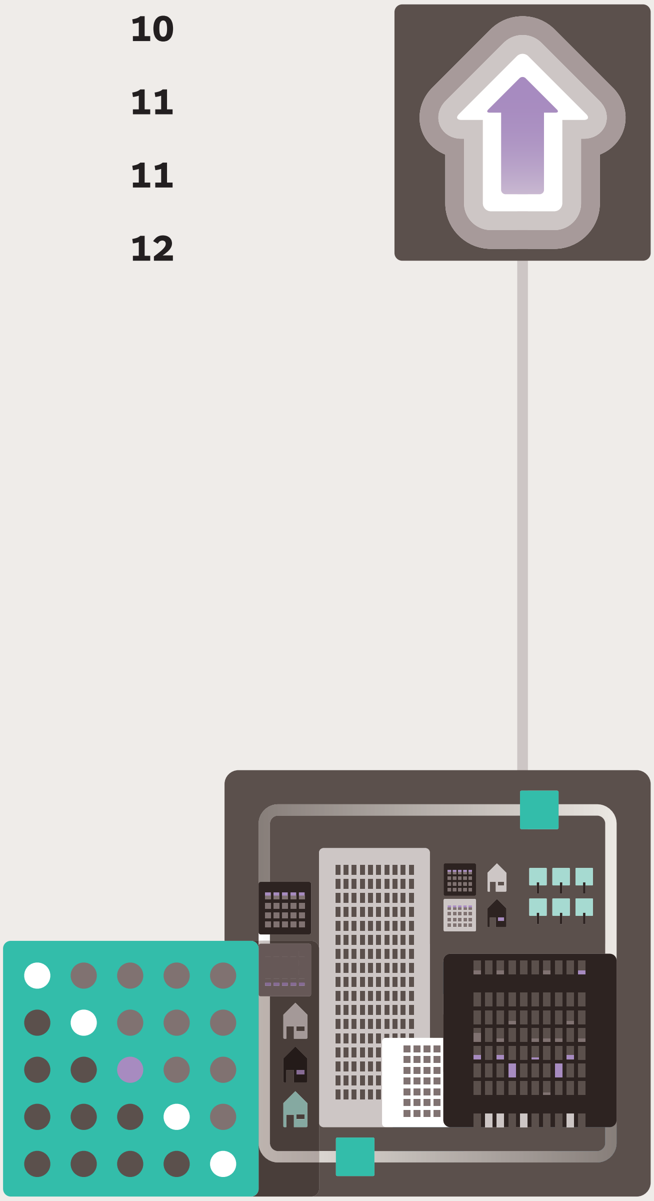
How Australians feel about privacy

And how it impacts our use of online services

Insight paper

June 2017

Contents



The trade-off between convenience and privacy is more relevant as the amount we do, share and transact online grows exponentially.

Consumers and businesses are asked to provide personal and or sensitive data in exchange for access to services. And organisations are finding new ways to extract more value from that data – from designing better products and services to selling insights to third parties.

Meanwhile, there's a heightened awareness of the risks of sharing personal information. Major security breaches have become a constant reminder, and identity theft is one of the most common crimes in Australia.[1]

So it's no surprise that privacy is the major concern for Australian consumers when it comes to using online services. Research suggests 69% are more concerned about their online privacy than they were five years ago.[2]

Consumers are making conscious decisions every day about the organisations they trust and are willing to deal with. Australia Post's research has identified a range of behavioural segments when it comes to making those decisions.

The spectrum of Australians online, ranges from 'relaxed natives', who may choose convenience over privacy, to 'worried rejecters', who find it hard to keep up with technology.

It has never been more important for businesses and government to proactively manage this privacy trade-off. Providing a trusted framework that enables both sides to gain value from the data exchange – without increasing their financial, social or reputational risk, is key.

In this insight paper we explore how the concept of privacy has changed in our digital age, and the increasing importance of trust and transparency. We also identify some guiding principles and the potential impact of new regulations on the way we understand and manage privacy in the future.

[1] Trends in Identity Crime, Attorney-General's office – Nov 2016

[2] Australian Community Attitudes to Privacy survey results, Office of the Australian Information Commissioner – May 2017

Part A: Our evolving attitudes to privacy

Security and privacy go hand in hand. Without data security, there's no privacy. And perhaps, less confidence that our personal information can be protected.

The latest Attitudes to Privacy survey results reveal Australians believe online services and social media sites pose the biggest privacy risk to their security.

They are most reluctant to provide their financial status (42%), address (24%), and date of birth (14%).

The main reasons given were fear of financial loss (17%) and that the information may be misused or passed on without their knowledge (15%). For another 16%, it is simply 'none of their business'.[3]

ACMA's Managing your digital identity report found that while most Australians are comfortable providing personal data (such as their phone number or date of birth) to government agencies, they resist sharing this with businesses.[4] Some may avoid this requirement by going elsewhere for services –

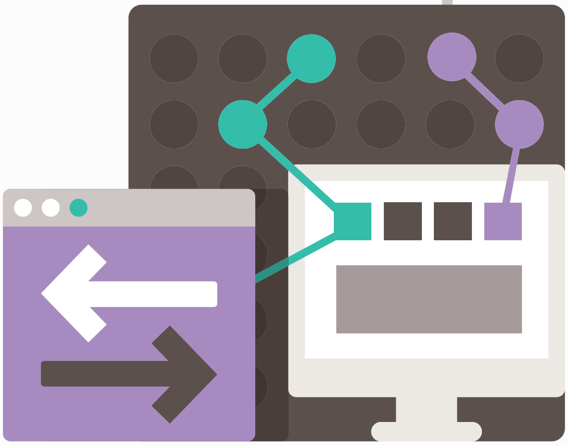
while as many as 47% may provide incorrect information.

And while most people are aware that companies collect information about them, the majority fail to realise just how much they're sharing. In a recent global survey, just 23% realised they share their web searches and 25% their location.[5]

Behavioural segmentation

Research conducted for Australia Post by Data2Decisions in December 2016 benchmarked changing attitudes to digital confidence, control and security. The results of the Online behaviours, attitudes and beliefs study segmented online users by their attitudes towards privacy and security. We found that overall, concerns about the invasion of privacy through new technology was down, when compared to a year ago – but was still the main concern for 68% of Australians online.

Just over a third (36%) feel comfortable giving their credit card details over the internet and only 29% feel comfortable giving their personal details online.[6]



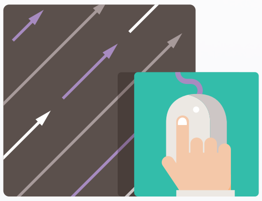
[3] Australian Community Attitudes to Privacy survey results, Office of the Australian Information Commissioner May 2017

[4] Managing your digital identity: Digital footprints and identities research—Short report 1, ACMA – Nov 2013

[5] Customer data: designing for transparency and trust, Timothy Morey, Theodore Forbath and Allison Schoop, HBR, May 2015

[6] Online behaviours, attitudes and beliefs, Data2Decisions/Australia Post, April 2017

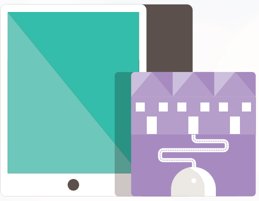
Attitudes to the trade-off between privacy and convenience (The numbers below represent the % of Australians online)



Worried Rejecters do not feel digital technologies are giving them control, they are worried about privacy, and the prospect of easy internet access does not appeal to them.

16%

"Technology is changing so fast, it's difficult to keep up with it."



Fence Sitters are not convinced the internet is giving them control, but they are not concerned about threats to their privacy.

16%

"I would spend more time using online services if it wasn't always so complicated."

Concerned Explorers are not sure technology is empowering. They're worried about privacy threats, but they also want to be able to access the internet seamlessly.

22%

"I might do more tasks online if it was more secure and more convenient."

Experienced Adapters feel that technology empowers them but are concerned about risks to their privacy.

30%

"Security and privacy safeguards can't keep up with the pace of technological change."

Relaxed Natives feel that computers and technology give them more control. They're not worried that technology is a threat to their privacy.

16%

"It's such a hassle having to log in all the time."

The convenience and privacy trade-off

As Data Governance Australia's white paper highlights, "consumers expect great experiences from brands and, increasingly, from government... There's a mindset shift from suspicion ('what are you doing with my data?') to frustration ('why aren't you using my data?')."[7]

There's a line in the sand when it comes to sharing personal information. Organisations should only collect the data they need at that moment in the customer relationship. Any more, and you risk diluting trust.

We increasingly expect personalised data to help improve our experience of products and services (such as product recommendations, adapting to our preferences, or helping us save money).

Government agencies are also increasingly opening up access to data to improve the way they deliver services – such as analysing health services or road and transport usage. Australians are more open to government sharing their data between agencies (33%) than businesses sharing it with other businesses (10%).[8] Australia Post's 2015 research into eGov services also found that 48% of Australians wouldn't mind government agencies sharing personal data with other agencies if it made their lives easier.

If consumers and organisations are to benefit from the use of personal data, it's helpful to consider the potential value different data holds – and what we might expect to gain from it.

It's also important to be clear about the different elements to our personal data and how technology enables advanced analytics and algorithms to rapidly predict outcomes.

At Australia Post's Annual Privacy Awareness Week event, the Victorian Commissioner for Privacy and Data Protection Professor David Watts shared his views on the potential issues with big data.

> "Although big data offers society benefits derived from new insights and pattern recognition, like all technologies it can cause harm. There is a growing body of evidence that big data can be used to manipulate individual and public opinion, cause discrimination and increase marginalisation."

He classifies this data into five categories:

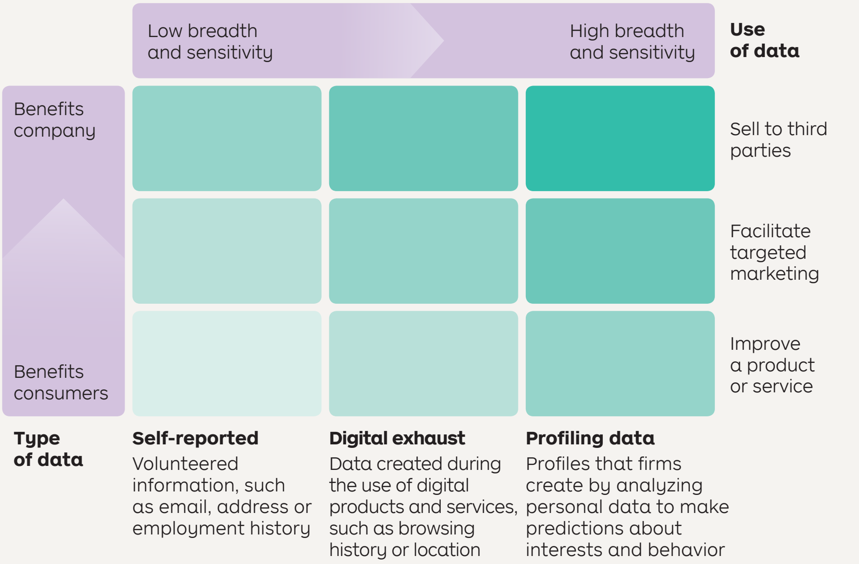
- Human generated data
- Web and social media data
- Transactional data
- Biometric data
- Machine to machine (Internet of Things (IoT)) data

These data types can combine to form a clear picture of who we are – and what we are likely to do or need next. Professor Watts also noted that algorithms can 'go wrong' – they are only as useful as the accuracy of both data and programming. For example, Centrelink's recent issue with robo -debt collection letters highlights the potential risk of automating data linkage assumptions.

Data collection, storage and analysis are clearly more than a compliance issue. Organisations need to ensure they are transparent about the way data will be used. They also need to provide value in exchange – and respect the consumer's right to their privacy.

Swapping value for data

The more people value data, the more they expect companies to provide in return for it.


Low breadth and sensitivity
High breadth and sensitivity
Use of data
Benefits company
Benefits consumers
Sell to third parties
Facilitate targeted marketing
Improve a product or service
Type of data

Self-reported
Volunteered information, such as email, address or employment history

Digital exhaust
Data created during the use of digital products and services, such as browsing history or location

Profiling data
Profiles that firms create by analyzing personal data to make predictions about interests and behavior

Source: Customer data: designing for transparency and trust, Timothy Morey, Theodore Forbath and Allison Schoop, HBR, May 2015

[7] Building consumer trust, Data Governance Australia in association with ADMA – Feb 2017

[8] Australian Community Attitudes to Privacy survey results, Office of the Australian Information Commissioner May 2017

Crossing the 'creepy line'

Within businesses seeking to make the most of data,

"there is an omnipresent tension between legal and compliance departments and marketing departments,"

commented Saara Mistry, NAB's Acting Chief Privacy Officer, at the Privacy Week event.

"The challenge is to balance the need to realise the inherent value of customer data, but also retain privacy and security of their information. The key to retaining their trust is clarity about how we collect and use their information – and remaining true to these promises."

And with online behavioural data being cross-referenced in new ways to enable retargeting and other digital marketing techniques, consumers feel a sense of being 'stalked' by businesses. Just 21% of Australians are comfortable with targeted advertising based on their online activities.[9]

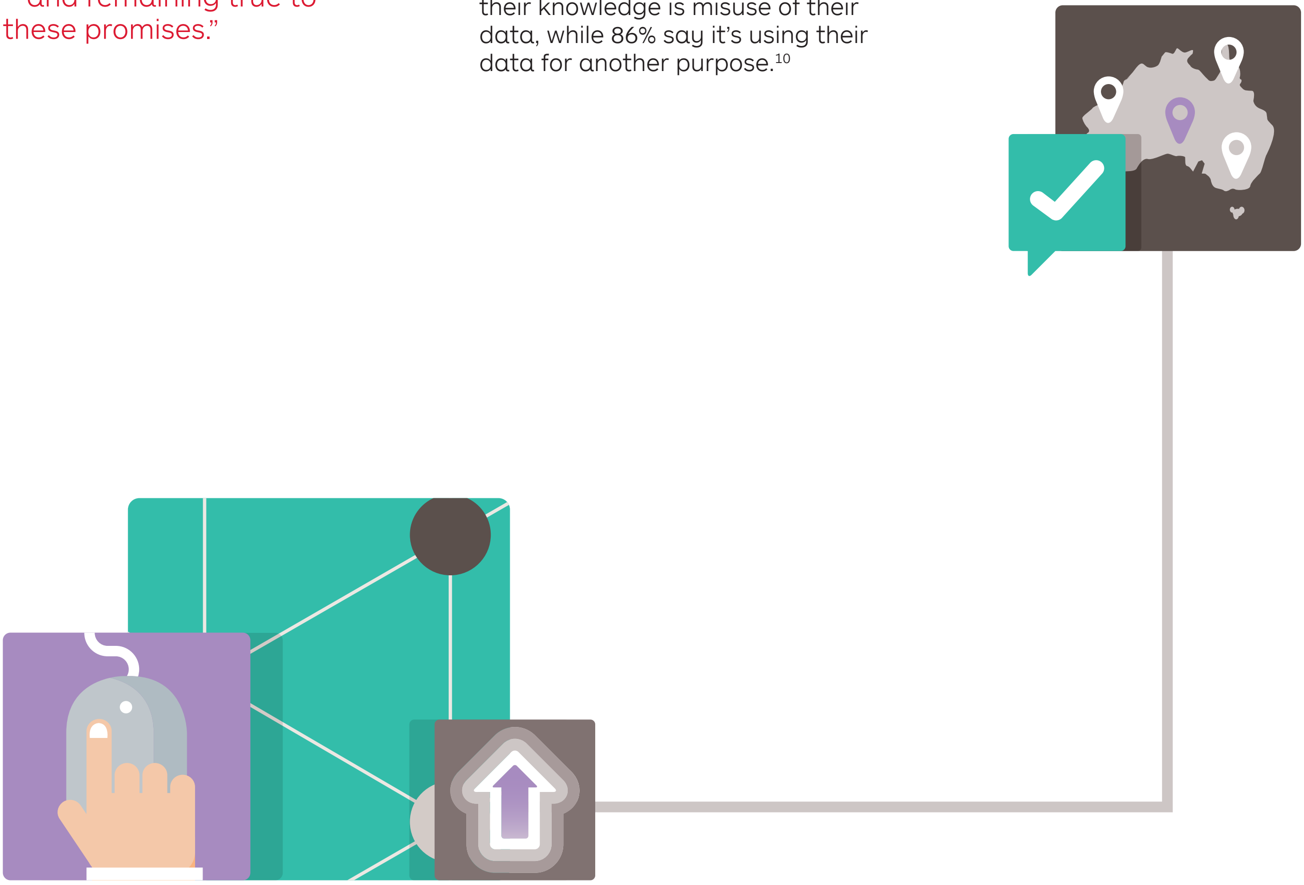
That 'creepy line', or what we might define as 'misuse' of our data, means different things to different people. Younger Australians are less concerned with targeted advertising, with 49% of those under 35 being uncomfortable with it, compared with 67% of those aged 35 and over.

However, in general, 84% of Australians believe monitoring their activities on the internet and recording that information without their knowledge is misuse of their data, while 86% say it's using their data for another purpose.[10]

We have the right to control this through consent, but many users unknowingly provide this – only 29% of people read website privacy policies, fewer than in 2013. Given many fine print contracts run to 30,000 words or more, this is hardly surprising.[11]

Professor Watts believes

"One of the main culprits of this is contract law. Perhaps what we need is a strengthening of consent, not a complex new right."

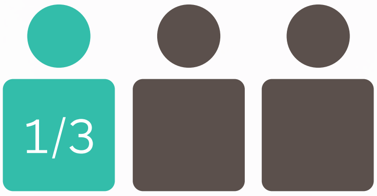


[9] Australian Community Attitudes to Privacy survey results, Office of the Australian Information Commissioner May 2017
[10] Australian Community Attitudes to Privacy survey results, Office of the Australian Information Commissioner May 2017
[11] Will you read this article about terms and conditions? You really should do, Robert Glancy, The Guardian, 2014

The importance of trust

As global ransomware attacks such as Wannacry in May 2017 and security breaches such as Yahoo's in 2016 highlight, online data is exposed to a different level of threat to the physical world; it can cross borders and scale quickly.

There's a growing awareness of the risks of online behaviour.



One-third of Australians know someone who has been a victim of identity theft – or have been a victim themselves. They are now more likely to read privacy policies to alleviate their concerns.[12]

There is a business cost to this lack of confidence. More than half

58%

of Australians have decided to avoid dealing with a private business because of privacy concerns – while

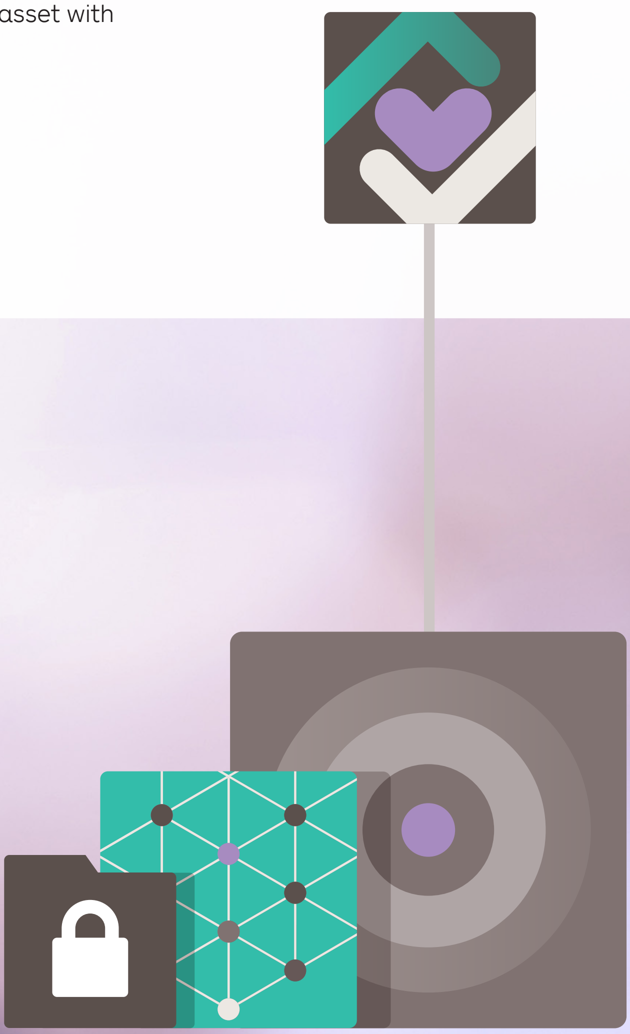
16%

have decided to avoid dealing with a government agency.[13]

And that's why trust has become a key point of difference for many organisations, and an asset with measurable value.

Meanwhile, even before the Australian Census website was reportedly taken down in a DDoS attack in August 2016, there were alarm bells ringing amongst the Australian public; they were concerned their personal data (including names and addresses) would be kept and stored.

Part of the 'social contract' Australians make when they provide information is that their information will be de-identified as quickly as possible.



[12] Australian Community Attitudes to Privacy survey results, Office of the Australian Information Commissioner May 2017
[13] Australian Community Attitudes to Privacy survey results, Office of the Australian Information Commissioner May 2017

Part B. New guidelines for a digital age

Privacy principles for online services

Resolving the issues of privacy consent, trust and transparency are complex, especially as new technologies make it easier to capture, store and analyse data. From biometrics to blockchain, and artificial intelligence-enabled machines, there are many new ways data can be used – or mis-used.

When creating Australia Post's new Digital iD™ solution, we developed a set of privacy principles – informed by the OAIC Australian Privacy Principles. These principles met the customers' need for security and control, and provided the convenience they are seeking when transacting online.

Digital iD™ will enable consumers to easily prove who they are, via their computer or smartphone. Having identified the friction that comes with managing multiple login and password combinations, it may also help overcome password fatigue.

ACMA's Managing your digital identity report reveals most Australians manage between five and 50 login and password combinations to do everyday activities online. Increasingly, some Australians are side-stepping that process by using their Facebook, Google or LinkedIn credentials to log in to online platforms – potentially putting them at risk.

BCG modelling also found that by addressing the gaps in the current online identity management process in Australia, $11billion[14] could be saved through reduced cost to serve, reduced cost of fraud and improved consumer experience.

"Many other countries are trying to resolve this digital identity challenge,"

explains Regis Bauchiere, Australia Post's General Manager of Identity Services. Bauchiere was involved in the development of India's Aadhaar biometric identity platform – a voluntary solution used by more than 1 billion Indian citizens to access services.

"Privacy is a sensitive topic in India. To ensure that privacy aspects were taken into account, a pilot was established at the early stage of the project, which ultimately influenced the design of the solution.

Firstly, the Aadhaar number is random and does not carry any information such as gender, religion or state of origin. Secondly, to minimise exposure to privacy breach, the Aadhaar solution only stores a minimum set of attributes: name, date of birth and phone number. Thirdly, the Aadhaar platform allows people to authenticate themselves when accessing a public service but only provide a yes / no answer without divulgating personal details to the service provider".

"In Australia, we want to embrace digital technology and have convenience. But we also want to make sure our data is securely stored,"

explains Bauchiere.

"When we interact, we want to know how our data is being used, and we only want to provide what's required for that service."

So Digital iD™ relates to a specific level of assurance and asks the user for consent to disclose information. Only the relevant information for each service is shared with the provider with the express consent of the user.

[14] Calculated by BCG based on the following sources: publicly available data on identity services requirements for Federal and State Government, financial services, utilities and telcos, Identity crime and misuse in Australia 2013–14 (Attorney General's Department), How Australians use their time 2006 study (ABS), Value of unpaid work (ABS), NAB Online Retail Index, Internet of things: the re-imagination force, TCS

'Privacy by design'

Any online service or application needs to have privacy embedded into its design. This has been termed ‘privacy by design’, and goes beyond compliance to include the following principles:

1. Proactive prevention – rather than reactive once breach occurs

2. Value privacy as a default setting – don’t over-collect data

3. Embed privacy alongside every function – such as authentication and encryption

4. Cover the full user lifecycle – collecting, creating, sharing, retaining and destroying data

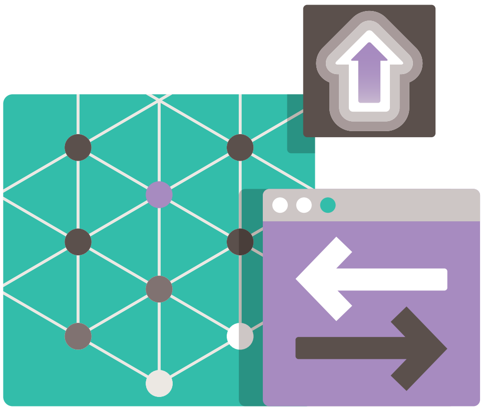
5. Transparency – be clear about what users can expect. Use plain English in privacy agreements

6. Customer-centric design – make sure you use their data to provide them value, relevance and trust.

These principles were applied during the design process for Digital iD^{TM}. During industry workshops, we tracked the flow of user data through the platform. The solution had to limit the need to ‘over-share’ information – otherwise there would be a 'disconnect' in the user experience.

Bauchiere believes biometric technology will become a valuable capability to protect our privacy.

> “Biometric is by essence the ideal technology to authenticate someone. It’s something you intrinsically are – not something you have or know – that can be shared, stolen or lost. The challenge is establishing the first binding reference you can trust, and then make sure that the authentication service is resistant to spoofing attacks" says Bauchiere.



Mandatory notification requirements

In addition to these elements of design, we will need processes to respond quickly to data security breaches.

From early 2018, Australian government agencies and businesses will be required to notify any individuals affected by a data breach that is likely to result in 'serious harm', under the Data Breach Notification Bill. This will provide more transparency over the risks and response.

"Soon, we will know more about security breaches,"

comments Professor Watts.

"The transparency this legislation offers is welcomed. It introduces a measure of security accountability,"

he continues.

Jason Holandsjo, Chief Compliance Officer for Telstra, believes the new bill is the bare minimum expectation for organisations.

"If you're a customer-centric organisation who wants to keep your social contract, you'll already have that collection, use and management process in place. We need to engage quickly with our community to share accurate and timely information if something does go wrong."

Defining 'serious harm' is challenging. NAB's Mistry suggests

"putting ourselves in our customer's shoes; does it allow a third party to transact on their account, or facilitate identity theft or fraud? Do we know who has the information – and do we have a relationship with them so we can get a swift response to secure their information and their accounts?"

In saying that, the Data Breach Notification Bill does give guidance about determining whether a breach causes 'serious harm'.

The business case for protecting data

"In the past, privacy was seen as a compliance issue 'at a minimum cost'. Now organisations see proper management of privacy as a differentiator that provides value to their customers and builds trust,"

comments Bauchiere.

So how can we do this without restricting the free flow and use of information? Without causing friction for the consumer, or reducing the more meaningful insights we can get from combining different data-sets?

This is at the heart of the convenience / privacy trade-off. But lessons from Yahoo, Wannacry, Census and more, make it clear that privacy must come first. Otherwise, the costs will add up quickly: in lost customers, time, reputation and business value. Not to mention the tangible risk of legal damages.

Professor Watts believes 2017 is the year Australian information security law will emerge – but that

"real legal consequences (damages verdicts from class actions) may be essential to developing a corporate and government culture where information security is taken seriously."

What will be needed are deep behavioural changes – at an organisation, government and individual level.

Everyone shares a responsibility for protecting privacy and security – from understanding the impact of our own behavior online and what we are agreeing to share, to risk management protocols that keep pace with increasingly sophisticated cyber-attacks.

"Australia Post's identity services are based on trust, security and transparency. We have to keep this in mind at all times for our customers,"

says Bauchiere.

Conclusion

Overcoming the data trust barrier

Privacy is the key concern of the majority of Australians using online services. And if we are to fully realise the economic and social benefits of an increasingly digital society, we need to overcome the trust barrier.

This means embedding security within every aspect of online product design; going beyond compliance to ensure transparency and value to users. Businesses and government have a responsibility to be clear about what data they really need to collect, and how it will be shared and used – so they avoid crossing the 'creepy line'.

Ultimately, privacy is about individual control. And while consumers remained concerned, they don't always know what they're being asked to trade for the services they use. To securely reduce friction in online processes, solutions such as Digital iD™ can help put users back in control of their data.

With solutions like this, and with a clear and transparent privacy framework, Australians may have a better understanding about their rights, and make smarter security choices about their privacy in the digital age.

To find out more about our enterprise and government solutions, please visit auspostenterprise.com.au