



# accan

**MAGAZINE**

THIS EDITION:

# THE PRIVACY ISSUE

**PUBLIC VS PRIVATE**  
- HOW *OUR WORLD* IS CHANGING

HOW TO: *CREATE SAFE, STRONG PASSWORDS*

PLUS: *MEET THE PRIVACY COMMISSIONER*

TWITTER'S PRIVACY POLICIES *PLUS MUCH MORE*

WINTER  
2012

ACCAN.ORG.AU

**ACCAN  
MAGAZINE**

ISSUE: 05

# OUR CEO: TERESA CORBIN



This Winter, we've dedicated ACCAN Magazine to privacy following a spate of hacking of high-profile websites (see our story on page 3). This again highlights the need for consumers to take care with what they share their online and how they secure their personal information (see page 9).

The right to privacy is one long-held in our society. When asked, most people say privacy is an issue they care a great deal about. But interestingly, if you ask people how they take steps to protect their privacy online, they usually say they're not too sure what they should be doing – other than trying to keep across the changes to Facebook privacy policies.

The internet offers great potential to make the way we live easier. Most of us already take for granted some of the many communication tools we have at our fingertips like email, internet banking and social media. But there are risks to sharing all this information online, and consumers need good information about how to minimise them.

We've taken a look at some of the big issues in privacy at the moment, including law reforms currently underway that will increase the Australian Privacy Commissioner's powers (page 4). We also chat with privacy advocates, the Australian Privacy Foundation (page 12), and look at some of the solutions being proposed by copyright holders and governments around the world to address illegal peer-to-peer file sharing.

I hope you enjoy the issue. As always, if you'd like to get in touch please email [teresa.corbin@accan.org.au](mailto:teresa.corbin@accan.org.au) or phone me on 02 9288 4000 or TTY 02 9281 5322.

Warm regards

Teresa Corbin  
Chief Executive Officer  
ACCAN

## ACCAN OUR STORY

ACCAN is the peak organisation representing all consumers on communications issues including telecommunications, broadband and emerging new services. Our mission is to ensure the availability, accessibility and affordability of communications services for all Australians.

### CONTACT US:

Phone: 02 9288 4000

TTY: 02 9281 5322

Web: [accan.org.au](http://accan.org.au)

Twitter: @ACCAN\_AU

Email: [info@accan.org.au](mailto:info@accan.org.au)

## MAGAZINE CONTRIBUTORS

### EDITOR

Elise Davidson

### DEPUTY EDITOR

Erin Turner

### EDITORIAL ASSISTANT

Mark Callender

### CONTRIBUTORS

Dani Fried

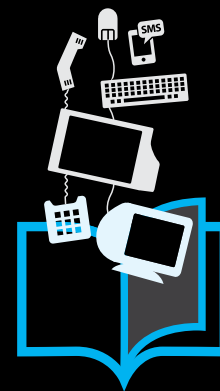
Jonathan Gadir

Robin McNaughton

### DESIGN

Creative Order

[www.Creative-Order.com](http://www.Creative-Order.com)



**6-8**

**CAN YOU  
HAVE  
A PUBLIC  
PROFILE  
AND A  
PRIVATE  
LIFE?**

**CONTENTS**



- 2** **UP FRONT**  
What's making news across the telecommunications industry
- 4** **INDUSTRY IN FOCUS**  
Meet Australia's Privacy Commissioner, Timothy Pilgrim
- 5** **THIS IS HOW I... USE THE NET**  
IT industry personality, Pia Waugh, explains how she manages her online profile
- 6** **COVER STORY**  
Can you have a public profile and a private life?
- 9** **CONSUMER TIPS**  
How to keep your personal information safe online
- 10** **POLICY IN FOCUS**  
We take a look at what's happening with online copyright
- 11** **GRANTS IN FOCUS**  
Melbourne University on how high-speed broadband will change households
- 12** **MEMBERS IN FOCUS**  
We chat to Nigel Waters, Board Member of the Australian Privacy Foundation



# LATEST NEWS

## ACCAN gets tick in government review



ACCAN has only been around since 2009, but our effectiveness as Australia's peak consumer telecommunications body was recently highlighted by the Department of Broadband, Communications and the Digital Economy (DBCDE).

In a mid-term review into ACCAN's first two years of operations, the DBCDE acknowledged our successes as well as providing welcome constructive feedback.

"The review recognises the significant difference ACCAN has made to the telecommunications landscape in a relatively short period of time," Senator Stephen Conroy, Communications Minister, said in a statement.

Some of ACCAN's early accomplishments include the establishment of a \$250,000 per annum Independent Grants Scheme; successfully advocating for changes to call costs to 13/1800 numbers from mobile phones; and the publication of well-regarded research, submissions and consumer information.

Twenty-four submissions were received by the review, all of which were supportive of ACCAN's continued funding. ACCAN's Board and staff are keen to now implement the report's suggestions – and continue the work we're doing to support Australian telecommunications consumers.

CEO Teresa Corbin said, "The ACCAN Mid-term Review makes a number of recommendations, which we'll reflect on and make some changes as we grow as an organisation. Particularly, we are hoping to have a greater focus on small business and formalise our existing relationships with industry by putting in place regular roundtable events."

## Twitter's privacy policies in the spotlight

Although the Electronic Frontier Foundation ([www.eff.org](http://www.eff.org)) recently awarded Twitter a very respectable 3.5 rating out of 4 for their protection of user privacy against government intrusion, many in the 'Twitterverse' remain concerned that their information is being tracked and harvested and may be used improperly in the future.

There are a number of tools that Tweeters can choose to opt out of being tracked – Do Not Track Plus and Twitter Disconnect, among others. But these rely on the customer actively opting out of the tracking system.

Many users may well see benefits in being alerted to other accounts they'd like to follow. ACCAN encourages Twitter and other social media sites to put privacy first and allow their customers to opt in if they choose to.

### THUMBS UP OR DOWN



#### BIG UP

- ☺ For the Digital Switchover Taskforce who have commissioned special "talking" set-top boxes as part of the Household Assistance Scheme. This will ensure blind and vision-impaired Australians can access television
- ☺ For Telstra who will be sending location-based emergency SMS notices to mobile customers this bushfire season

#### WAY DOWN

- ☹ To TPG and Apple who have both received \$2 million-plus penalties for misleading advertising following action by the Australian Competition and Consumer Commission.





## Cyber-attacks on the rise

Consumers have more reasons to be concerned about their privacy with Telstra recently suffering its third privacy breach in six months and social media site LinkedIn, music site LastFM and dating site eHarmony all losing millions of passwords to hackers. First State Super Trustee Corporation (FSS) was also recently found to have breached the Privacy Act after a hacking incident last year.

The Australian Privacy Commissioner, Timothy Pilgrim, said, "...it is worrying that hacking incidents like this are occurring more often. These incidents highlight the importance of businesses ensuring that they maintain the most up-to-date security systems to ensure the protection of the personal information they hold about customers."

FSS has been acknowledged for notifying affected customers immediately but that's certainly not the norm in some of these cases. One way of holding big companies to account might be to compel them to disclose privacy breaches, as happens in the US, UK and Europe.

## 2011-2012 Regional Telecommunications Review findings released

In May, the findings and recommendations of the 2011-2012 Regional Telecommunications Review were released.

The Chair of the Regional Telecommunications Committee, Rosemary Sinclair, said, "The availability of reliable, affordable high-speed broadband in homes will enable changes in service delivery, from the way people access health, education and government services, to the way they live and work."

Key recommendations made by the Committee include:

- The establishment of a co-investment program, and roaming and access arrangements, to expand mobile coverage in regional areas.
- A review of the eligibility criteria for access to the NBN Interim Satellite Service (ISS)
- The formation of a "National Digital Productivity Council of Experts" to address targeted ICT training, and barriers to the development of telehealth and e-learning.

To see all recommendations and findings, visit [www.rtirc.gov.au](http://www.rtirc.gov.au)

## Crunching the Numbers:

# 15 MILLION

*Number of Australians aged 14 years and over who used the internet during the December quarter of 2010*

# 6.6 MILLION

*Number of Australians who check Facebook daily*

# 6.2 MILLION

*Number of Australian households with broadband internet access in 2010-11*

# 88%

*Percentage of 15 to 17 year olds who participated in social networking on the internet in 2010-2011*

# 68%

*Percentage of Australian internet users who made a purchase over the internet in 2010-2011*

# TIMOTHY PILGRIM

## AUSTRALIAN PRIVACY COMMISSIONER

---



### **Privacy is in the spotlight more than ever before. What are the biggest consumer issues?**

Privacy is a basic and important human right. I'd like to see Australians making informed decisions about their privacy. Privacy is becoming increasingly important as more personal information is collected, stored and shared, often outside Australia. The online storage of personal information creates risks, including that the information may be compromised by a data breach incident. Consumers need to think carefully about what personal information they choose to disclose and whether the organisation collecting their information has adequate security systems in place.

### **A privacy law reform process has been under way since 2006. Where are we up to?**

The Australian Law Reform Commission (ALRC) finalised its inquiry in 2008, making 295 recommendations for reforms to the federal Privacy Act. Given the report's size, the Government decided to respond in two stages: the first stage response to 197 of the 295 recommendations was released in October 2009, and the Government introduced the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 in May this year.

One of the key changes is the establishment of a single set of Australian Privacy Principles that will apply to both businesses and government agencies covered by the Privacy Act. New provisions will also strengthen the powers of the Privacy Commissioner to resolve complaints and promote compliance with privacy obligations.

### **How will your powers be strengthened under the new laws?**

At the moment I can only make enforceable determinations in response to complaints. However, under the proposed laws, I will be able to make a declaration that privacy has been breached and require specified steps be taken within a specified period regardless of whether there

has been a complaint or I have initiated my own investigation. I will also be able to seek enforceable undertakings, as well as civil penalties in the case of serious or repeated interferences with privacy.

### **Are there any particular privacy issues relating to telecommunications?**

Mobile phones today store much more than telephone numbers. We are increasingly using handheld devices for a variety of online transactions that involve the sharing of our personal information. Your smartphone is no different to any other device that stores personal information. You need to protect it with a secure password and be mindful to look after it.

I'd also urge people to be wary when using location-based services that use technology to find your mobile phone's geographic location. While they can be useful and fun, there are also risks to consider. For example, each time you 'check-in', you give other users information about your personal and social patterns like favourite destinations, affiliations and memberships, and likes and dislikes. This activity can have unintended consequences, like someone following your movements, or pose a security risk for your family and home.

---

### **About Timothy:**

Timothy Pilgrim has been the Australian Privacy Commissioner since July 2010, and prior to that was Deputy Privacy Commissioner from 1998. He has led investigations into major data breaches, engaged with government and business to ensure best privacy practice and made a significant contribution to law reform to ensure privacy regulation keeps pace with developments in technology.

---

# PIA WAUGH GEEK AND ACTIVIST



## You're a recognised IT industry personality, how did you become involved in IT activism?

In about 1999 I was new in the industry, working as a junior techie at a large IT systems provider. Just for fun, I started playing with Linux. I had only recently discovered Linux and – as a technical

person – it was amazing! I learnt more in the first few months than I had learnt using Windows and before that DOS for most of my life. My mum was a techie so I have always been around computers and software. Later when I went to my local Linux user group I discovered the ethos of software freedom and collaboration, the concept that the tools you use define the life you lead, and thus the freedoms you have.

In 2003 I was elected president of Linux Australia and my work there demonstrated to me the gaping chasms between industry, government, community and academia. I later became president of Software Freedom International, the body behind Software Freedom Day, and saw that the ethos of software and technology freedom was universal. I also saw the freedoms technology enables for people to improve their lives, freely connect with others across the globe and express themselves.

In 2009 when Senator Kate Lundy headhunted me for an IT policy adviser role, I jumped at the chance to understand how government works, how policies are created and the impact on us all. My passion is society, democracy and freedom, and working in politics was part of a journey in understanding the different aspects that shape our lives. With the Senator I embarked upon the path of Open Government, which is all about transparency, public engagement and a citizen-centric approach.

My next endeavour is into the belly of the beast, the public service, where I want to better understand how policies are implemented, how

the public service works (and doesn't work). I look forward to helping improve how government uses technology for the benefit of the society it serves.

## How do you manage your online profile and privacy?

I just be who I am. I think the idea of splitting our online lives into personal and professional is unworkable in the long run and just being myself has served me far better than any "strategy". I have been online since the mid '90s and a semi-public figure in my community for almost 10 years, I am used to it. It's like real-world security, be sensible, don't leave your wallet just sitting around, don't announce to the world where you are every second of the day. But at the end of the day, if someone really wants to get you, they generally can. So have backups, some skills and friends to help you in the event of a breach.

## Do you think people should be concerned about their online privacy?

I think people need to be taught how technology works better so they can make more informed decisions about their life. The tech literacy in this country is appalling, with IT in schools having been reduced to making documents. If all kids were taught how the internet works, basic online citizenship, basic programming, we would have a safer and more innovative population.

Again, it is the technology we use and how we use the technology that defines our freedoms, so if we are to have a free society, we need people to be skilled and confident in the tools they use, and in creating the tools they need.

We are starting to see all the traditional bastions of power break down through the democratisation of publishing, communications, monitoring and enforcement. We have, in my opinion, a slim window in which we can reshape the future. As geeks, as the ones who imagine and make the tools of tomorrow, we have a special responsibility to help ensure the most free and meritocratic society possible.

FEATURE  
STORY:

**CAN YOU  
HAVE**

**A PUBLIC  
PROFILE**

**AND A**

**PRIVATE  
LIFE?**

Story by Elise Davidson



**Few would argue that the internet hasn't fundamentally changed both the way we live as individuals and our society as a whole. Technology is moving at a phenomenal pace, and it is international technology companies like Google, Facebook and Apple that are the power players of the 21st century.**

With companies able to track what we view online, what we buy and even where we live, it brings with it a whole lot of questions about privacy and what it means – what are our rights to privacy in a world where everyone is connected? What rights do we have to protect our personal information? Most importantly, how can we do that, as we move deeper into the digital era?

## LOCATION-BASED SERVICES – WHY WHERE YOU ARE MATTERS

In addition to geographic data collected when using your credit card, or electronic road pass, the location-based apps offered by most smartphones mean many of us are inadvertently or knowingly sharing a lot of information about our locations. Many phone apps, including everything from news and restaurant finders to games and transport information, are able to pinpoint your location using Google maps.

People using social media like Facebook, Twitter or FourSquare seem often blithely unaware that the personal information shared could be used maliciously to find out where someone lives, work and socialises. People who announce on Facebook they're taking a family holiday for example, make it simpler for a thief to realise there's an empty house in town for the next three weeks. Sure, there are privacy settings that you can use so only your "real friends" have access to that information, but privacy settings change regularly across these sites and it's left up to the individual to be diligent in ensuring that what they're sharing isn't ... oversharing.

Social media of course also poses risks to our personal safety, in the event of domestic violence or stalking.

## IDENTITY THEFT

Identity theft is another great concern with the information we provide online. Fifteen years ago we might have carefully ripped our bank statements into tiny squares. Today, we provide information about our name, date of birth and address to any number of companies online, often without securing the information with a strong, safe password (see page 9). This information could be used by modern-day criminals to obtain your ID, access your bank accounts, or take out a loan or credit card in your name. Once your identity is stolen, it can take months or even years to unravel. *(See Melissa's story)*

## ARE ATTITUDES CHANGING?

There's no doubt that attitudes are changing. Information our grandmothers would never dream of sharing in company is routinely shared by Gen Ys (and the now-teenage Gen Zs) over social media. Questions are raised about how this information is shared and how it will affect people down the track when looking for employment, making friends and even entering relationships.

One thing is for sure, it isn't an issue that's going to go away – with data breaches on the rise, consumers need to be more careful than ever to protect their information – whether it is online or through a smartphone app.

### MELISSA'S STORY

Melissa, a director of a small business, contacted the Telecommunications Industry Ombudsman (TIO) in January 2012 after she was the victim of a scam. She told the TIO that her business mobile had been transferred to another provider without her knowledge, which led to a large amount of money being withdrawn from her bank account.

Melissa said after receiving a text message that read "SIM Card not provisioned", she contacted her service provider. It advised her that a third party, "Tara", had authorised the transfer of her mobile service to another service provider.

When Melissa's bank subsequently contacted her to advise that its fraud group had identified a suspicious transfer of \$38,000 from her account, it became apparent to her that the mobile service transfer was part of a banking scam. The scammers target consumers whose internet banking feature requires SMS authentication for funds transfers. The TIO have received 36 similar complaints regarding this scam. The TIO have kept track of the complaints and have provided relevant information to the ACCC and Federal Police.

These cases demonstrate the importance of keeping all your personal information private, using safe, secure passwords online and not disclosing any personal information in response to an unsolicited email, SMS or phone call.

## ROZIE – GEN X

### What does privacy mean to you?

A certain level of freedom from public scrutiny and personal security. I want some control over my life (in the real world and online), and to be able to keep personal matters to myself and my partner.



### How do you keep your personal information safe online?

I don't use my real full name online. I use the privacy settings on Facebook (friends only), on Flickr personal photos are made private for viewing by friends and family only. My Twitter account is public, but I take care not to tweet anything too personal.

### Are people more worried about privacy than they used to be?

Some younger people who have lived their whole lives online may be less concerned with privacy, whereas older people remember a time when everyone didn't need know "what you ate for breakfast".

## BEN – GEN Z

### What does privacy mean to you?

To protect yourself from other people accessing your personal information. I think privacy is more of an online issue, especially with Facebook where my personal information could be accessed by almost anyone.



### How do you keep your personal information safe online?

My Facebook privacy settings allow my friends to access all of my photos, status updates, friends list etc and I also want to see their full profile. I generally don't accept someone's friend request if I don't know the person.

### Are people more worried about privacy than they used to be?

The risk of having personal privacy breached is higher than before with everyone being more connected, but I am still fairly relaxed about the content that I post on my profile.

## BILL – BABY BOOMER

### What does privacy mean to you?

I try to respect someone's personal space, and this should be reciprocal. I would refrain from putting somebody in an uncomfortable position, especially in a public context.



### How do you keep your personal information safe online?

I prefer to have conversations via email rather than on Facebook. I don't like to share photos on Facebook without the permission of the people taken in the photograph.

### Are people more worried about privacy than they used to be?

I'm definitely more cautious, rather than worried. I really don't feel comfortable when somebody can Google my name and find out personal information about me.

## NAN BOSLER – PRESIDENT OF THE AUSTRALIAN SENIORS COMPUTER CLUBS ASSOCIATION (ASCCA) - SENIOR

### What does privacy mean to you?

It is very important that we all take responsibility for information we make available about others if we have not first sought their permission. The internet has a very, very long memory so it is good practice to think before you click.



### How do you keep your personal information safe online?

Because of my role with ASCCA many people know some general details about me but I try to be careful and not share any personal details. I select those I give my personal email or phone number to and think before posting on social networking sites.

### Are people more worried about privacy than they used to be?

I think that older people have become very concerned about privacy. Unfortunately many younger people become caught up in the excitement of use social networking sites and they tend not to think about the implications of what they display.

## IT'S YOUR INFORMATION, DON'T JUST GIVE IT AWAY

Below are some tips from the Privacy Commissioner, Timothy Pilgrim, to help you protect your personal information.

**ASK** yourself a few questions before you provide personal information, including information like your name, date of birth and where you live. Who else will see it and how will it be used?

**THINK** about how much personal information you reveal and to whom you reveal it. When you make lots of information about yourself public, you make it easy for identity thieves.

**CHECK** your privacy settings so you are aware of how your information is used. It's important to understand what someone else intends to do with your information, to choose who sees your information and to exercise your right to know what information is collected about you. You can also opt out of receiving marketing material if you choose to.

**READ** privacy policies to know how an organisation protects your information.

# HOW TO CREATE STRONG, SAFE PASSWORDS



Ensuring the security of multiple online accounts might seem like a big task, but it's really important you don't use the same password for everything. Data breaches of well-known websites are becoming more common, and using the same password across multiple accounts puts you at risk of cyber-criminals accessing your banking, social media, and other personal information. Here are some tips for creating strong, unique passwords that will keep your personal information safe online.

## DOs

**Use long passwords** They're harder to crack. Aim for eight or more characters.

**Use variety** The greater variety of characters in your password, the better. A strong password will include a combination of lower and upper case letters, a special character (e.g. \$, #, \*), and a numeral.

**Change your passwords regularly** Set an automatic reminder to change them every few months.

## DON'Ts

**Don't use the same password** for more than one account. If hackers are able to obtain your online password for one account, they can run software to try the same email/password combination for all your other accounts.

**Avoid using common words** that can be found in any English or foreign dictionary.

**Avoid words spelled backwards & common misspellings**  
e.g. koolpassword, retupmoc ('computer', backwards).

**Don't use sequences or repeated characters** e.g. 123ABC, qwerty.

**Don't use any of your personal information** even if it's easy to remember, e.g. your name, your or your family's birthdays, street name or your passport number.

## SOME CREATIVE SOLUTIONS TO KEEPING TRACK OF ALL YOUR PASSWORDS

Create a short phrase that you're likely to remember. For example, *John Smith will make 30 cakes on Friday*. Now, simply take the first character from each word to create your password, where the example would become *JSwm30coF*. Notice how there is a mixture of upper case, lower case, numerals, and just to be sure, you can put a special character at the end, to create *JSwm30coF\**.

Another example, *Alex Harris can eat 10 hot dogs only on Thursdays*, will become *AHce10hdooT*. Once again, adding a random, special character will add to the strength of your password, so this password becomes *#AHce10hdooT*. These types of passwords are extremely strong, as they are very long and don't use common English words.

You could also consider using password-management software. Depending on which software you choose, the basic idea is that the software will generate and manage your passwords for all your sites across all your computers. Some examples include LastPass, RoboForm Pro, or Sticky Password. But make sure that any password-management site you use is secure by reading their privacy policy.

This tip sheet and more are available online via [www.accan.org.au/tipsheets](http://www.accan.org.au/tipsheets)

# PRIVACY, INTERNET SERVICE PROVIDERS & DOWN- LOADING

The legal battle between Hollywood studios and internet service providers (ISPs) has ended with a decision in the much-publicised iiNet case. The Australian Federation Against Copyright Theft (AFACT) had argued that iiNet was guilty of authorising its customers to illegally upload or download movies. But the High Court said that, when presented with an allegation that one of their customers was illegally engaged in peer-to-peer file sharing, iiNet not doing anything about it does not mean that it was authorising copyright infringement.

In the wake of the decision, proposals still being considered by government and industry include some kind of “graduated response” scheme to try to stop consumers from peer-to-peer sharing of copyrighted material. That means warning and educational notices would be sent out once content owners provide evidence of infringement to ISPs. Content owners can only usually identify potential infringers by reference to a customer’s Internet Protocol (IP) address, so they rely on ISPs to find out which account holder has that IP address.

One proposal has ISPs handing over details of repeat infringers to content owners so the content owners can take legal action themselves. But this seems unlikely to happen in Australia any time soon. At present, none of the proposals floated in Australia by various parties involve disconnecting people from the internet. More likely would be an arrangement for ISPs or an independent body to send warning notices after they are presented with evidence by content owners – but without disclosing the account holders’ details to the content owners.

The toughest such scheme in existence is probably the so-called ‘three strikes’ procedure introduced in France. The third strike means suspending internet access for the offending internet connection for anywhere from two months to one year. The French Government established an agency, HADOPI (*Haute Autorité pour la Diffusion des Oeuvres et la Protection des Droits sur Internet*), which began sending out warning notices in October 2010.

HADOPI has the power to obtain customer details from ISPs. It doesn’t pass subscribers’ details to content owners, but rather to prosecutors in preparation for enforcement action on the ‘third strike’. This occurred for the first time in February 2012.

Other schemes are more respectful of consumer privacy. In the US, the new Copyright Alert System (CAS), involving the major ISPs, ensures that no personal information about a subscriber is passed to anyone without the subscriber’s express consent.

In New Zealand the three-strikes scheme, which was introduced in 2011, enables content owners to go to the Copyright Tribunal after the third notice – and ISPs are required to pass on account holder details to the Tribunal. Generally the minimum penalty is \$275 and maximum \$15,000, payable to the copyright owner. However, there are significant privacy implications because of what is in the notices. The date and time of an alleged infringement, along with the name and type of the work (e.g. a TV show or movie) will be included. Remember the notice goes to the account holder. Bearing in mind that internet connections are often shared by multiple individuals – family members, housemates, colleagues etc – there is potential for embarrassment, or worse.



# HIGH SPEED BROADBAND & HOUSEHOLD MEDIA ECOLOGIES

## The Project

Brunswick is a culturally diverse suburb in Melbourne with a growing population of new families and shared households. It is also a first-release site of the National Broadband Network, making Brunswick residents some of Australia's first high-speed broadband adopters.

An interdisciplinary team at the University of Melbourne is asking Brunswick residents to share their experience of how high-speed broadband access is changing their use of media and communications technologies at home. Surveying over 200 Brunswick households, the study will measure change over time as more premises connect to the NBN and residents adjust to their new higher speed connections.

## Household Media Ecologies

The way we connect with our world from home is changing as the media and communications landscape converges with services like video-on-demand and VoIP. The concept of 'media ecology' describes how we set up our devices, connections and software to interact in our home. The possibilities enabled by high speed broadband are likely to change the way we do business and the way we consume entertainment media – both part of the growing digital economy in Australia.

For example, the survey asks what media and communications devices are used and in which rooms. Early data suggests an unsurprising trend toward mobile devices, and the research will explore their role in household media ecologies.

The researchers are also exploring motivations and levels of satisfaction with current services in surveyed homes. The study will shed some light on the changing landscape of costs and benefits associated with different plans and bundles of services and will be looking at changes in household spending after connecting to an NBN service.

## What does this mean for you?

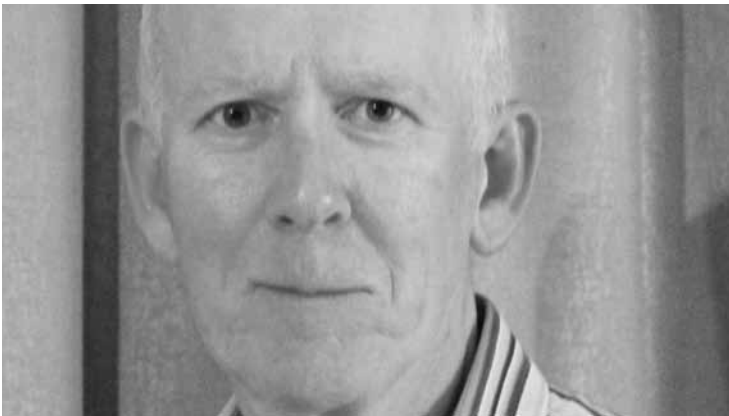
Many consumers still want to know what the NBN will do for them and what changes they can expect. A plain language resource will be developed that begins to unpack some of these questions for consumers and to scope changes that we might expect based on the experience of Brunswick's first NBN adopters.

*The report and consumer resource will be released in November 2012. To receive a copy of either publication, email [info@accan.org.au](mailto:info@accan.org.au).*

## About ACCAN Grants:

ACCAN awards \$250,000 annually to projects that align with our vision for available, accessible and affordable telecommunications for all Australians. Visit [www.accan.org.au/grants](http://www.accan.org.au/grants) for more info.

# AUSTRALIAN PRIVACY FOUNDATION



**NIGEL WATERS**  
BOARD MEMBER

## Tell us about the Australian Privacy Foundation.

The Foundation is a 'virtual' NGO of volunteer privacy advocates, and has been the principal voice for better privacy protection in Australia since it was formed to oppose the Australia Card in 1986.

## Why should Australians be concerned about their privacy?

Privacy is a fundamental human right, and privacy laws also provide tools for individuals to use to protect themselves against arbitrary, unfair and unwelcome intrusion and treatment. Many recent examples of large-scale data security breaches illustrate the dangers associated with the ever-growing databases of personal and often highly sensitive information.

## What are the biggest privacy issues affecting Australians today?

We all deserve better protection from the seemingly remorseless development of a 'surveillance society' in which governments and businesses know more about us than they need to, and more than is healthy in a liberal democracy. There are many benefits from data sharing and matching, but also great potential for error and harm. E-commerce, social media and technologies such as face recognition and other biometrics are creating new challenges, and both the privacy laws and the various Privacy Commissioners are lagging well behind. Recently introduced amendments to the Commonwealth Privacy Act are not all welcome – some further weaken the already inadequate protection, and governments at all levels continue to allow far too many exemptions.

## Do you have any suggestions for someone wanting to protect their privacy?

We should all challenge organisations which ask us for personal information as to why they need it and what they intend to do with it, and say 'no' more often. But power imbalances, and information overload, often make it impracticable for individuals to resist, so we should also lobby our elected representatives to set more limits, and to provide more effective monitoring and enforcement of privacy law.

## Why is the Australian Privacy Foundation a member of ACCAN?

Privacy of communications is particularly important, and increasingly so as more of our daily life is conducted over telecommunications networks – online commerce and banking, mobile payments, smart utilities, etc. While there are more limits on who can obtain access to the content of voice, email, texts and other communications, there are far weaker controls over how 'traffic data' can be used. ACCAN is an important player in policy debates on these issues and APF values our longstanding cooperation with ACCAN (and its predecessor CTN) in these debates.

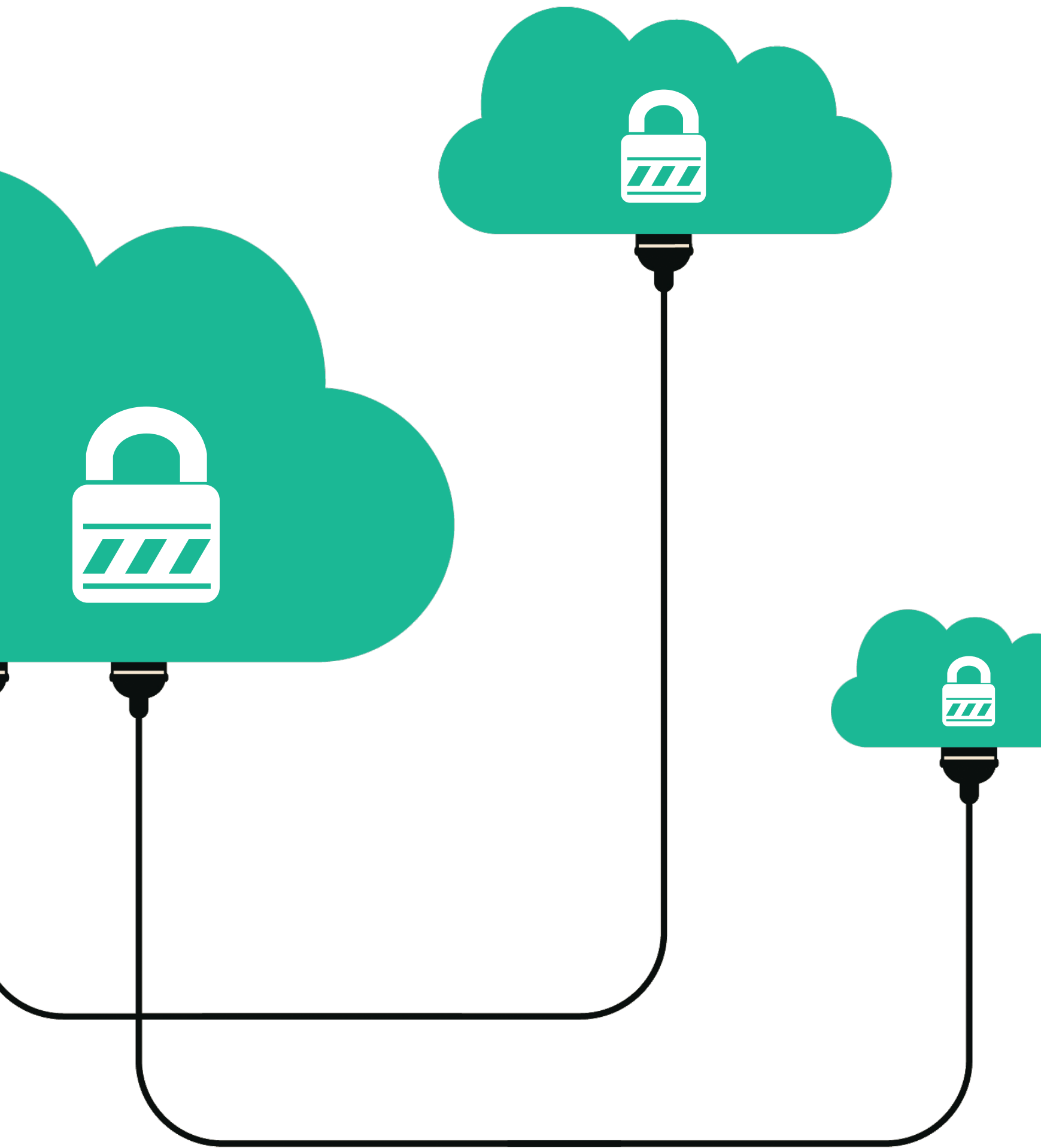
Australian Privacy Foundation website: [www.privacy.org.au](http://www.privacy.org.au)  
Contact Nigel: [board5@privacy.org.au](mailto:board5@privacy.org.au)

## AND MEET A NEW MEMBER



**International Copper  
Association Australia**  
Copper Alliance

**The International Copper Association Australia** – previously known as the Copper Development Centre – is a global Copper Alliance member and the peak copper industry body in the Oceania region. ICA.Australia helps to identify and support new uses for copper across a broad range of areas, and in particular smart building technologies like the Smart Wiring™ initiative it established with a number of leading telecommunication partners.







Register online  
via [regonline.com.  
au/delivering](http://regonline.com.au/delivering)  
Book before  
July 31 to receive  
an earlybird  
discount

# 2012 ACCAN NATIONAL CONFERENCE

5-6 SEPTEMBER  
UTS AERIAL FUNCTION CENTRE, SYDNEY

## DELIVERING FOR CONSUMERS

**accan**

Australian Communications  
Consumer Action Network