truism to another level as the arrest and subsequent conviction of the IT Auditor were not the end of the matter for either Morisons or the affected employees.

Action by the victims of the data breach and the Court’s findings

The affected employees alleged that Morisons was:

- Directly liable, for breach of statutory duty and under common law; and/or
- Vicariously liable for the actions of the IT Auditor.

The Court held that the data breach was attributable to the IT Auditor - not Morisons and that Morisons had met its obligations under the DPA to have appropriate security systems in place.

However, the Court found a sufficient connection between the actions of the IT Auditor and the “course of [his] employment”. It is this as aspect of the finding that makes the case noteworthy.

The key reasons for the Court’s finding were:

- There was an unbroken thread linking the employment to the disclosure as a “seamless and continuous sequence of events”;
- Morisons deliberately entrusted the IT auditor with the data during the course of his employment. The IT Auditor had the responsibility of storing the data and disclosing it to a third party; and
- Morisons tasked the IT Auditor with receiving, storing and disclosing the data. His actions were

1 Various Claimants v Wm Morisons Supermarket PLC [2017] EWHC 3113 (QB) 2017
2 Section 4(4) of the DPA
3 Misuse of personal data and breach of confidence including the tort of misuse of private information, and equitable claim for breach of confidence
The Court’s finding against Morrisons was made despite the fact that:

- the data was disclosed from a personal computer;
- several months after the data was copied; and
- all malicious activity took place outside of work time.

The specific malicious intent of the IT Auditor was irrelevant. Similarly irrelevant was the fact that the actions were criminal in nature and imposing vicarious liability would (in part) assist that criminal intention.

Morrisons has leave to appeal the finding of vicarious liability.

Are there any lessons for privacy practitioners in Australasia?

Despite the legal differences, yes...

The technical legal arguments in relation to liability would be different, largely because of the differences between UK and Australian and New Zealand laws, including important differences between the DPA and the Privacy Act 1988\(^5\).

However, many of the practical implications stand, namely:

1. Security remains key. Were it not for Morrisons’ robust security measures it would probably have faced primary liability as well.
2. Address internal risks and do so on an ongoing basis. Internal risks must be part of your risk assessment and privacy programs. Organisations should consider internal access control regimes and test the measure that impact on the protection of personal information; who has access to that such information, for what purpose and for how long? What does a given type of access enable the person to do? Be prepared to be role and time specific and be especially careful with functions that are ‘entrusted’ to handle or protect personal information. In this case, it was critical that the role of the senior IT auditor was data facing and that as the IT Auditor enjoyed a broad set of user rights, including disclosure to third parties and had access to operating systems user regimes and cryptography. Be similarly careful with the appointment of contractors and service providers.

3. Motive is not relevant. Breaches can happen by accident or maliciously. Motive is not necessarily relevant and certainly not a bar to liability!
4. Affected individuals will take action\(^6\). Individuals are increasingly prepared to press their privacy rights, even if it means launching novel actions. Be prepared to consider the impact of breaches on the individuals and handle their concerns and grievances accordingly.
5. ‘Privacy by design’ is not just relevant to developers. Privacy by design and default often includes a need to take an interdisciplinary approach to privacy in your organisation. Many of the important developments relevant to your role as privacy professional will come from developments and disputes that are not always pure privacy matters. The privacy function must include and partner with aligned functions such as Security, Vendor Management and of course, Human Resources as part of the various privacy initiatives.

\(^4\) Various Claimants v Wm Morrisons Supermarket paragraphs 182 to 196
\(^5\) For example, the different definitions of the two Acts and the employee record exemption under section 7B of the Privacy Act 1988
\(^6\) 5,518 individuals took action in this case

Olga Ganopolsky is the General Counsel – Privacy and Data at Macquarie Group Limited. She is the Chair of the Privacy Committee of the Law Council of Australia and a member of the Dispute Resolution Specialist Accreditation Committee of the Law Society of New South Wales. She is also Australia’s representative on the SWIFT data protection working party and a director of the International Association of Privacy Professionals ANZ.
LESSONS LEARNED FROM THE STRAVA DATA DEBACLE
By: Anna Johnson

Strava is a social network of people who like to not only use devices like FitBits to track their movements, heart-rate, calories burned etc, but to then share and compare that data with fellow fitness fanatics. In November 2017 Strava released a data visualisation ‘heat map’ of one billion ‘activities’ by people using its app. In late January 2018 an Australian university student pointed out on Twitter that the heat maps could be used to locate sensitive military sites. Uh-oh.

The Strava data debacle illustrates a number of privacy problems with open data initiatives.

First, the sheer power of geolocation data is incredible. It can show patterns of behaviour of both individuals and groups, and reveal sensitive locations. Not understanding the risks involved in your data before releasing it publicly is negligent.

Second, geolocation data can be used to find out more about identifiable or already-known individuals; removing identifiers from the data does not make it anonymous.

Third, privacy harms (including physical harm) can be done to individuals even if they are not personally identifiable. (I have previously argued that our privacy laws currently fail to recognise this risk, by protecting only what is ‘identifiable’ data.)

Fourth, when individuals comprise a group, say personnel at an army base or worshippers at a mosque or clients of an abortion clinic, the risk posed by or to one becomes a risk for all.

Fifth, when data is combined from different sources, or taken out of context, or when information is inferred about you from your digital exhaust, the privacy issues move well beyond whether or not this particular app, or device, or type of data, poses a risk to the individual. The risks become almost impossible to foresee, let alone quantify.

Finally, and of importance well beyond geolocation data: the utter failure of the US-model of privacy protection, which relies on ‘notice and consent’ instead of broader privacy principles placing limitations on collection, use or disclosure. Many commentators have been quick to judge the users of the Strava app, saying that military personnel for example should have never allowed themselves to be tracked. And sure, it is easy to judge. But first, look at how the app works. Privacy by Default it ain’t.

The Future of Privacy Forum’s review found that Strava’s request for access to location data – that little box that pops up on your phone when you first install the app, asking you to ‘Allow’ or ‘Don’t Allow’ did not mention public sharing. Instead, it says “Allow Strava to access your location while using the app so you can track your activities” (emphasis added).

A Strava user herself has explained how she discovered that her workout routes were accessible to (and commented on by) strangers, even when she thought she had used the privacy settings in the app to prevent public sharing of her data. A Princeton professor (who happens to be an expert in re-identification) noted that if he couldn’t understand whether or not Strava’s privacy settings actually worked to obscure the user’s home address, or whether the use of a fake name would be enough to prevent cross-linking with other data, how is a more typical app user supposed to determine where their own level of comfort sits, and how to achieve it?

So before blaming the users, perhaps instead we should be asking why the company did not follow Privacy by Default design rules, why the privacy controls settings are so complex, and why the initial permission request to users about their location data was so misleading.

This is not just a problem with Strava. The 2017 OAIC Community Attitudes Survey found that 32% of people ‘rarely or never’ read privacy policies and notifications before providing personal information. (And let’s face it: the other 68% of people probably lied.) Burying detail in complex privacy policies is a lawyer’s art form. Is it really reasonable to expect consumers to have read and understood them before they click ‘I accept’?
Then there are apps which track your location (or copy your address book, or turn on your microphone) without you being told at all: 16% of Android apps in one survey were found to give no notice about the data they were collecting from users. Add in the revelation that Google was tracking the location of users of Android phones, even when they switched off all their location settings, and you can see that consumer-blaming is utterly misplaced.

But even if Strava had done a better job of informing its users about how their data would be shared (with the company, with other users, and ultimately with the public), there remains a problem with the 'notice and consent' model of privacy protection. As academic Zeynep Tufekci has noted, ‘informed consent’ is a myth: “Given the complexity (of data privacy risks), companies cannot fully inform us, and thus we cannot fully consent.”

Putting the emphasis for privacy protection onto the consumer is unfair and absurd. As Tufekci argues in a concise and thoughtful piece for the New York Times:

“Data privacy is not like a consumer good, where you click ‘I accept’ and all is well. Data privacy is more like air quality or safe drinking water, a public good that cannot be effectively regulated by trusting in the wisdom of millions of individual choices. A more collective response is needed.”

“The data is de-identified so there is nothing to worry about.”

“If you don’t like it, opt out”.

“If you’ve done nothing wrong, you’ve got nothing to hide.”

It’s time to put those fallacies to rest. The US model of ‘notice and consent’ has failed. Privacy protection should not be up to the actions of the individual citizen or consumer. It’s the organisations which hold our data – governments and corporations – which must bear responsibility for doing us no harm.

Anna Johnston is a Director at Salingar Privacy. Salingar Privacy offers privacy consulting services, compliance training, and a range of publications including a free Privacy Officer’s Handbook, template policies and procedures, checklists and ebooks. Find out more or sign up for their monthly newsletter at www.salingarprivacy.com.au
It’s quite a spectacle. The commencement of Australia’s data breach notification scheme and, for some global actors, the looming start date for the GDPR, has created a nationwide level of in-house “compliance readiness” chaos that I have rarely seen in my career. It’s both wonderful and woeful. Wonderful because government agencies and organisations (including those offering cloud services and cool apps or platforms) are achieving a level of demonstrable best privacy practice across business streams, services and technical systems. Woeful because folks ought to have been getting their privacy ducks in a row before now.

The OECD, in 1980, released its “Guidelines on the Protection of Privacy and Transborder Flows of Personal Data” and established 8 principals for the fair handling of personal information in any medium which are now found in some form or variation in privacy laws the world over. In Australia, the protection of personal information has been codified since 1988. The States and Territories, with their own laws or administrative schemes, were not far behind.

So, while a collective sigh of relief might be heard after passing the tongue-in-cheek Data Breach Notification Day, as a privacy practitioner I don’t think we should be patting ourselves on the back just yet. Focusing on a specific and measurable compliance goal certainly goes some way to addressing the bigger privacy picture, yet it also highlights for some organisations that their privacy programs have been lagging behind.

Why the lag?

The allocation of responsibility for ensuring privacy compliance is a key tripping point for organisations. The answer varies, depending on who you talk to. In-House Counsel appears to be the logical choice for many; however, this is asking our lawyers to stray from their primary role (ie., the provision of sound legal advice as regards identifying and mitigating privacy risk) into the territory of developing audit tools, conducting privacy impact assessments, writing policies and procedures, developing and delivering staff training, and so forth. Another logical choice may be the Information Security Team, particularly when an organisation is largely “data” focused and operates more in the cloud and less on the ground. This is asking technical security professionals to make principle-based decisions about the handling of personal information throughout its lifecycle – perhaps without the benefit of a policy or best practice lens through which to view (or even identify) a privacy risk.

So, let me offer this: The obligation for privacy compliance lies with the organisation as a whole, not with its component parts. Robust privacy practice (and any chance of achieving meaningful levels of compliance) requires a multilayered internal privacy network, led by a skilled Privacy Director (aka: Privacy Manager, Chief Privacy Officer, Privacy Lead) or, if you are a GDPR aficionado, a “DPO”. The network would benefit from having a number of privacy-skilled but clearly cross-functional members from areas including (but not limited to):

- Legal
- Legislative policy
- Access to Information
- Ethics
- Human resources
- Risk management
- Complaints management
- ICT
- Information security
- Internal audit
- Information asset management
- Records management
- Communications/ media

There is room for an organisation (in support of the work of the Privacy Director) to be clear that best privacy practice is the responsibility of all employees, business streams and business outputs – always. To elevate general privacy-mindedness to an effective on the ground privacy culture, organisations should set expectations of employee and enforce them in a tangible way. For instance, linking privacy awareness and preparedness to employee KPIs can be very effective (providing, of course, that privacy isn’t relegated to a “tick and flick” induction topic covered once yearly in desktop online training).
If, upon reflection, organisations believe they already have the “people” part of their privacy house in order... consider that a privacy program can also slow to a snail’s pace when there is a knowledge gap. What is it that we are protecting?

For a privacy program to be effective over time, organisations need to know their business inside-out and understand where and how personal information is involved. There is no overstating the importance of knowing – really knowing – about the personal information your organisation holds. Consider:

- How much do you have and who is about?
- How is it collated?
- Where is it stored?
- What do you do with it and why?
- Who has access to it and when?
- What risks are associated with having the personal information?
- Are the risks minimised if you have less of the information or manage it in some other way?
- If there was a data breach involving that personal information, would there be a serious impact on a person or group of people? If yes, can the information be dealt with differently now to reduce the risk of a breach?

As a strong proponent of multifaceted privacy programming and accountable privacy culture, I’m interested in the extent to which targeted compliance initiatives (such as data breach notification readiness) has caused organisations to look inward and critically assess their privacy programs as a whole. For those who have been on privacy pause, it’s certainly time.

Nicole Stephensen is a Privacy Specialist with extensive local and international experience in operational and strategic privacy matters. She is Principal Consultant at Ground Up Consulting, a boutique firm she established in 2011. Nicole is a member of the IAPP, as well as iappANZ where she sat for three consecutive terms on the Board.
As at 23 February 2018, three amendments have been made to the Privacy Act.

The first privacy professionals are very well aware of but the others perhaps less so

- **Privacy Amendment (Notifiable Data Breaches) Act 2017 (12 of 2017) [CTH]**

The Act, which came into force on 22 February 2018, amends the Privacy Act 1988 (Cth) (the Privacy Act) by introducing a mandatory eligible data breach notification regime for those entities which are regulated by the Privacy Act.

An “eligible data breach” occurs when there is either unauthorised access to, or disclosure of, information; or information is lost in circumstances likely to result in unauthorised access to or disclosure of information. For such unauthorised access or disclosure to be classed an “eligible data breach”, it must be objectively considered that such access to, or disclosure of, information would result in serious harm to any of the individuals to which that information relates. However, if an entity takes remedial action prior to any consequential serious harm or loss of information following the unauthorised access or disclosure, the act will not be considered an “eligible data breach”.

- **Intelligence Services Amendment (Establishment of the Australian Signals Directorate) Bill 2018 [CTH]**

In response to the recommendations of the 2017 Independent Intelligence Review, the Government has proposed to amend the Intelligence Services Act 2001 (Cth) by shifting the Australian Signals Directorate (ASD) away from the control of the Department of Defence. The Bill proposes to keep ASD within the Defence portfolio, however it would be established as an independent statutory agency and the ASD Director-General would report directly to the Minister of Defence.

ASD will have the responsibility of providing assistance, advice and material to specified persons on matters relating to the security and integrity of electronically stored, processed and communicated information.

More specifically, the Bill grants ASD the power to prevent and disrupt information and communication technologies that are used to commit or facilitate serious crimes by people or organisations outside Australia. As part of the proposed Bill, the Australian Cyber Security Centre (ACSC) and the national computer emergency response team (CERT) would be transferred to ASD. The Bill was referred to the Senate Foreign Affairs Defence and Trade Legislation Committee for inquiry on 15 February and the subsequent report from the Committee is to be released on 21 March 2018. Public submissions to the Bill will close 9 March 2018.

- **National Consumer Credit Protection Amendment (Mandatory Comprehensive Credit Reporting) Bill 2018 [CTH] (Draft)**

The Bill seeks to amend the National Consumer Credit Protection Act 2009 (Cth) by introducing a mandatory comprehensive credit reporting regime. Introduced into Parliament on 2 November 2017, these changes are proposed to be operative from as early as 1 July 2018. Compliance with the proposed mandatory reporting system will be monitored by the Australian Securities and Investment Commission, who have been granted additional investigatory powers under the Act.

The Bill is aimed at providing credit lenders and credit reporting bodies with greater access to data, so that lenders are able to make more informed decisions when assessing individuals for loans. Under the proposed legislation, credit reporting bodies will be able to access comprehensive credit information on any active consumer credit accounts that have been opened with large Authorised Deposit-Taking Institutions (ADIs) and their subsidiaries. As the title to the Bill suggests, it will be mandatory for large ADIs to provide this information. Submissions to the exposure draft and explanatory materials have recently closed on 23 February 2018.
2018 EVENTS OVERVIEW

Jan  
- Privacy After Hours
  - BNE
  - MinterEllison

Feb  
- Social Media and Privacy
  - WEL
  - KPMG

Mar  
- Privacy After Hours
  - PER
  - Deloitte

Apr  
- GDPR in Action
  - AKL
  - Microsoft

May  
- General Event -
  - ADL
  - Thompson Geer

Jun  
- Privacy After Hours
  - SYD
  - CBA

Jul  
- Privacy After Hours
  - AKL/WEL

Aug  
- Privacy After Hours
  - SYD

Sep  
- General Event
  - AKL/WEL/SYD/MEL

Oct  
- Privacy After Hours
  - SYD

Nov  
- Privacy After Hours
  - MEL

Dec  
- Privacy After Hours
  - MEL

- iappANZ Summit

Additional Events:
- Sheila Fitzpatrick
  - Syd/Mel/Adl – elevenM, MinterEllison and Thompson Geer

- Privacy Awareness Week (PAW)
  - BNE, SYD, MEL, ADL, AKL, WEL
  - OAIC – Brisbane
  - OPC Forum - WEL
NAID MANDATORY DATA BREACH NOTIFICATION LAW WORKSHOP

Join NAID in this one day workshop especially designed for data destruction & privacy professionals, compliance and security officers and facility managers.

The agenda will focus on the new Data Breach Notification Law, the impact this Law has on business and how to convey the necessary changes to information managers, suppliers and clients.

Speakers include:
• Malcolm Crompton, former Australian Privacy Commissioner & IIS Director
• Victor Chin, Thales Australia
• Paul Curwell CPP, Director, Deloite Risk Advisory
• Richard King, Security Program Manager, Office of the NSW Government Chief Information Security Officer (GCISO)

Half Day: Content appeals to privacy professionals, compliance and security officers, and NAID-ANZ Members in Australia.

Full Day: Content is geared for NAID-ANZ Members.

Full Agenda

22 MARCH, THURSDAY
Rydges Sydney Central Hotel
9.30am – 12.30pm Half Day
9.30am – 3.30pm Full Day

$95 – Half Day
$133 – Member Full Day
$171 – Non Member Full Day

Note: All pricing is reflected in USD.

Full Day registration includes arrival tea and coffee, morning and afternoon tea, buffet lunch with soft drinks.

Half Day registration includes arrival tea and coffee and optional buffet lunch with soft drinks.