Privacy Unbound iappANZ

June/July 2016

UNLOCKING THE TRUTH ABOUT PRIVACY

ISSUE 72

President's Letter

By Kate Monckton
President
M: 61 409 613 029

Dear Members,

Many of you who have ever had a query about iappANZ, attended an iappANZ Summit, workshop or helped on a sub-committee would likely have met or had contact with our wonderful General Manager, Emma Heath. After a great few years with us, Emma is moving on to a new challenge. She has been pivotal in growing our organisation and providing all our members with high quality information, help and events. On behalf of the Board and all our members I'd like to thank Emma for all her hard work and wish her well in the future. You can continue to contact us with any questions or suggestions you have on admin@iappanz.org.

If you are in New Zealand in early August we'd love to see you at the 'An Electronic Health Record For Every New Zealander by 2020 - What Does This Really Mean Forum' will be held in Wellington with a live video link to Auckland. Speakers include the Director General of Health, Chai Chuah, New Zealand Medical Association Chair, Dr Stephen Child, and OPC Senior Policy Adviser Sebastian Morgan-Lynch. It is free for iappANZ members ($99 for non-members). Register for Wellington here and for Auckland here.

Coming up on 21st September in Sydney it's the NAID-ANZ Data Protection Made Easy: A Teamwork Approach Conference and iappANZ members are entitled to a 50% delegate discount making the cost of attendance $124.50. For more information, including the program for the day please visit naidanz.org.

As always I love to get your feedback on what we're doing well or what we could improve on to keep supporting you all in the privacy space.

Cheers,

Kate

Kate Monckton
iappANZ President

Vice-President's Foreword

By Anna Kuperman
(Joint) Vice-President

Dear Members

We have a super mix of articles in this edition looking at the latest technology trending with some privacy dressing to throw in the mix as always. From blockchain to the Pokémon Go craze, there's something for every privacy enthusiast and closet technologist. On a serious note, the articles share a fundamental theme which is the complex balancing act between data protection and new technology. Navigating the balancing act requires the application of privacy controls in a sensible way whilst allowing the users to experience the benefits of new technology. It's not a trade off but a trade up.

Some of our members will have heard Russell Burnard, the Government Chief Privacy Officer (GCPO) in New Zealand speak at iappANZ events and our annual Summit. Russell is a generous and valued contributor to our association and a vibrant and engaging speaker. There is an interesting profile on the GCPO, its recent activities and steps taken to help ensure trust in government – the biggest collector of data.

Richard O'Neill from the Office of Australian Information Commissioner (OAIC) highlights the OAIC's latest review of loyalty programs with a special mention of a brand that has certainly been over exposed in recent weeks – you know it's the app that makes you look for little creatures!

Annelies Moens addresses the perceived virtues of blockchain technology and the privacy implications of this seamless way of transacting. Is it really the Holy Grail it promises? Is trustable auditable computing possible in a decentralised form without compromising privacy?

Board Director and Co-Editor of our journal, Carolyn Lidgerwood writes on the recent media attention on Veda for using online forms to obtain a free or paid for credit report as a 'marketing opportunity'. Some food for thought on the use of pre-ticked boxes … often a marketing short-cut tool to expand databases. But no, like other places around the globe, pre-ticked boxes are not an acceptable way of gaining consent.

For express consent to exist, a person must actively and deliberately give consent.

Alexander Vulkanovski looks at some high level outcomes from the Internet of Things in our privacy space, and Kyle Lees writes a brilliantly entertaining piece on Pokémon Go. What's the bargain being made by these app enthusiasts? Any less invasive then other popular apps? Probably not, just the sheer appeal of the craze and public attention to the nomad walker sightings brings about curiosity as to the choices made by default to allow indiscriminate access to personal data.

Happy reading ☺

Anna

A message about iappANZ membership:

Membership benefits

iappANZ has grown into the pre-eminent forum for people with an interest in privacy in Australian and New Zealand, offering our members a wealth of opportunities to expand their privacy knowledge, compliance, interests and networks. We continue to work with private entities across all industry sectors as well as regulators in both countries.

As an iappANZ member you are entitled to receive a range of great member benefits as outlined at: www.iappanz.org.

Through our affiliation with the global body, the International Association of Privacy Professionals (**iapp**), you are also entitled to additional member benefits, including the knowledge and resources located within the members' only area of the iapp website at: www.privacyassociation.org.

You can access benefits available to you through your iapp account. Simply login to your MyIAPP account using your email address as the username. If you do not yet have a password or have forgotten yours just click on the 'Reset your password' link and instructions on how to create a new password will be sent to you. If you don't want us to confirm your membership details to iapp in accordance with iappANZ's privacy policy, please let me know by emailing me at emma.heath@iappanz.org.

I hope that access to these additional privacy resources will be of benefit to your work as a privacy professional.

Emma Heath, iappANZ General Manager

Visit our website, join us on LinkedIn or follow us on Twitter

To join the privacy conversation, keep up to date on developments and events and to make connections in your professional community, connect with us today!

Our website is www.iappANZ.org.au. You can log in to our member area from our website homepage with your email and password to access past bulletins. You can also get a new password or be reminded of your username if you have forgotten it. Just click on the links on the log in box. If you still need help email us at admin@iappanz.org.

Our LinkedIn group is:
http://www.linkedin.com/groups?gid=1128247&trk=anetsrch_name&goback=.gdr_1281574752237_1

Follow us on Twitter at: https://twitter.com/iappANZ

Pokémon GO: "The Delusion of Solitude"

by Kyle Lees

The recent mania around Pokémon GO– a smartphone centered augmented reality game not only brings into sharp relief Guy Debord's revelation of the society of spectacle – a global social praxis split into reality and image – but also serves as a unique platform upon which to question how we value privacy in an increasingly post-digital society. [1]

Millions of people have downloaded Pokémon GO to smartphones in the last week. Almost overnight, the game has become a literal cultural phenomena of our epoch, seemingly surpassing society's need to date, tweet, or download anything else.[2] In downloading the game – the result of a collaboration between retro gaming company Nintendo, and a former Google start up – unsuspecting 'Poketrainers' delivered colossal amounts of user data to the company's developer, Niantic Inc.[3]

When originally released, the game had the potential to do the following by default: read email, send email on your behalf, access and delete Google drive documents, see your search history and maps navigation and access any private photos.[4] Tech Security writer, Adam Reeve soon discovered that signing on to the service through iOS effectively allowed the app carte blanche access to a person's entire Google Profile, furnished with all the information in their Google Account.[5]

Cue moral-digital outrage.

After an unrelenting howl on social media from the battlefields of the tech cyber security world, Niantic issued an official statement. Having seen a riot about to break out, the developer directed users to their own privacy policy for further details and like Pilate, washed their hands before the crowd. We are innocent of this blood they said, and you shall bear the responsibility.6 Further, Niantic tasked benevolent brother, Google with correcting the issue. "Once we became aware of this error, we began working on a client-side fix to request permission for only basic Google profile information, in line with data that we actually access."[7] Privacy panacea pacified, or a beguiling attempt to discretely capture an information goldmine? Between the lines, the statement could have read: 'all of that access was merely a simple design error, we are not the big data *Decepticons* you dread, and outside of a simple standard Google ID and email address, none of your personal information was *or will be* accessed.' The question remains: why did millions upon millions of people grant full access to their personal information, essentially by choice?

According to its own updated privacy policy following the fix of this seemingly innocuous privacy pitfall, Niantic continue to track your phone's location whilst playing the game, your IP address, and the webpage you visited most recently before playing – using a Google map of your city and GPS location data to place you in real locations where virtual Pokémon lurk uncaptured. Niantic can also share the data it collects with Pokémon Co., a partial subsidiary of Nintendo, who, along with Google are investors in Niantic.[8] Interestingly, the leviathan, Niantic, takes its name from a whaling ship that brought fortune to San Francisco.[9]

But is all this precious information critical to supporting people's use of the application?

---

[1] Guy Debord, *La Société du Spectacle*, Buchet-Chastel, Paris (1967).pp.1-37.
[2] See:https://itunes.apple.com/au/app/pokemon-go. As an aside, *Pokémon GO* went to the top of Download list in both app stores and is set to have more daily users than Tinder.
[3] See: *Drew Olanoff, Niantic Labs, Maker Of Ingress, Spun Out Of Google As Its Own Company, Tech Crunch (August 12, 2015).*
[4] See Adam Reeve's blog: http://adamreeve.tumblr.com/post/147120922009/pokemon-go-is-a-huge-security-risk. See also, Robert Abel, *Prepare for Trouble: Pokemon Go sparks privacy issues, malware*, muggings, SC Magazine (July 12, 2006).
[5] *Ibid.*
[6] Niemtec Privacy Policy. https://www.nianticlabs.com/privacy/pokemongo/en.See also: Matthew 27:24, *Berean Study Bible*, BIble Hub; 1st edition (2016)
[7] 'Niantic Permissions Update'. See: https://support.pokemongo.nianticlabs.com/hc/en-us/articles/222648408-Permissions-update
[8] Drew Olaff, *Op cit.,* See also: Nathan Olivarez-Giles *Pokémon Go' Creator Closes Privacy Hole But Still Collects User Data,* Wall Street Journal (July 12, 2006).
[9] See (reluctantly) Wikipidea https://en.wikipedia.org/wiki/Niantic_(whaling_vessel)

As Marc Rotenberg, President of the Electronic Privacy and Information Centre attests, 'you can build a game that superimposes graphics over the real world that relies on maps and locations, without having to know a person's name. Niantic made the choice not to do that'. [10]

Herein lies the rub.

Privacy controls around applications can't or *won't* discriminate between which pieces of personal data users want to share. The privacy choice becomes an opt-in wedged between a rock and a proverbial hard place. On one hand, use the app and provide some level of access to your personal information, or on the other, don't.

Outside of the privacy realm, there are other factors to contemplate where technology intersects with the real. Augmented reality and virtual reality are extremely interesting technologies with a plethora of perceivable benefits for humankind – socially, economically and virtually. Yet amidst the hysteria of *Pokémon GO* and its release are the well-trodden media examples of young Poketrainers stumbling unbeknownst into murder scenes, court houses, or extreme right wing strongholds whilst playing the game.[11] Is this an example of what Debord termed the 'negation of life' becoming visible?[12] Let's take the idea of *Pokémon GO* itself, its release and meteoric rise as an example of a spectacle. Debord writes that the spectacle presents itself to society as a means of unification. Debord would argue that the unification *Pokémon GO* achieves is nothing but the official language of universal separation. [13]

Source: NSW Department of Justice Facebook Page

Caption: *Pikachu, Pika! I love you so much.*

[10] Quoted in Nathan Olivarez-Giles, *Op cit.*

[11] Media examples abound. See notably: Shelby Carpenter, *Westboro Baptist Church Uses 'Pokémon GO' To Battle 'Sodomites*, Forbes (12 July 2016)

[12] Debord, *Op cit.*

[13] *Ibid.*

Perhaps, there's no escape from reality. As ever, time will tell if this rise of so called 'ubiquitous computing' [14]also wields the opportunity to be pervasive and thereby inescapable. Could the same be said of *Pokémon GO*?

What remains for the future – as increasingly bright consumer technology glistens provocatively behind an ever more intricate web of privacy and security considerations – is difficult to ascertain. Are we creating a panopticon privacy nightmare? Or, a *Blade Runner's* dream – replenish with kitchens which order food, washing machines working by themselves and cars calling on behalf of a patient etherised upon a table? Perhaps the solution to reclaiming our privacy rests in the concept of 'privacy by design' and increasing the sophistication of how an application handles the problem of letting users choose which information they'd like to share or protect. Or, more clearly, a collective social manoeuvre towards forcing Technocrats into only collecting information they truly need to make an application function. But with personal information increasingly a commodity, this certainty for the time being remains unlikely. This writer wonders if the Office of the Australian Information Commissioner (OAIC) will make inroads into this space to ensure that the collection – or moreover the definition of personal information in the face of expanding technology – doesn't escape the reality of Australia's *Privacy Act*.

Kyle Lees writes in a personal capacity and as an iappANZ member.

[14] Weiser, Mark & Brown, John Seely, *Designing Calm Technology*, PowerGrid Journal, v 1.01, (July 1996). See: http://powergrid.electriciti.com/1.01. See also, Weiser, *Mark, The Computer for the 21st Century*, Scientific American, (1991). See: http://www.scientificamerican.com/article/the-computer-for-the-21st-century/

The Government Chief Privacy Officer (New Zealand): Who is he and what does he do?

From the Office of the GCPO

Background

New Zealand responded to a number of privacy/data breaches and incidents by establishing a Government Chief Privacy Officer (**GCPO**). This may be the only GCPO in the world or at least the only one with that title.

Russell Burnard was appointed in 2014 as the GCPO to be responsible for privacy leadership across government including:

- setting the vision for privacy in government
- development of guidance
- capability building within agencies
- providing assurance to government and
- system-wide engagement with the Privacy Commissioner and other stakeholders.

The Government Chief Privacy Officer is not the regulator - that is John Edwards, the Privacy Commissioner (www.privacy.org.nz).

Nor is the GCPO the official Administrator of the *Privacy Act* 1993, responsible for the Act itself and the policy work that supports the Act. That is the role of the Electoral & Constitutional team at the Ministry of Justice.

The GCPO role is that of functional lead for the management of personal information across the NZ Government. This role falls within the within the broader functional leadership of the Government Chief Information Officer, Colin MacDonald. Colin is also the Chief Executive of the Department of Internal Affairs. Along with the responsibility for system-wide policy, directions, and standards for ICT, the Department includes the National Library, Archives New Zealand, and Government Information Services which publishes the New Zealand Gazette. It is a deliberate concentration of government professional expertise in a broad range of information related disciplines.

The first two years

The GCPO team will have been in operation for two years in July this year. It is a small team of 8 full-time employees focused on working with each individual agency.

In our first year, the focus was on building relationships across the 41 core government agencies then within our mandate and getting guidance and support out to help agency privacy officers with their often sizeable responsibilities. In July 2015, the 20 District Health Boards who are responsible for providing or funding the delivery of most health services in New Zealand were added to our mandate for a total of 61 agencies today – comprising some 100,000 employees.

In common with our GCIO colleagues, our model is 'centrally led and collaboratively delivered', which means that agencies retain their decision-making autonomy but are expected to work with us to meet government's goal of improved management of personal information. In 2014, the GCPO issued ten core expectations of all agencies within our mandate that represent good practice for privacy management and government within the State services. Those expectations are supported by a Privacy Maturity Assessment Framework (PMAF) that helps agencies assess their own privacy capability and identify where and how they can make improvements (https://www.ict.govt.nz/assets/Guidance-and-Resources/Privacy-Framework-August-online.pdf).

The PMAF and core expectations assume that agencies will apply a risk-based approach to their investment in personal information management. Small agencies with little or no personal information beyond employee data are not expected to implement systems

comparable with those of large agencies with thousands of employees and information about many or all New Zealanders. Our primary target in year one was to emphasise the vital importance of getting robust governance in place for personal information, executive oversight and commitment and allocate resources for a suitable privacy programme. This year we provided agencies with a self-assessment reporting tool that was completed and signed off by chief executives in March. We will report to Ministers by 30 June on the results of that self-assessment exercise.

Our model is deliberately based on self-assessment because we cannot be responsible for decisions made by chief executives and their senior leadership teams. Nor are we funded to undertake any model that requires a formal audit function - we believe that agencies' internal and external auditors are responsible for that role.

Having said that, we believe that most of the agencies in our mandate have taken on board the message about the importance of good governance, and that they now have a member of their senior leadership team explicitly responsible for good privacy practice. This year's self-assessment is intended to establish a baseline for all agencies, individual and severally. We will be reporting aggregate data only on three groups of agencies: large agencies with substantial personal information holdings, mid- and small-sized agencies, and thirdly, the District Health Boards. We will not publish information about any individual agency.

Our immediate future

We have published several other pieces of collateral in the last two years, some to provide basic support for agencies in getting privacy programmes and messages out to their people. We have established a Privacy Forum that meets about 5 times a year for all agencies within our mandate to encourage the development of a community of practitioners within government and provide them with practical support. Our emphasis now is on getting beyond the basics and looking to promote privacy as an opportunity to build customer-centric services. The tools we have developed for that have been very well received including by operational people who find the documents speak to their needs (https://www.ict.govt.nz/assets/GCPO/Privacy-Realising-opportunities-Handout.pdf).

Those tools we hope will be of particular use in supporting agencies faced with significant collaborative work programmes to respond to government's 10 better public services (BPS) results areas. Key outcomes from those 10 results areas are: reducing welfare dependence, supporting vulnerable children, boosting skills and employment, reducing crime, and improving interactions with government. Helping agencies to put in place the necessary information sharing mechanisms that will allow appropriate and safe information sharing to support the BPS outcomes will be a key part of our work programme this year.

Our other major goal is to improve our working relationship with the District Health Boards. As their name suggests, they are scattered the length and breadth of the country. This provides a new challenge as we can no longer simply work through agency privacy officers headquartered in Wellington.

Whatever unexpected challenges this next year brings, one thing will stay constant: trust remains paramount because citizens will trust the government with their information only so long as they are confident we will not misuse it.

Russell Burnard is the Government Chief Privacy Officer (GCPO).
The GCPO and his team can be contacted at: gcpo@dia.govt.nz

Update from the OAIC – simple breaches, the price of loyalty, and what does Pikachu know about you?

by Richard O'Neill

In July the OAIC is taking a particular focus on building awareness of basic privacy rights (and how to access them) in Australian consumers and communities – and three recent announcements have been useful in highlighting our messages to individuals about basic good privacy practices.

Firstly, at the start of July the Australian Privacy Commissioner, Timothy Pilgrim, released five privacy determinations that bust the myth that privacy breaches inevitably involve high-tech approaches and complex 'hacks'. The fact is that many privacy breaches are simple, basic human errors, yet can do significant damage to those affected. While the five determinations have differing stories, they are all cases of 'low tech' privacy breaches resulting from human error or basic failures in business management – and demonstrate how privacy obligations are part of everyday business management – not just 'an IT issue'. They remind business leaders that data breach risks often lie not with some unknown hacker, but with their own staff and processes – and reinforce to consumers that a breach of their privacy can be as simple as a misdirected letter, and need not involve technology at all.

In mid-July the Commissioner released an assessment report into the two biggest consumer loyalty schemes in Australia – Coles Flybuys and Woolworths Rewards. Given that over 80 percent of Australians have a loyalty card, the story attracted significant consumer interest, with the Commissioner speaking to the Today show, ABC PM, and other many other media outlets, generating significant new knowledge of privacy rights amongst Australian consumers. While the assessments showed that both Coles' flybuys and Woolworths Rewards had appropriate privacy notices that were consistent with their practices, the public interest generated by the report highlighted the importance of customers being aware of the bargain we enter with retailers when we sign up for loyalty programs.

Finally, in timing that was serendipitous for a month focussed on individual privacy practices, the PokemonGo phenomenon burst onto the Australian public. With mixed messages and reports emerging about exactly what data was captured in the rush of Australians to join the craze, the Commissioner announced that the OAIC would be making initial enquiries with the app's provider to ensure that personal information of users is being managed in accordance with the Australian Privacy Act. The media coverage of the craze also allowed another opportunity for the Commissioner to reinforce the need to check privacy policies on apps before playing them. After all, catching a Zubat in the office is fine – provided you've read the privacy policy first.

Richard O'Neill is the Director, Strategic Communications and Coordination, Office of the Australian Information Commissioner

Unravelling the mystery of blockchain – Do privacy professionals need to be concerned?

by Annelies Moens

"I am in the process of booking an apartment in Stockholm and I have the option of paying through a company that purports to be able to send money with the real exchange rate (not marked up), which sounds great, until I start to read the privacy policy… which essentially says that all my information including account information could be shared with a wide ranging number of third parties."

I thought this practical scenario was a good lead in to my participation at the European Identity and Cloud conference in Munich in May which included a full day on blockchain and where I raised my Stockholm booking scenario. Blockchain is an electronic distributed ledger system designed to cut out costly middle agents to enable faster and cheaper processing, not dissimilar to the company I was going to use to transfer money to pay for the apartment in Stockholm.

This technology is being talked about everywhere, but how new is it and do we really understand it? This article is an attempt at explaining the basics of blockchain with a perspective for privacy professionals. The original intent of blockchain was to conduct trusted transactions between parties over untrusted networks. Blockchains involve a large number of parties that see the data within blocks and use consensus algorithms to reach agreement on the integrity of the distributed blockchain. The revolutionary factor in blockchain is that it locks down an event in real-time.

Blockchain is not a new concept and is derived from a 1979 patent on merkle trees (Mastering Bitcoin, Chap 7: The Blockchain). Each block in a blockchain contains a summary of all the transactions in the block, using merkle trees, which are binary hash trees used for efficient verification of data integrity (Bitcoin Developer Reference, 2015 p.3).

Blockchain's strength lies in determining the provenance and trackability of transactions. As such, it works well where there are:

- Brokers and intermediaries involved which can be eliminated;
- Highly regulated businesses with strong audit and governance requirements;
- Lengthy processes and settlement of deeds;
- Shared businesses with multiple parties involved.

Blockchain can be used in many situations including, identity and authentication, finance, internet of things, cryptocurrency, smart contracts, government and legal record keeping. There are many businesses starting to use blockchain technologies. A few examples include:

- International payments – Ripple – the first global decentralised transaction settlement network designed to reduce clearance and settlement time
- Cryptocurrency – BitStamp – first EU bitcoin exchange platform with a banking licence in Luxembourg
- Real estate financing – Ubitquity – securely, recording, tracking and transferring of title
- Digital content – Ascribe – sharing and tracing digital work
- Smart contracts (or not so smart contracts) – Ethereum – platform which runs contracts

So what, from a privacy view, do we need to think about as the blockchain technology rolls out in various different applications and sectors? - Keeping in mind that this is a new field of technical activity with a lack of standardization (though National Standards Bodies, including Standards Australia are keen to address this through international standards setting).

Responsibility/Governance

Who would be regulated and responsible if there was a data breach?

Earlier, I mentioned that blockchains use consensus algorithms to reach agreement on the integrity of the distributed blockchain. In a decentralised model there is a shared responsibility, so changes can only occur with "consensus", which generally means that more than 50% of participants in the network need to agree. Consequently, when there is a data breach, it is not necessarily clear how responsibility is going to be allocated.

For example, in mid June, Ethereum (a platform which runs smart contracts) was subjected to a multi-million dollar hack which exploited a loophole in its code. The code was being rigidly followed but produced unforeseen and undesirable outcomes. "Unlike normal contracts which can be interpreted by smart people, … smart contracts are interpreted by computers. Computers are dumb. They can only do what they are told."

It remains to be seen how the Ethereum hack will play out and be resolved. Broadly speaking, the governance of blockchain still needs to mature.

Trust

Can we trust blockchains?

Trust is an integral component to effective privacy and takes significant effort to establish and takes seconds to undo. The original permissionless (public) model of blockchain was intended to overcome the problem of (not) trusting third parties (Development Bank of Singapore, Understanding Blockchain Technology Feb 2016 p.16).

However, it is impossible to eliminate trust, as it is:

- An unavoidable element of human life
- We don't know the future but plan for it
- We don't know to what extent our perceptions are true; and
- We don't know to what extent our memories are real or not

Permissioned (private) blockchains have been set up to limit users and ironically attempt to assure trust at the expense of resilience and robustness which a permissionless model provides (UK Government Office for Science, Digital ledger technology: Beyond block chain p.48).

Again, it remains to be seen how trustworthy blockchains will be and, in my view, their level of trustworthiness is, in part, dependent on the quality of their governance framework.

Right to be Forgotten

Can we delete information?

Internationally, relatively new privacy concepts, such as the right to be forgotten are being introduced. That will sit rather uncomfortably with blockchain technology which is designed to keep transactional information in perpetuity. The extent to which this encompasses personal information remains to be seen. However, the global trend towards information being more easily attributed to individuals suggests to me that this will eventually become a thorny issue.

Transparency

Can we keep our privacy?

Transactions in blockchain are recorded in a decentralised model in such a way that there is complete transparency as to all the transactions that have taken place from first to most recent – hence why its strength lies in determining provenance and trackability of

transactions. This means that information, including potentially personal information, will be widely accessible and is why I didn't go ahead with my Stockholm booking as outlined at the beginning.

So, let me leave you with another quote, this time from a discussion about the Bitcoin blockchain from a UK government report (Digital ledger technology: Beyond block chain p.51).

"Unlike traditional online payments, which are only visible to transacting parties and financial institutions, Bitcoin payments — including the wallets involved, the approximate time of the transaction, and the transaction values — are recorded in a publicly visible block chain. Anyone can process the block chain and draw inferences about, for example, the turnover of an on-line merchant, the buying profile of a particular user, or even the many transfers between private individuals — a capability that was restricted in the past to financial institutions and law enforcement."

Annelies Moens is the Deputy Managing Director, Information Integrity Solutions and is a former President of iappANZ.

Annelies can be contacted at: amoens@iispartners.com

Ticked off: pre-checked boxes and privacy

by Carolyn Lidgerwood

A recent report in *The Sydney Morning Herald* has criticised credit reporting company Veda for its use of 'pre-ticked' or 'pre-checked' boxes to obtain consent for direct marketing.[1] In summary, a consumer is reported as being surprised to receive direct marketing material from a bank after applying for a personal credit report from Veda:

> *'I got the letter a few weeks after I bought my personal credit report from Veda … I feel my privacy's been breached, but I did fill out the form in a rush because I was under pressure, so they may have gotten my consent without me realising' …. It appears Simon left a pre-ticked box at the end of the online form untouched, inadvertently giving his consent to Veda and its 'corporate partners' to use his personal data for marketing purposes…*[2]

Following this media report, pre-ticked boxes could still be seen in Veda online forms, including this:

> ☑ You agree to Veda group and its corporate partners using and disclosing your personal information to contact you about other goods and services and using your information for direct marketing purposes including contact by phone, email, SMS or other electronic means.[3]

From where I sit, the most surprising thing about this is the purported reliance on pre-ticked boxes to evidence consent for electronic and other marketing. It's not what I'd expect in this day and age.

In Australia, the *Spam Act* governs the sending of 'commercial electronic messages', including email and SMS direct marketing communications. The Spam Act is enforced by the Australian Communication & Media Authority (**ACMA**), rather than the Office of the Australian Information Commissioner (**OAIC**).

Under the Spam Act, there are three pre-conditions to the lawful sending of commercial electronic messages – and one of those is consent. The definition of 'consent' under Schedule 2 of the Spam Act means either express consent or 'consent that can reasonably be inferred' from a person's conduct or from business and other relationships. When it comes to the issue of whether a pre-ticked box amounts to consent, the ACMA's guidance couldn't be clearer:

> **Can I use pre-ticked boxes to obtain consent to send messages?**
> *No. Pre-checked tick boxes—for example, on a website where people can join a mailing list—are not an acceptable way of gaining consent.*[4]

There's nothing new in this – that same guidance has been provided (in one form or another) since the Spam Act was enacted back in 2003. The ACMA is firm on the position that a pre-ticked box won't amount to express consent or inferred consent for Spam Act purposes.

Further, if we look at the use and disclosure of personal information for direct marketing purposes more broadly, Australian Privacy Principle 7 in the *Privacy Act* 1988 also presents challenges when it comes to reliance on pre-checked boxes. APP 7.2 permits the use

---

[1] The Sydney Morning Herald: *Credit reporting giant Veda under fire for the way it obtains customer consent*, 27 June 2016 (see at http://www.smh.com.au/business/consumer-affairs/credit-reporting-giant-veda-under-fire-for-sneakily-obtaining-customer-consent-20160624-gpqvwe.html).
[2] ibid
[3] https://forms.mycreditfile.com.au/Apply/Index?form=FreeCreditFile&_ga=1.120387018.391896087.1467338095
[4] Australian Communications & Media Authority http://www.acma.gov.au/Industry/Marketers/Anti-Spam/Ensuring-you-dont-spam/spam-consent-ensuring-you-dont-spam-i-acma

and disclosure of personal information for direct marketing purposes if a four-pronged test is met, namely:

a. the organisation collected the information from the individual; and

b. the individual would **reasonably expect** the organisation to use or disclose the information for that purpose; and

c. the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and

d. the individual has not made such a request to the organisation. (*emphasis added*)

If someone doesn't notice a consent accompanied by a pre-ticked box, I suggest that it becomes difficult to argue that the second limb of the APP7.2 test is met. While an objective assessment (or argument) may be that 'they should have seen' the pre-ticked box and hence 'reasonably expect' the relevant use or disclosure of their personal information, complaints about interferences with privacy will turn on the facts. As the OAIC states in its APP Guidelines:

> *6.20 The 'reasonably expects' test is an objective one that has regard to what a reasonable person, who is properly informed, would expect in the circumstances. This is a question of fact in each individual case. It is the responsibility of the APP entity to be able to justify its conduct. (*emphasis added*)*

Further, if there's no 'reasonable expectation', that will mean that consent for the relevant direct marketing is required under APP7.3 - unless it is 'impracticable' to obtain that consent. Again, it seems hard to argue that it is not practicable to collect consent from a person who is completing a form. This takes us back to where we started – with a pre-ticked box and whether that can be taken to be consent.

As with many issues in data privacy, it can be interesting to compare approaches in other jurisdictions. There are numerous overseas examples of pre-ticked boxes not amounting to consent. For instance, under Article 4 of the new EU *General Data Protection Regulation* (which will commence in 2018), 'consent' of a data subject is defined as:

> *any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*

Recital 32 of the GDPR clarifies that such an affirmative action may include 'ticking a box', and goes on to say '*Silence, pre-ticked boxes or inactivity should not therefore constitute consent*'.

Anti-spam regulation in Canada can also be seen to be applied in a very similar way to that in Australia. For instance, the website of the Canadian Radio-Television and Telecommunications Commission (**CRTC**) says this about Canada's Anti-Spam Legislation (often described as **CASL**):

> **Can I use pre-checked boxes in order to obtain express consent?**
> *The manner in which you request express consent cannot presume consent on the part of the end-user. Silence or inaction on the part of the end-user also cannot be construed as providing express consent. For example, a pre-checked box cannot be used, as it assumes consent.*
> *Rather, express consent must be obtained through an opt-in mechanism, as opposed to opt-out. The end-user must take a positive action to indicate their consent. For example, this can be done by providing a blank box which a user can check off to indicate consent.* [5]

[5] Canadian Radio-Television and Telecommunications Commission http://crtc.gc.ca/eng/com500/faq500.htm. In a broader Canadian context, the Privacy Commissioner of Canada is also currently considering how to enhance the current consent model under Canada's federal privacy legislation See *Consent and privacy: A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act*: https://www.priv.gc.ca/information/research-recherche/2016/consent_201605_e.asp#fn15

My point in mentioning these examples is to illustrate that Australia is 'not an island' when it comes to the issue of pre-ticked boxes and consent – particularly in an anti-spam context.

So is it worth the argument that a pre-ticked or pre-checked box is good evidence of consent? If you do this, what does it say about your company's attitude towards the personal information of its customers, or other people it does business with? What does it suggest about trust and accountability?

In the last issue of *Privacy Unbound*, Marta Ganko[6] wrote about the Deloitte Australian Privacy Index 2016 (described as an annual assessment of the privacy practices of more than 100 leading consumer brands operating in the Australian market). Amongst this year's findings was that more than 90% of the 1,000 Australian consumers surveyed valued trust over convenience.

That's some food for thought if your company is thinking about pre-ticking a consent box.

Carolyn Lidgerwood is a board member of iappANZ. The views expressed in this article are Carolyn's personal views.

[6] Ganko, M, *Trust without Borders*, Privacy Unbound, issue 71.

The Internet of Things and the Australian Privacy Landscape

by Alexander Vulkanovski

On face value, 'Internet of Things' (IoT) refers to connecting everyday objects to the Internet, and to each other. In 2013, the term was admitted into the Oxford English Dictionary, defined as "the interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data"[1] . This may be an oversimplification. A mature IoT ecosystem would include hundreds of sensors and data collection points collecting data on almost anything– environmental indicators, physical movement, biological data, technical functionality, and more. All of this data can then be combined with other datasets, processed, analysed, and used to draw intimate inferences on the subjects, including personal information.

It is not hard to see the implications on consumer privacy.

The Connected Home, Human and Habitat

IoT case studies are virtually unlimited. The Connected Home will contain appliances that can be monitored and controlled via the Internet, including fridges, toasters, espresso machines and dishwashers. Even water bottles, door locks, air conditioning units and toothbrushes can be Internet-enabled, as well as include other sensory networks. The Connected Human is able to quantify their wellbeing like never before, including wearable activity trackers, heart-rate monitors, GPS systems and even Internet-enabled insulin pumps and pacemakers. Smart cities, smart vehicles and sensor-enabled agriculture form the Connected Habitat, where movements and behaviors in cars and public spaces are able to be quantified like never before. All of these devices collect data on individuals and their behavior, and with enough datasets, may form personally identifiable information from metadata.

The Conceptual Implications of IoT on Privacy

IoT will have a number of effects on privacy management. The complexity of information privacy will be heightened by new data collection points and methods, and the risk of unwittingly capturing personal information is alleviated by the intimate nature and quantity of IoT data. Preserving personal privacy will also be trickier, with more connected 'things' able to collect personal information, as well as the increasingly intimate nature of the data collection. For example, the home, car and human body will increasingly become valuable sources of individual data and personal information. Finally, a lack of IoT security and interoperability standards alleviate the risk of communication privacy being compromised.

However, IoT does not create any new privacy issues; instead, it adds complexity to existing privacy issues by enabling greater volumes, new types and methods of data collection. These complexities are summarised at a high level below[2] :

1. Scale – It creates more data collection points, since more 'things' collect data;
2. Method – It creates novel ways of collecting data, such as via sensors and smart things;
3. Reach – It penetrates more intimate areas of our lives, such as data on our bodies and inside our homes;
4. Nature – An advanced IoT ecosystem is designed to collect data covertly and 'in the background' via sensors and other digital tools, meaning that consumers may not be aware of the collection of personal information; and

[1] Definition of 'Internet of Things', *Oxford English Dictionary (UK)*
[2] Vulkanovski, Alexander, Home, Tweet Home: Implications of the Connected Home, Human and Habitat on Australian Consumers (2016) Australian Communications and Consumer Action Network, Sydney <http://accan.org.au/our-work/research/1154-home-tweet-home>

5. Depth – The collective result of the above four concepts will be greater than the sum of the parts. As a result of greater scale, new methods, reach and nature of data collection and processing, IoT will have a synergistic effect on existing privacy concerns.

As the industry eagerly awaits the result of the Privacy Commissioner's appeal in the matter of Ben Grubb v Telstra Corporation Limited [2015] AICmr 35, it is important to consider the implications that this decision may have as big data gets bigger, more intimate data is collected on people and spaces, and processing methods improve. As the IoT industry matures, Amara's Law seems applicable to privacy implications as well as technological development – "we tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run".

Alexander Vulkanovski writes in a personal capacity and as an iappANZ member.

Events

Where and when	Event details	Price
WELLINGTON and AUCKLAND **Monday 8 August** 9.15am – 12.30pm *The event will be held in Wellington with a video link to Auckland* WELLINGTON Chapman Tripp Level 17, 10 Customhouse Quay Wellington AUCKLAND (via video-link from Wellington) Level 35, 23 Albert Street Auckland	**An Electronic Health Record For Every New Zealander by 2020: What Does This Really Mean?** *The recent strategy announced by the Ministry of Health to establish a national electronic health record for individuals will affect every New Zealander. The strategy will impact how and where health records are stored and used by health practitioners (and potentially others) and how patients will be able to access their health information.* *It is intended that electronic health records will be accessible across the country and the Ministry of Health has said that "Privacy is Assured". Actions to design and implement the strategy are scheduled to commence in 2016/2017.* This event is for leaders and senior managers in health, privacy and Health technology and leaders in patient advocacy wanting to understand the strategy implications and be part of the discussion. You will: • Hear from Chai Chuah, Director General of Ministry of Health, about the details of a national eHealth Record and the rationale for adopting the strategy. • Understand how this will affect the efficacy of medical practitioners from Dr Stephen Child, Chairman of the New Zealand Medical Association. • Learn about the privacy impacts of an eHealth Record system from Sebastian Morgan-Lynch, • an expert on the topic from the Office of the Privacy Commissioner. • Understand the patient perspective from Barbara Robson, an experienced health consumer advocate. • Gain insight into the lessons learnt internationally in implementing similar systems from IT expert Dr Bernard Robertson-Dunn, Chair of the Health Committee of the Australian Privacy Foundation. • Enjoy an opportunity to network with other industry leaders and professionals.	**COST:** Free for iappANZ members Non-members $99NZD (deductible from iappANZ joining fee if you become a member) WELLINGTON - register here AUCKLAND - register here **https://an-electronic-health-record-for-every-new-zealander-what-does.lilregie.com/step1**

SYDNEY **Wednesday 21 September** Australian Technology Park 2 Locomotive Street, Eveleigh	**NAID-ANZ - *Data Protection Made Easy: A Teamwork Approach Conference*** Join us for a day of insightful information and discussion on key issues regarding secure information handling now and into the future. At the seminar you will: • Learn what the future of data security holds • Discover tools to ensure that your business is protected • Explore the human factor - how to raise security awareness and create trust in your business • Selecte the service provider that suits your needs • Network with like-minded people	For more information and to register visit naidanz.org NAID will give iappANZ members a 50% registration discount on the NAID Member Delegate Rate. As an iappANZ member, your Delegate Rate will be USD92, ~AUD124.50.
SYDNEY **Monday 14 November** 8.30am – 6.20pm incl. 1 hour networking Dockside, Darling Harbour	**** SAVE THE DATE**** **iappANZ *TRUST IN PRIVACY* Summit** Are you up to date with the latest privacy trends, developments and issues? Are you interested in hearing from some of the world's leading privacy thought leaders? Do you want to network with like-minded privacy people? Come and join us for a day of insightful information and discussion on the key issues regarding privacy now and into the future. Speakers and program agenda to be announced shortly.	Summit enquiries: admin@iappanz.org

IAPP Certification

Privacy is a growing concern across organizations in the ANZ region and, increasingly, privacy-related roles are being made available only to those who can demonstrate expertise. Similar to certifications achieved by accountants and auditors, **privacy certification** provides you with internationally recognized evidence of your knowledge, and it may be the edge you need to secure meaningful work in your field.

Our global body, the International Association of Privacy Professionals (iapp) says:

> *'In the rapidly evolving field of privacy and data protection, certification demonstrates a comprehensive knowledge of privacy principles and practices and is a must for professionals entering and practicing in the field of privacy. Achieving an IAPP credential validates your expertise and distinguishes you from others in the field.'*

What certifications are available? Are they relevant to my work here?

Currently, the iapp offers six specialised credentials, two of which are particularly relevant to iappANZ members, namely the Certified Information Privacy Professional/ Information Technology (CIPP/IT) and the Certified Information Privacy Manager (CIPM).

To achieve either of these credentials, you must first successfully complete the Certification Foundation. The Certification Foundation covers basic privacy and data protection concepts from a global perspective, provides the basis for a multi-faceted approach to privacy and data protection and is a foundation for the distinct iapp privacy certifications.

It has recently been announced that a new CIPP Asia certification is coming in 2016, and a CIPP ANZ certification is anticipated for next year – watch this space!

What about testing?

Certification testing is available to iappANZ members locally (at iapp-approved computer-based testing centres). The iapp manages certification registrations and materials, and you can set an appointment to sit your exam online at a testing centre in Australia or New Zealand.

FIND OUT MORE at: http://www.iappanz.org/index.php?option=com_content&view=article&id=34&Itemid=5

Employment opportunities for privacy professionals

News about employment opportunities is provided as a service to iappANZ members. If you would like a notice about employment opportunities at your organisation published in Privacy Unbound, please contact our editors (see details on last page)

Digital Trust and Privacy Advisor

Company: SAP

Location: Sydney, NSW, AU

Expected Travel: 0 - 30%

Career Status: Professional

Employment Type: Regular Full Time

COMPANY DESCRIPTION

As market leader in enterprise application software, SAP helps companies of all sizes and industries innovate through simplification. From the back office to the boardroom, warehouse to storefront, on premise to cloud, desktop to mobile device – SAP empowers people and organizations to work together more efficiently and use business insight more effectively to stay ahead of the competition. SAP applications and services enable customers to operate profitably, adapt continuously, and grow sustainably.

PURPOSE AND OBJECTIVES

The primary objective of this is newly created role is to be the internal and external advocate of SAP's data protection and privacy guidelines compliance. The position will be a central pivot interfacing with SAP's global Data Protection & Privacy Office (Germany), SAP's Cloud Services Security & Audit (Germany and US), and SAP ANZ's Management, Legal and Sales leadership with respect to both SAP's data protection policies and procedures from a Customer Contract perspective. The Role is both outward facing in terms of our Customers' data privacy policies and practices, and in terms of being knowledgeable with the current local and regional data privacy laws, and internal in terms of ensuing the Company's compliance with its contractual commitments with respect to data privacy and security. The Role will have reporting into Corporate Management.

ROLE AND RESPONSIBILITIES

Your primary role is the Company's Data Protection and Privacy advocate as it relates to all of SAP's ANZ operations.

In this role, you will be the internal and external champion of SAP's Policies, Processes and Data Processing Agreement in the Company's commercial negotiations and contracts, working closely with the Company's Sales Organisation and Management, and its customers in relation to Australian and New Zealand personal data privacy and security.

You will be the communicator of SAP's global and regional personal data agreements and policy. You will be advocate of SAP's legal positions to Sales and local Management, and also be an advocate of relevant local considerations. You will also articulate Customer's issues and concerns to the Company, the DPO, Cloud Security & Audit and other relevant lines of business. You will call out relevant risks to SAP's business areas. You will also monitor the Company's local compliance – ANZ law and SAP data policy and internal

agreements – under existing contracts. You will also be responsible for working with the DPO and global Field Legal Operations in terms of regional amendments to SAP's global Data Processing Agreement.

SKILLS AND COMPETENCIES

Required skills

- Legal Practitioner admitted to practice in at least one Australian jurisdiction with superior academic credentials, or superior experience in data privacy practices
- ANZ, EU and US personal data law knowledge and experience
- Fluent in English
- Strong written and verbal communication and presentation skills
- Assertive and convincing personality, high level of commitment and flexibility.
- Excellent team-working skills;
- Ability to work in an international environment
- Ability to maintain both privilege and confidentiality

Preferred skills

- Prior experience as a Chief Privacy officer or as principal legal advisor to a Chief Privacy officer;
- Prior experience supporting Software sales, in particular Cloud based software (SaaS)
- Prior experience with the Office of the Australian Information Commissioner
- Prior experience with the Privacy Act Codes

WORK EXPERIENCE

Experience as a legal practitioner with working experience in a law firm or a large corporate specialising in data protection and privacy law, in the legal department and/or the data protection office of an IT company, or equivalent.

SAP'S DIVERSITY COMMITMENT

To harness the power of innovation, SAP invests in the development of its diverse employees. We aspire to leverage the qualities and appreciate the unique competencies that each person brings to the company.

SAP is committed to the principles of Equal Employment Opportunity and to providing reasonable accommodations to applicants with physical and/or mental disabilities. If you are interested in applying for employment with SAP and are in need of accommodation or special assistance to navigate our website or to complete your application, please send an e-mail with your request to Recruiting Operations team (Americas:Careers.NorthAmerica@sap.com or Careers.LatinAmerica@sap.com, APJ: Careers.APJ@sap.com, EMEA: careers@sap.com). Requests for reasonable accommodation will be considered on a case-by-case basis.

Additional Locations: No Selection

Job Segment: ERP, Sales Operations, Software Sales, SAP, Compliance, Technology, Sales, Legal

Apply: Please email updated resume to vineeta.srivastav@sap.com

Closing Date: August 15th 2016

Privacy Commissioner
Te Mana Matapono Matatapu

Office of the Privacy Commissioner, New Zealand

We are looking for an experienced Team Manager to join our Auckland office who can successfully mentor and lead a team in investigating and resolving complaints received about alleged breaches of privacy. We use alternative dispute resolution (ADR) to facilitate settlement between the parties wherever possible.

For details click here:

Team Manager, Investigations and Dispute Resolution (Auckland)
Applications close 25 July 2016

Our contact details

Privacy Unbound is the journal of the International Association of Privacy Professionals, Australia-New Zealand (iappANZ), PO Box 193, Surrey Hills, Victoria 3127, Australia (http://www.iappanz.org/)

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

Veronica Scott (**veronica.scott@minterellison.com**)
Carolyn Lidgerwood (**carolyn.lidgerwood@riotinto.com**)
David Templeton (**David.Templeton@cjsh.com.au**)

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