# Contents

<table>
<thead>
<tr>
<th></th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>VICE-PRESIDENT’S FOREWORD</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Veronica Scott</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>PART 2 OF THE IAPP WASHINGTON DC SUMMIT REPORT</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Christopher Rogers and Susan Bennett</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>NZ OFFICE OF THE PRIVACY COMMISSIONER’S FORUM 2018</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>Fiona Colman</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>PRIVACY UNPLUGGED WITH PRIVACY COMMISSIONER JOHN EDWARDS</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>Katherine Gibson</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>NZ OFFICE OF THE PRIVACY COMMISSIONER’S PRIVACY TRUST MARK LAUNCH</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>Annabel Fordham</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>PRIVACY: FROM PRINCIPLES TO PRACTICE – HOW TO ACHIEVE GOLD STANDARD</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>LOOKING BACK AT IAPPANZ’S PAW PANEL EVENTS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Georgia Milne &amp; Lyn Nicholson</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>KIWI BUSINESS STORING DATA IN AN AUSTRALIAN “CLOUD”?</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>AUSTRALIAN PRIVACY LAWS MAY APPLY!</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Frith Tweedie</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>FIRST EVER PRIVACY AFTER HOURS EVENT IN PERTH</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>Nina Yiannopoulos</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>MEET YOUR IAPPANZ BOARD</td>
<td>24</td>
</tr>
<tr>
<td>10</td>
<td>UPCOMING EVENTS</td>
<td>25</td>
</tr>
</tbody>
</table>
Author Guidelines - subject to the discretion of the editor

Criteria for articles

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

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

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

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

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

Copyright and Licence

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

2. No fees are payable by iappANZ.

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

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

Acknowledgement

1. iappANZ will use all reasonable endeavours to ensure that the author’s name is published with the article.
Welcome to our Autumn edition of Privacy UnBound.

What a month it has been! We have had Privacy Awareness Weeks in New Zealand and Australia, with a series of successful events organized by our Events Sub-Committees, including Privacy: From principles to practice – how to achieve the gold standard’ which are reviewed by Georgie Milne and Lyn Nicholson. We also had our first ever PAH in WA earlier in April which was hosted by Deloitte. Nina Yiannopoulos was there and is looking forward to more of them.

GDPR has finally commenced 😊. Our inboxes have been jammed with organisations telling us about their new privacy policies (even if we have never heard of them...) and many of us are feeling just a bit wearier for it all. But this really does feel like a new phase in the maturing global privacy and data protection framework and time will tell how the impact of GDPR will be felt in practice across ANZ. If you want to get a ringside seat to what will be happening in the EU, just read Chris Rogers’ report on the comments made by Helen Dixon, Data Protection Commissioner for Ireland at a recent event in Washington during the IAPP Global Summit. It’s the Summit that keeps on giving, with more on blockchain and its impact on privacy and identity as well as the growing tension between data localization laws and regulations and the top 10 Fails during data breach responses all from Susan Bennett.

Fiona Colman reports on the NZ OPC 2018 Forum with presentations on a range of topics including the new Privacy Bill, the impact of automating algorithms decision making and the effects of GDPR. The Forum also launched the OPC Privacy Trust Mark, with the first two recipients recognised, agencies RealMe and TradeMe. Annabel Fordham provides us with more detail on the Trust Mark.

Katherine Gibson was at the lunchtime discussion with John Edwards, New Zealand’s Privacy Commissioner, to hear his views on the Privacy Bill and the protection of privacy in New Zealand as well insights into what has been called his Grand Facebook Gesture! Also a chance to meet one of our newer Board members Marina Yastreboff who has a wealth of experience to give us some insights on the technology/privacy interface, Finally, what about storing New Zealand data in the cloud in Australia – what laws apply? Frith Tweedie explains.
Christopher Rogers shares his insights on his experience as set out below.

Data protection regulators from around the world were in Washington DC in late March to attend the IAPP Global Privacy Summit. I was fortunate to be invited by Sidley Austin to attend a focus roundtable just prior to the Summit, where panellists engaged on the intricacies of EU data protection law. The guest panellists on the roundtable included Helen Dixon, the Data Protection Commissioner for Ireland. I found her observations and remarks to be both interesting and informative from a GDPR-readiness perspective.

**Harmonisation issues:**

At the time of the Summit, we were within the final remaining weeks before the implementation of the GDPR. With a tight turnaround time since the GDPR came into force in May 2016, Dixon said that not all EU Member States have their local laws in place to give effect to the GDPR. According to Dixon, the downside of this is that not every aspect of EU data protection law will be harmonised under the GDPR, particularly in areas such as the age of consent for children and the processing of criminal conviction data.

**Dispelling the myths:**

Dixon has been hearing analogies between “25 May 2018” and “Y2K” and believes that these analogies are “dangerous” and a “bad idea”. In her view, the GDPR is not some form of millennium bug which can be patched once and then forgotten about. Nor does she agree with suggestions that the GDPR is “massively overhyped” and that after 25 May, nothing will happen to companies that haven’t embraced it. Dixon said this is what we will see more of in the post-GDPR environment whenever we deal with organisations: concise and clearer information provided to us about an organisation’s data collection and use.

**Transitioning of enforcement to the GDPR:**

From an enforcement perspective, Dixon confirmed that there will be no further transition period for the GDPR after 25 May 2018. She said though, that there may be a time lag before enforcement of the GDPR commences. For example, Section 8 of the new Irish Data Protection Bill confirms that the existing Irish data protection legislation, based on Directive 95/46/EC, will continue to apply to any existing complaints from individuals that the Irish DPA is handling and any investigations that are already underway. Dixon said it would take a little bit of time for new issues that occur post-GDPR to cycle through; however she believes this will happen soon enough.

**Differences between Directive 95/46/EC and the GDPR:**

How does the GDPR differ from its predecessor, Directive 95/46/EC? Dixon said that not only is the GDPR a “harmonised” and “modernised” law, it has also incorporated the case law from the Court of Justice of the European Union, with its recently issued seminal data protection judgments. The GDPR has built in tests around necessity and proportionality which Dixon believes are the essence of the fundamental right to data protection.

From an organisational compliance perspective, Dixon noted that the GDPR adopts a risk based approach, which she said makes it useful and proportionate in terms of scalability for different types and sizes of organisation. It

What will data privacy in Europe look like post 25 May?

Dixon expects to see clear differences immediately post-GDPR as compared to pre-GDPR, which she said are becoming apparent already. Post-GDPR, there will be implications for individuals, even from the perspective of the “man on the street”. For everyday activities such as getting your car repaired at the local garage, individuals will receive a detailed privacy notice informing them why their personal information is being collected and how it is being used. Dixon believes this is what we will see more of in the post-GDPR environment whenever we deal with organisations: concise and clearer information provided to us about an organisation’s data collection and use.
also reinforces in her view, that in the specific circumstances of any data processing scenarios, the organisation itself must conduct the risk analysis and implement technical and organisational measures which are appropriate to the identified risks.

Dixon observed that the GDPR has retained all of the familiar basic principles of data protection law seen in Directive 95/46/EC, starting with lawfulness and fairness. In addition, she noted the introduction in Article 5 of two new principles of general applicability, the first being security and integrity of data and the second being a new broad based principle of accountability, which Dixon considers to be the bedrock of the GDPR. In terms of the new principle of accountability, Dixon said she has already seen organisations coming to grips very successfully with the different enumerated requirements, including the appointment of Data Protection Officers and the carrying out of Data Protection Impact Assessments (DPIAs).

**New requirements under the GDPR for organisations:**

With respect to Record of Processing Activities (ROPA) requirements under Article 30 of the GDPR, Dixon said she has been surprised by the debate and controversy this has caused within various organisations. Legal practitioners allege, she said, that the requirement for ROPAs have been “over-egged” by consultants who are selling their solutions for data mapping and data analysis. In Dixon’s view, the requirement under Article 30 to document data processing operations through a ROPA has to be the starting point of compliance with the GDPR. “If you don’t know what data you have and haven’t written it down, you are not tracking it or looking at the legal basis for it. It follows that you can’t effectively conduct the risk assessment you are required to do under Article 24 [and] put in place appropriate organisational and technical measures to protect the data,” Dixon said. In her view, organisations don’t need to use an automated tool to carry out the ROPA, it can be done with a manual spread-sheet, but in any event it is still a critically important requirement.

The implementation by organisations of systems which will deliver on data subjects’ rights under the GDPR (including the new right to data portability) are also critically important in Dixon’s view. This is because the timeframe for organisations to respond to Subject Access Requests will reduce under the GDPR and no fees will be required to be paid. Dixon said she anticipates a big increase in data subjects’ access rights being exercised across the board. She has observed organisations which expect a significant volume of these types of rights, building systems and tools to deliver on this. While there is no set way to carry this out, Dixon said it is important that an organisation can deliver when a data subject seeks to exercise his or her rights, as a failure to do so here attracts the highest degree of fines under the GDPR.

**Areas for improvement by organisations:**

Where are organisations falling behind in their GDPR-readiness activities? Dixon said there are three main areas where she has observed a lack of clear change or visibility as follows:

1. **Transparency.** Dixon said that for data protection regulators, transparency has to be key and this is their number one regulatory and enforcement priority. Vague privacy policies that don’t communicate concise and intelligible information to data subjects are in her view just not good enough anymore and are not what the GDPR is calling out for. In this regard, Dixon reiterated the guidance of the Article 29 Working Party, which provides that privacy notices shouldn’t use qualifiers such as “may”, “might” and “it’s possible”, nor should they use very generic descriptions of processing such as “we may use your data to develop new services”.

2. **Legal Basis for Processing.** Dixon said that even at this late stage, data protection regulators are seeing a lot of confusion on the part of companies and processing entities about the legal basis they are relying upon to legitimise their data processing activities. “Some organisations are seeking to move [away from consent] to processing based on necessity for the performance of a contract, when it is not clear that all of the processing will be strictly necessary for the performance of a contract.” Dixon said. With the continued uncertainty around legal basis, Dixon confirmed that her office is available to discuss and provide guidance if needed.

3. **Children.** With Recital 38 of the GDPR specifically demanding higher standards of protection for children, Dixon said that data protection regulators have not seen companies that target services at children taking account of the Article 29 Working Party, which provides that privacy notices shouldn’t use qualifiers such as “may”, “might” and “it’s possible”, nor should they use very generic descriptions of processing such as “we may use your data to develop new services”. Dixon said that her own personal bias is always in favour of very clear and narrative words and language to convey messages transparently.

**Conclusion:**

In her concluding remarks, Dixon said that the Irish Data Protection Authority has been gearing up over the past three years to prepare for its role under the GDPR. “The Irish authority now has over 100 staff and we are recruiting another 40 or 50 this year...we are now in the top tier of highly resourced national data protection authorities in the EU,” she said. Dixon confirmed she will be using the expanded toolkit which the GDPR provides to regulators, including the introduction of punitive fines. She said that it
would be necessary to deploy those fines in order to ensure there are no repeats of cases of large scale infringements of fundamental rights. Noting that the GDPR is about better outcomes and everyone “being in it together,” Dixon confirmed that the Irish Data Protection Office is available to be consulted with and will guide organisations wherever it possibly can.

Disclaimer: The views expressed in this article are the views of the author, not EY. This article provides general information, does not constitute advice and should not be relied on as such. Professional advice should be sought prior to any action being taken in reliance on any of the information. Liability limited by a scheme approved under Professional Standards Legislation.

In summary, preparation is key to responding to data breach events. Organisations need to be responsive – the challenge is striking the balance ensuring what is said is responsive and accurate and that it doesn’t make the situation more damaging to your organisation and for customers.

How Blockchain Will Transform Privacy and Identity

This session was presented by Stuart Levi of Skadden and Allison Clift-Jennings of Filament. A quote from Roy Amara, Stanford Research Institute set the scene:

“We tend to over-estimate the impact of major technological breakthroughs in the short run and underestimate the impact in the long run.”

During 2017, blockchain was adopted at a breakneck speed across numerous industries ranging from financial services to logistics management. In this presentation, the speakers explained blockchain and the significant impact that the technology is expected to have on privacy and identity.

Blockchain technology uses a distributed ledger system instead of physical currency in the traditional marketplace exchange or a trusted third-party solution. The problems with the trusted third-party solution include: security, as it is reliant on one third-party; you are charged a fee for the transaction; and in cross-border transactions there can be hours and days of delay to finalise transactions.

The distributed ledger system enables everyone to have a copy of the ledger and in real-time they can see it without the involvement of a trusted third-party. The key
challenge is how to verify each transaction and ensure that each block in the chain is legitimate and, in an environment where everyone can fully trust each other. This can be done by using Private Key/Public Key cryptography. This enables you to authenticate the identity of someone as things are added to the network. The Public Key allows one to verify that the holder of the paired Private Key sent the message. Only the paired Private Key holder can decrypt the message encrypted with the Public Key.

In order to enable a new block to be added to the chain a message is sent to all the nodes on the network (the ‘miners’, which are the computers on the network that work on a complex mathematical problem). Once 51% of the nodes on the network confirm that it is a valid transaction, the new block is added to the chain and the all the ledgers are updated. This is referred to as ‘Proof of Work and the Consensus Algorithm’. Once the transaction is validated, the miner is financially rewarded and the process begins again.

Blockchain is secure and immutable because each block is transformed into a unique 64 character comprising random letter and numbers, which cannot be reverse engineered. Even a small change to a block dramatically changes its hash. The algorithm to add a new block incorporates the hash from the prior block. For example, if you go back and try to change a transaction from 4 blocks ago, you will change its hash. This means that every block after that will show an error.

### Issue of Identity

The issue of ‘identity’ may include the sovereignty of the individual, the sovereignty of the machine operating on behalf of the individual, authentication of the other party to the transaction and whether they have the ability to do certain things – referred to as authorisation. These concepts are important because if you want to store identity in a blockchain you need to consider what you want to include. This enables you to put what identity or parts of identity that you want to use in the payload - e.g. real name, pseudonym, social security number. You can include it in a blockchain and it can be private, but still verifiable. Cryptography enables you to verify without revealing your identity. This is where the concept of digital sovereignty becomes important. Many start-ups try to enable verified digital identity in a blockchain. Digital identity can be used where people may not otherwise have an identity, for example, in a developing country or war-torn country where individuals do not have official identification documentations.

Presently we use numbers as unique identifiers for humans – e.g. passport, driver’s license, social security. However, when you bring in cryptography, such as the Public and Private Keys, you don’t need to trust numbers anymore as you have an enhanced version of your number. This is because you have in the Public and Private Keys the mechanics of the maths to prove who you are and that you will do what you say you will do. A good analogy is an email anyone can send to you, but only you can read. A Public Key allows anyone to send you anything encrypted and only you can decrypt it with your Private Key.

The right question is how do we rethink identity in a concept of mathematically secure verification and the speed of computers?

Currently there is not very much privacy on a blockchain, because the first generation of blockchains require you to see the entire ledger history to verify that none of the hashes have been changed. The transactions will always be public in the first generation blockchains, such as, bitcoin.

Some of the new and emerging technologies that enhance personal privacy are:

- **Zero Knowledge Proofs** – this allows one party to reveal to the other party enough about a transaction but not the whole transaction to enable the other party to verify the transaction, such as Zcash (which is similar to bitcoin, but is anonymous). It is likely this will be the way forward where you no longer see public viewable transactions on blockchain as you do on first generation blockchains.

- **Next generation consensus algorithms and Machine-anonymity** – this is about enabling machines to transact with each other. Machines which can add to or change the ledger can remove friction from enterprise. Machines have the same issues around identity and privacy as people do. This is because they operate on behalf of their owners and machines will need anonymity and privacy in the same way as humans. A group of 100 machines can through cryptography share the same Public Key and any Private Key can identify it. There is considerable research and technology development in this area, such as Intel’s EPID (Enhanced Privacy Identification).

### If a blockchain is immutable, what does that mean for GDPR compliance?

Early blockchain technology is very much like dial-up era of the internet and is not very compatible with GDPR. While the right to be forgotten won’t be able to be implemented on the first generation blockchain it will be able to be implemented on the next generation of blockchain. One practical way is to include an expiration date on the transaction, such as, a statute of limitation period.
In summary, developments in blockchain technology will enable people to control their own data, determine who gets to use that data, how much of it and for what purpose. This paradigm shift in personal privacy, data monetization, trans-border data flow, and government access to personal information will significantly influence the future of transactions, many of which are already being fully and securely verified without knowing the identity of the user.

Conflicts between US Legal Demands for data and global data protection laws

This session highlighted the growing complexity for organisations operating at cross-borders arising from the growth in data localization laws and regulations. The presenters were Walter Delacruz of Deutsche Bank, Brian Hengesbaugh of Baker McKenzie and Hugo Teufel III of Raytheon.

While the session was presented from a US perspective, the issues for companies operating cross-borders are similar for Australian and New Zealand companies. The session explored the differing legal demands for global data and global data protection and other legal restrictions on data transfer and disclosure. The different types of legal demands and the types of data restrictions that need to be taken into account are set out below.

1. Cross-Border internal investigation

Legal demands include anti-bribery, financial fraud, Code of Conduct Violation, and other compliance issues.

Key Data laws include Data protection, telecoms privacy, labour laws, anti-investigatory/blocking statutes (maybe), and professional secrecy.

Elements to address include privacy solutions, key facts (location of data, controller, restrictions), collection and production protocols, negotiation with authorities and protective orders.

Indicators of data law risk include aggressive data protection officers of works councils, high profile company, media attention, actual wrong doing and disputes.

2. Cross-Border penetration testing and security monitoring

Legal Demands include security requirements due to industry-specific regulation, public company requirements, data protection laws and contractual duties.

3. Cross-Border third-party due diligence and background screening

Legal Demands include third party due diligence and background screening as needed to address EIM/ITA, OFAC, AML, or other requirements.

Key Data laws include Data protection, labour laws, blocking statutes.

Elements to address include privacy solutions, protocols on data collection and use, local segmentation.

Indicators of data law risk include aggressive data protection officers or works councils, use of data for discipline, high profile company and media attention.

4. Cross-Border Regulatory demands

Legal Demands include industry specific regulatory requirements due to oversight or investigatory powers (typically home office, but can be local).

Key Data laws include Data protection, telecoms privacy, labour laws, anti-investigatory/blocking statutes, professional secrecy.

Elements to address include privacy solutions, key facts (location of data, controller, restrictions), protocols on data collection and production, negotiation with authorities and protective orders.

Indicators of data law risk include aggressive data protection officers or works councils, use of data for discipline, high profile company, actual disqualification of third parties.

5. Cross-Border National Security or Law Enforcement demands

Legal Demands include law enforcement or national security demands.

Key Data laws include Data protection, telecoms privacy, anti-investigatory/blocking statutes, labour laws, professional secrecy and data localisation.
Elements to address include privacy solutions, key facts (location of data, controller, restrictions), protocols on data collection and production, negotiation with authorities and protective orders and litigation/defence.

**Indicators of data law risk** include third-party data, high profile company, media attention, frequency and expansiveness of demands.

In summary this session highlighted:

a. Companies are being caught between various regulations, data localization laws, and law enforcement.

b. Data laws are proliferating.

c. Legal Demands for global data are increasing.

d. The digital age is accelerating cross-border integration.

e. Addressing conflicts required multi-layer approach that:
   - Reduces data law risk,
   - Manages legal demands, and
   - Importantly, handles remaining conflicts in a consistent manner.

Susan Bennett is the Principal of Sibenco Legal & Advisory, Co-Founder Information Governance ANZ. Susan is a Fellow of the Governance Institute of Australia (FGIA), a member of the International Association of Privacy Professionals (iappANZ), a member of the Asian Privacy Scholars Network (APSN), a member and graduate of the Australian Institute of Company Directors (AICD).
**Opening Address - Hon Andrew Little, Minister of Justice**

The Minister talked about the Privacy Bill, how it was still flexible and principles-based, and that the reforms were fit for purpose. New provisions such as mandatory breach notifications will align us better internationally; compliance notices will allow the Privacy Commissioner to better respond to non-compliance, and access directions can be made by the Privacy Commissioner, instead of by the Human Rights Review Tribunal (HRRT).

Under GDPR, New Zealand’s adequacy status is not immediately affected, but the Privacy Bill will better align us with GDPR.

The Minister closed with a comment that the Privacy Forum was the opportunity to thrash out the issues and Officials in the audience were there to hear them. He noted that submissions on the Bill close on 24 May.

**Keynote address - John Edwards, Privacy Commissioner**

The Commissioner started his presentation with a demonstration of Shazam, the music identification app, and relayed a story of mistaken musical identity in the case of iTunes mislabelling a song in his collection as ‘A’. This meant that it automatically plays first in his car, much to his family’s annoyance.

This linked to a theme of his presentation about automating algorithms and using technology to solve social problems. Risks of algorithms include selection bias, and inaccuracy. There was evidence of misidentification of gender in algorithms, and that assumptions can have significant impacts.

With predictive risk modelling there is often a lack of explanation or reluctance to reveal the methodology. Two new GDPR articles address automated decision making and artificial intelligence, and give individuals the right to human intervention in cases of adverse decisions. These protections are significant in the context of international benchmark setting and the Commissioner will draw attention to them in making submissions on the Privacy Bill. Quotes from Cathy O’Neil’s book *Weapons of

**Math Destruction** appeared for the first of several times during the day, to illustrate the issues related to big data use.

The Commissioner closed his remarks with a plea for participants to make submissions to the Select Committee on the Privacy Bill.

The full transcript from The Commissioner’s speech can be found here: [https://privacy.org.nz/assets/Uploads/Privacy-Commissioner-Privacy-Forum-keynote-speech.pdf](https://privacy.org.nz/assets/Uploads/Privacy-Commissioner-Privacy-Forum-keynote-speech.pdf)

**Panel on little data: How algorithms affect our daily lives**

This was a panel discussion on how algorithms - predictive risk modelling (automated decision making and machine learning) affect our daily lives, with John Edwards (Chair), Associate Professor Gavaghan (Otago University) and Nic Blakeley (Ministry of Social Development).

Associate Professor Gavaghan began with an overview of algorithms. The positives are that they can be accurate, efficient when processing large amounts of information, and remove human bias. The downsides are the erosion of discretion and transparency, and the replication/reinforcement of bias. We should not automatically feel confident in human intervention as this could give false reassurance, and unconscious bias.
Nic Blakely talked about how decision making had existed for a long time at MSD, but decisions were traditionally made by humans. At MSD, predictive modelling could help determine who was most likely in need, what help could be provided, and how could this be done responsibly. Work is underway at MSD to be more transparent about the algorithms used and how they were applied.

The panel discussed the role of law versus ethics, the possibility of an independent body to overview artificial intelligence and provide guidance, and how we prepare for machines refining their techniques beyond recognition of the original programming. Modern algorithms are only as accurate as the data you put into them and should ideally be used only to augment decision-making. Artificial Intelligence has been known to have a demoralising effect on decision-makers, such as Police, who feel that their discretion and local knowledge is being eroded.

Panel on GDPR implications

Rick Shera (Lowndes Jordan) chaired a panel with Jacqueline Peace (Air New Zealand), Ken Wallace (Ernst Young) and Professor Paul Roth (Otago University) discussing the implications for New Zealand when GDPR commences on 25 May.

From an operational perspective, Jacqueline Peace from Air NZ talked about how GDPR is about just doing privacy right. GDPR is about best practice and Air NZ will be trying to apply the GDPR principles across the board regardless of residence status.

Professor Roth talked about the process New Zealand went through to get EU adequacy. New Zealand was seen as a pioneering country and some of the concerns the Article 29 Working party had about New Zealand have been addressed by subsequent legislation such as the Harmful Digital Communications Act and possibly in the Privacy Bill.

Ken Wallace from EY said that 25 May is the beginning, not the end. People will try to test GDPR provisions and it will be a wonky ride at first. Many organisations lack the capacity and funding to apply GDPR requirements, so EY is helping clients decide what’s feasible to comply with.

The panel discussed breach identification and raising awareness in the organisation by tailoring education to what’s necessary for each role. The Privacy Bill needs to have explicit requirements for consent like the GDPR does, and organisations that are wilfully non-compliant should be ‘held to account in a way that’s painful’. When it comes to privacy by design, the message is, ‘just because we can doesn’t mean we should’.

Questions ranged from implications for agencies that deal with EU citizens’ data in New Zealand to the practical ways that the EU can enforce rights on New Zealand agencies. It was revealed that only five of 28 EU countries have passed GDPR enabling legislation, implying that New Zealand companies don’t need to rush to make any changes themselves.

The consensus appeared to be that it would be terrible for New Zealand to lose our EU adequacy status. The Privacy Bill will help, and will show that progress is being made. New Zealand has a potential $38 billion in our digital economy. Being non-adherent would make it harder to realise that potential.

Compliance orders – Katrine Evans, Haymans Lawyers

Katrine Evans led a session on the new Bill provisions for the Privacy Commissioner to issue compliance orders on non-compliant agencies. Using dog memes as metaphors to illustrate the transition from a ‘puppy’ to ‘watchdog’, the talk outlined the Commissioner’s current powers and those proposed under the Bill. Marie Shroff, previous Privacy Commissioner, was on hand to note that the Commissioner’s role was once referred to as a ‘toothless tiger’.

The audience discussed whether non-compliance notices should be routine or saved for special cases, the types of breaches worthy of a notice, and mandatory and relevant considerations of the notices. A key point is to not ignore the notice because the powers in the new Bill provide the Commissioner with teeth. There was a strong role for voluntary action; voluntary compliance should result in no notice. The elephant in the room is the Human Rights Review Tribunal and the impact that its delays and backlog could have on the effectiveness of compliance orders.

Panel on Mandatory data breach notification

Susan Bennett (Sibenco/Information Governance ANZ),
Daimhin Warner (Simply Privacy) and Sarah Auva’a (Spark) participated in a panel discussed on mandatory breach notification, chaired by Michele A’Court.

Susan Bennett ran through various international data breach notification laws, outlined the Australian experience in recently implementing a notifiable data breach reporting regime, and talked about recent serious breaches, such as Equifax and Talktalk.

Daimhin Warner discussed the language of breach notification in the Bill and the criteria tied to harm. Tying notification to harm is a difficult test, and remedies taken to address that harm won’t excuse notification.

Sarah Auva’a gave the specific example of Spark’s experience with Yahoo breach. The consequences of a low reporting threshold are that New Zealand may look like it has a lot of notifiable breaches, potentially reducing confidence in New Zealand agencies’ data management practices.

The discussion talked about the necessity for third party contractors to be aware of the requirement to notify breaches. Staff awareness of a breach is also the key to good breach management. A concern was raised about the ability of small agencies and NGOs to resource breach management and implement privacy controls.

**Closure**

The Privacy Forum closed with comments from John Edwards summarising the day. The Privacy Trust Mark was then launched, with the recognition of TradeMe and RealMe as the first recipients.
was the level of concern about the use of drones in urban areas – this is an example of the need for the law and social mores to keep up with the rapid pace of technology. The Commissioner was pleased to see a good level of public awareness of the Privacy Commissioner, his Office and the Privacy Act, and this was generally higher than the awareness of the privacy regulators in other jurisdictions who also undertake a similar survey (being those in the Asia-Pacific Region – APPA Members). He noted however that the Government still has some work to do on maintaining trust – there is a growing level of concern about the Government’s ability to protect our data.

The Privacy Bill as drafted does not give him teeth – but a reasonably serviceable set of dentures.

In case you have not heard it, the background to this is in response to a reporter commenting that the Privacy Commissioner is a “toothless watchdog”, the Commissioner said - I may be toothless but I can exert quite a lot of pressure with my gums. We were told that the Bill as drafted won’t give him any teeth but the enhancements to the enforcement mechanisms in the Bill are “a reasonably serviceable set of dentures”. So there is still a way to go before he is given any “chewing and tearing functions”.

The Bill in its current form is fit for 2013.

The Privacy Bill does not change the fundamentals of the current law. However if the Bill is enacted in its current form, the Commissioner’s view is New Zealand will have a law in 2019 which is fit for 2013. We were asked – “is it good enough to have a law which is already outdated?” - as part of a plea by the Commissioner for everyone to make submissions on the Bill to ensure we do not have an outdated law when it is enacted in 2019. Submissions are due to close on 24 May 2018.

What is missing in the Bill?

A number of reforms. He referred to his Report to the Minister of Justice (under s26 of the Privacy Act, tabled February 2017) which included six recommendations for law reform - a data portability right, controls on
re-identification, new powers to require demonstrations of agency compliance, a new civil penalties regime, new criminal offences and public register reform. None of these reforms have been included. In addition, New Zealand has not even started a conversation on the right to be forgotten – and what about a right to object to automated processing – we need algorithmic transparency.

Why is the EU privacy regime being held up as the best standard?

The Commissioner said he was not holding up GDPR as the best data protection standard or aspiring to this foreign ideal – he is aspiring to a domestic ideal. The EU law and our Privacy Act both have a common provenance – the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. A major difference between the two regimes is the harm based enforcement here in New Zealand. That is not necessarily the case with GDPR – where compliance does not always lead to a positive outcome for individuals.

Personal information warrants the same level of protection as other rights.

In New Zealand, the protection of personal information operates in almost an entirely voluntary regulatory system. The Commissioner compared this to an individual’s rights to: a safe work environment; being remunerated by an employer in cash; and a supplier’s guarantees on consumer goods and services – these rights are all actionable by a regulator. The privacy law needs changing so that personal information has the same level of protection and regulation as those an individual enjoys as an employee or as a consumer of goods and services.

Mandatory breach notification – we are playing catch up.

With this reform we are only now catching up with GDPR, Australia, Japan, Korea – 48 States in the US have mandatory breach notification – New Zealand has fallen way behind in this regard.

To target systemic bad practice – demonstration of agency compliance.

The Commissioner explained the background to his recommendation to give the Privacy Commissioner the power to require an agency to demonstrate compliance with the law. The Law Commission in 2011 (and subsequently supported by the Privacy Commissioner at the time) recommended the Privacy Commissioner be given the power to audit agencies for compliance with the Act. The was met with resistance (“audit” envisages a significant power) and the Commissioner is now not recommending any broad auditing power, but something more targeted - a right to require an agency to show that they are complying.

Further on his 2017 Report recommendations for further law reform.

Introducing a fines regime: The Privacy Commissioner should be on par with a Labour Inspector and the Commerce Commission.

Public register reform: He supports the Government’s push for the sharing of more data sets and that public data should be available for public consumption. But how do you do that safely – we know if you just take out names and addresses this will not anonymise the information.

A new principle prohibiting re-identification of de-identified data sets: When this was suggested in the 2017 report this was quite “radical” but following on from that Australia has introduced federal legislation making re-identification a criminal offence and data protection law in the UK prohibits re-identification of de-identified data sets.

The approach to an enhanced enforcement regime.

The Commissioner indicated that agencies who reach out to his Office for help or notify the OPC that there has been a breach and take guidance are not the ones who are likely to be the subject of any enhanced enforcement regime. It is the ones who shun their responsibilities, who are recalcitrant repetitive agencies who will bear the force of any kind of enhanced enforcement regime – and these are a small proportion of agencies. All agencies won’t be judged by those who are shunning their responsibilities - most agencies want to comply given the right tools.

Proposed data breach notification – does the drafting work?

The Commissioner commented that whilst it is better than the previous draft, the drafting of the Bill is a matter that he is not going to take ownership of - that is for industry, academia and others to tell Parliament what will work and what won’t work. However, he noted that anticipating harm that might occur in the future is a much more complicated matter than assessing harm when it has already occurred (which is something the OPC does now and has experience in when assessing harm from a breach of the current IPPs).

Increased powers – the onus is now on the agency to challenge.

If the Bill is passed in its current form, the Commissioner will have the power to issue compliance notices (requiring
an agency to comply with the Privacy Act) and access determinations (requiring an agency to give access to an individual). With these new powers, the onus on challenging these matters has now switched. It is not up to the Privacy Commissioner or the individual to have to do the enforcement - if an agency wishes to challenge a compliance notice or an access determination they will have to take positive steps to do so through the Human Rights Review Tribunal.

**Will the new powers change the way the Office of the Privacy Commissioner works?**

The Commissioner confirmed that there is likely to be more litigation and so there will need to be a sharper distinction in his Office between the disputes resolution function and the enforcement function. He went on to explain – you cannot ask someone to come to the mediation table to resolve a dispute and make concessions and then if that fails the OPC then uses all that information against the agency at a later date before the Human Rights Review Tribunal. Some thought will need to be given to how the functions are going to be divided up and a recognition of the different hats the OPC has: investigation, resolution or enforcement.

**New Zealand’s EU Adequacy status is not at risk... for now.**

Our adequacy status is not a risk today, and probably not at risk if the Privacy Bill passes in its current form - but we cannot take it for granted. The Commissioner has to report to the European Commission on a six monthly basis on developments in New Zealand that might affect the privacy of Europeans – so for example, reports have been given on the Harmful Digital Communications Act and the Intelligence and Security Act and the Commissioner will need to report on the Privacy Act when it is passed. That may result in some questions that need answering.

**Deleting his Facebook account was not a Grand Gesture.**

This was not so much of a Grand Gesture but it had been bugging him for a while and he could show that it could be done in a leadership sense. He had a Facebook account for 10 years, seeing many changes to terms and conditions over that time - deleting the account was hitting the reset button. He felt that there would be an enormous aggregation of his data over that time and after recent events he did not want to trust the organisation with his data.

**Mydigital life application - the internationalisation of the digital economy.**

The Commissioner left the audience in no doubt that he considered this was an example of misrepresenting the use of data and purpose of collection and that we should not believe that this was the only instance of misrepresentation of use of data through that platform. This was an example that highlighted the internationalisation of the digital economy and the need to have a regulatory regime which recognises that.

**Enforcing Privacy Act – Facebook.**

The recent Facebook example shows the difficulties regulators have – enforcing the Privacy Act against an organisation that holds data on 2.5 million New Zealanders and advertises to local businesses. New Zealand needs to have an enforcement regime commensurate to some of our comparative jurisdictions so New Zealanders are not treated as marginal backwater to a business with over 2.2 billion users.
It can be hard to know who to trust with your data these days. At the Office of the Privacy Commissioner we repeated our regular public opinion survey a few months ago. The results showed that more than half (55 percent) of all New Zealanders are more concerned with their individual privacy now than they were in the last few years.

The number of people concerned about their individual privacy has risen slightly to 67 percent, up two percent from the last survey held in 2016.

Some sectors of the community indicate a greater level of concern; those with a household income of $50,000 or less were more likely to be concerned about individual privacy (77 percent) compared to those with a higher household income (63 percent).

Sixty-two percent of New Zealanders said they trust government organisations with their personal information – this is a drop of nine percent from when this was last measured in 2014. Trust in companies was significantly lower this year at 32 percent.

Results showed that we are likely to feel more vulnerable about sharing our personal information in certain circumstances, such as over social media. Thirty percent of people said they were comfortable sharing information on social media, compared to 65 percent who were uncomfortable. Only 18 percent were confident that their information would be looked after, while 75 percent had little or no confidence at all.

Recognising excellence and building trust

Our Privacy Trust Mark was launched during Privacy Week 2018 at the Privacy Forum at Te Papa Tongarewa, Wellington. At that event, we also announced the first two trust mark recipients.

We hope the trust mark will become an incentive for organisations and businesses to start thinking proactively about their customers’ privacy. Building privacy protection into products and services demonstrates best practice and can be industry-leading.

Organisations can apply to have the trust mark on their privacy-friendly product or service.

The awards recognise excellence in privacy-friendly products or services. The Privacy Trust Mark demonstrates that a “privacy by design” approach was used and it is intended to give consumers confidence in particular products or services.

We hope that a readily-recognisable trust mark will help New Zealanders make quick, informed decisions about who they can trust with their personal information and will give them assurance that a product or service has been designed with their privacy interests in mind.

First recipients

The first product and service to be awarded a Privacy Trust Mark are Trade Me’s ‘Transparency Reporting’ and the Department of Internal Affairs’ RealMe identity verification service.

Trade Me

“Trade Me is one of the few New Zealand agencies who participates in transparency reporting, above and beyond what is required of it by law. We were impressed with the way Trade Me draws wider privacy issues into its transparency reports as a way of keeping the public informed of topical issues,” Privacy Commissioner John Edwards said in awarding the Trust Mark.

RealMe

The Department of Internal Affairs’ RealMe service was also assessed as meeting the Trust Mark criteria. RealMe’s data minimisation and user control practices were assessed as being excellent. Users can control when and where their identity information is shared and can review all of their transactions and revoke their consent at their discretion.

---

1 UMR Research, Privacy concerns and sharing data, telephone online omnibus quantitative survey March / April 2018.
RealMe only collects and stores information that is required to administer the core service.

Our Office sees this project as part of our vision to help consumers to have trust and confidence that their information will be safeguarded.

If you are part of a New Zealand-based organisation or business that has a product or service that demonstrates excellence in privacy and deserves to be awarded with a Privacy Trust Mark, please contact the Office of the Privacy Commissioner: https://www.privacy.org.nz/privacy-for-agencies/applying-for-a-privacy-trust-mark/

There's more information in our Privacy Trust Mark FAQs.

The Privacy Trust Mark logo was created by a Christchurch graphic designer, Curtis Bain. Mr Bain’s design was the winner of the Office of the Privacy Commissioner’s Privacy Trust Mark Design Competition held earlier this year.

Annabel Fordham is a lawyer and Public Affairs Manager at the Office of the Privacy Commissioner New Zealand and oversees the development of the Office’s public affairs, communications, outreach, media and education functions.
Introduction

In case you missed it, Australia’s Privacy Awareness Week kicked off on 13 May 2018, continuing through until 19 May 2018 with this year’s theme honing in on privacy in the everyday, encouraging business to make privacy a part of everyday practice. In recognition of this important initiative, iappANZ ran a series of well-attended panel events, from Brisbane to Adelaide, with privacy professionals gathering to discuss ‘Privacy: From principles to practice – how to achieve the gold standard’.

Holding Redlich was pleased to be able to host events in Sydney, Melbourne and Brisbane. As each event had a separate panel, the content of the events varied significantly subject to the panel and the audience. Provided below is a summary of the event in Sydney (noting Chatham House rules applied) and a summary from our Brisbane colleagues. Herbert Geer also hosted an event in Adelaide.

At the Brisbane PAW function, the panellists considered the “gold standard” for privacy obligations was compliance - one of the most significant steps an organisation can take to achieve this “gold standard” is to establish the right “culture”. Also, whilst public documents (such as privacy policies and collection notices) were noted as important, panellists stressed that entities should focus on staff training to ensure staff have regard to privacy issues and compliance matters.

Feedback from the Melbourne event noted the panel was great, with an excellent combination of people with lots of insights and stories. There was a good sized audience including some new faces and questions from the floor. A great space and a well-run function, with terrific moderation from Dan Pearce.

Review of the Sydney Event

Those of us who attended the Sydney session were treated to a lively and engaging debate with a preeminent panel, made up of regular iappANZ contributor and international privacy expert Sheila Fitzpatrick (Fitzpatrick & Associates), Olga Ganopolsky (General Counsel, Privacy & Data, Macquarie Group Limited), and Alec Christie (Partner, Digital Law, Ernst & Young), expertly moderated by ex-Gilbert & Tobin partner Peter Leonard (Principal, Data Synergies).

The evening featured a wide-ranging and multifaceted discussion but one through which the GDPR current ran strong, with the 25 May 2018 commencement looming.

It was interesting in a range of ways to observe that while the introduction of Mandatory Data Breach in Australia in February, with a $2.1 million fine, did not seem to engage businesses, the advent of GDPR and the receipt by many businesses of data transfer and other agreements seeking to bind them to the GDPR, had really captured the attention of many businesses.
It would seem that having to sign an agreement with a European counterparty that predicated your continuing business relationship on compliance with the GDPR, has focused the attention of many Australian businesses far more than local law. This is also significant when businesses consider the potential fines under the GDPR and the fact that the local regulator is perhaps not well funded as compared to other regulators and, in the period since 2014 when it has been empowered to impose significant fines, it has rarely done so.

For those who missed it, there were a number of key takeaways from the Sydney panel on how and why business should strive for the gold standard, including:

- An emphasis on organisational design and culture;
- Distinguishing between privacy and technology;
- The value of transparency and consumer engagement.

Organisational design and culture

The notion of organisational design and the need to align your business structure with its strategic goals was raised early, as a key step to implementing effective privacy practices. The panel emphasised that privacy cannot be considered a sub-portfolio that sits within security, technology or customer management, a point reflected in the new GDPR requirements. Privacy is a cross-sectional practice that will affect most business units within an organisation, and this needs to be recognised and reflected in an organisation’s structure, ensuring that privacy operates as an independent business unit with direct lines of reporting to the c-suite and beyond.

The need for c-suite support was also raised and, while the panel expressed confidence that executive management is demonstrating increasing engagement with privacy, they reiterated that middle management is often the best place to foster organisational engagement and build a pro-privacy culture within your business.

Technology vs privacy

The conflation of technology and security with privacy was raised by both the audience and panel alike as a consistent roadblock to achieving effective privacy practices within organisations. As panel member Sheila Fitzpatrick observed, there is simply no point securing personal information if you are not entitled to collect it in the first instance. Rapid developments in technology are driving changes in privacy law and mean that neither business nor regulators can afford to be complacent, if privacy laws are to keep pace with technological advancements. For businesses striving to achieve privacy best practice, they need to recognise that privacy and security are distinct concepts and that the ability to collect and hold information is a pre-condition to keeping it secure.

Organisations need to assess the privacy practices first, with privacy impact assessments remaining a useful tool in this exercise.

Transparency and consumer engagement

One fundamental question put to the panel was that, given the reportedly low rates of privacy policy readership, what’s the value in a transparent policy? The response here was that building consumer engagement is a gradual process, and requires a cultural shift as well as a legal one. It was suggested that consumers will eventually come to regard privacy as akin to a human right, and that successful organisations will be the ones who anticipated this change in sentiment and adjusted their practices accordingly.

As a final takeaway, the panel reiterated that while privacy compliance could be negatively considered a burden, rather it could be positioned positively as a competitive advantage. They cautioned against an overemphasis on enforcement penalties and administrative burdens, in favour of a positive approach that encourages organisations to take a proactive approach to engage and empower their staff, respects the rights of users and builds compliance into their everyday practices. Businesses that strive to achieve this gold standard will be well placed to pitch their privacy credentials to a consumer market that is becoming increasing privacy-savvy.
Regulated Industries

The fact that Privacy Awareness Week coincided with a number of findings of the Royal Commission into banking led to a range of discussions about how organisations actually work and what the risk of reputational damage can look like.

It also raised the issue as to whether the organisations merely talk the talk or actually walk the walk and whether it is possible to have viable business models where there is disregard for consumer privacy. While it is early days in terms of Mandatory Data Breach, GDPR and the Productivity Commissioner’s proposal for Consumer Data, it is clearly leading into an era of much more transparency and failure to be transparent, leading to reputational risk.

That then led naturally to a discussion of recent scandals and their effect.

Facebook – Can we talk about privacy without mentioning Facebook?

The Facebook/Cambridge Analytica issue came to the floor a number of times as an example of an organisation that is in many ways reactive to consumer privacy, when it could deal with it in a very different context. It certainly sets up the position that there is a competitive advantage to be gained from being clear and transparent and also from having different business models. This was one of the issues raised – that a number of business models which are dismissive and disregard consumer privacy are likely to disappear over the next period of time, particularly as GDPR requires far more specific consents and opt ins than generic bundle consents on which many organisations have previously sought to rely.

Privacy by design

One of the key factors of the GDPR was noted as being the requirement that privacy by default and privacy by design be built into systems to collect and retain personal information. This should encourage a change in the way organisations deal with personal information, but we are yet to see how that will unfold.

The discussion lasted well beyond the allocated hour and when a question was raised as to the application of new technologies, such as facial recognition and smart cities, the audience decided it was time to adjourn for networking.

iappANZ is proud to deliver these member based events to allow members to share experiences, learn and network. Holding Redlich was delighted to be able to host three of these. iappANZ looks forward to continuing to provide these services to members in 2018.
As cloud storage becomes increasingly mainstream, New Zealand businesses are taking advantage of the proximity and lower latency of Australian data centres. Banks and government agencies in particular tend to take comfort from the perception that regulatory similarities make Australia a less risky prospect when it comes to offshoring personal information. However, it’s not widely recognised that Kiwi organisations storing personal information in an Australian-based cloud could find themselves subject to Australian privacy law. That includes the Notifiable Data Breaches (NDB) Scheme that came into effect earlier this year, introducing fines of up to A$2.1 million plus potential damages for failure to notify an “eligible data breach”.

Australian privacy law applies to any New Zealand organisation with an “Australian link” that collects or stores personal information in Australia, including in an Australian data centre/“cloud”.

- An “Australian link” is established by factors such as incorporation in Australia, being part of a partnership formed in Australia, or where the organisation “carries on business” in Australia and collects or holds personal information in Australia.

- “Carrying on business” from a privacy law perspective involves conducting some form of commercial activity in Australia. That could include a New Zealand-based organisation with staff in Australia, advertising in Australia, having a website that offers goods or services to Australians, the inclusion of Australia in website drop-down menus, regularly acting on Australian business or purchase orders or being the registered proprietor of Australian trade marks. These factors will need to be assessed in each individual situation.

So New Zealand organisations that “carry on business” in Australia and store personal information in an Australian cloud need to be aware that they will be subject to the Australian NDB Scheme and the associated penalties.

It is anticipated that New Zealand’s Privacy Bill will introduce similar breach notification requirements in 2019, but with maximum fines of only $10,000. Kiwi organisations caught by the NDB Scheme can therefore kill two birds with one stone by preparing a robust data breach response plan now that will future proof them for next year.

A good data breach response plan is essential, not only for the avoidance of fines and damages. Knowing who will do what and when in the event of a breach is key to stemming the inevitable fall out. An organised and transparent corporate response can help minimise negative customer impacts and re-build lost trust – exactly what the mandatory data breach notification laws of both countries are designed to achieve.

FIRST EVER PRIVACY AFTER HOURS EVENT IN PERTH
By: Nina Yiannopoulos

While Western Australia may be lagging behind the rest of the world without a public sector legislative privacy regime, there is an undeniable sense that change is bubbling just under the surface. The time feels ripe to give a voice to the privacy conversation in Perth!

On 5 April 2018 iappANZ had its first ever Privacy After Hours event in Perth, hosted by Deloitte. These events, which have been taking place regularly across Sydney, Melbourne and Brisbane for a couple of years now, are an opportunity for privacy professionals to come together and contribute their unique perspectives and experiences to the privacy discussion.

The event was open to both members and non-members and this was rewarded by the cross section of professionals who attended (including representatives from IT, business development, legal, risk and information management). The evening was an opportunity to share ideas, thoughts and challenges around privacy, and clearly demonstrated that you don’t need to be a privacy expert to bring (or take home) valuable insights from these types of networking events.

The evening began with a welcome on behalf of iappANZ and a brief introduction covering the recent commencement of the Notifiable Data Breaches Scheme and the upcoming introduction of the General Data Protection Regulation in the EU. After that, conversations flowed smoothly over drinks, cheese and antipasti, against a backdrop of the Swan River at dusk.

I personally hope this is the beginning of many such events in Perth, and that it gives a new voice and life to the privacy conversation on this far side of the country.
Marina Yastreboff is new to the board in 2018 and Privacy Unbound asked her whether she considered AI and algorithms threaten privacy? This was her answer:

Do AI and algorithms threaten privacy?

AI advances present significant legal and ethical dilemmas for human society.

Most AI algorithms require huge volumes of data to learn and make intelligent decisions. As made only too clear by recent events, our digital footprints, full of personal information, feed into that data pool.

In my opinion, if we have any hope in protecting our privacy, we humans need to adopt privacy by design (where privacy protection is built into systems and data protection is safeguarded in the system’s standard settings). As well as develop state of the art tools for data protection, like the Generative Adversarial Networks, Federated Learning Systems, and Matrix Capsules (a new variant of neural networks) and where possible mandate methods such as differential privacy which maximise the accuracy of queries from databases while minimizing the changes of identifying its records. But the best solutions are likely to be found using AI.

After all, even Siri likes her privacy:

Auto-bot: Siri what is your real name?
Siri: I don’t really like talking about myself, Marina.

If Siri did not disclose my name, this answer would have been attributed to an auto-bot who prefers to remain anonymous.

Marina Yastreboff is an experienced legal and compliance professional with extensive private and senior in-house practice experience, her employers and clients have included Philips Electronics and Healthcare (ANZ), Lafarge Holcim, CSC (now DXC Technology), Luxottica, Ernst & Young, and BlueScope Steel, as well as private companies and government.

She is currently contracting as Senior Legal Counsel at Steinhoff Asia Pacific where she is responsible for legal and compliance issues across the corporate group, including data protection, privacy, AML/KYC/KYTP, sustainability, franchising, cross border financing, IT contracts and dispute resolution.

She is passionate about technology, its development and application, especially the areas of intellectual property, big data analytics, block chain, quantum computing and the human genome.

Marina is admitted as a solicitor in Australia, New Zealand and the United Kingdom and is also a Certified Practising Project Manager, registered trade marks attorney and notary public. In the broader community, she is a member of the University of Wollongong Faculty of Business Advisory Board, a committee member of the NSW Society for Computers and the Law and co-founder of InspireArt.Foundation – a community based initiative that donates art to brighten up hospitals.
UPCOMING EVENTS

2018 iappANZ Summit
Date: 1-2 November 2018
Time: 8am – 5pm
Venue: ZINC @ Federation Square, Melbourne, Australia