Australian National University

WORKSHOP SUMMARY

HC Coombs Policy Forum and Charles Sturt University

Social Media, Privacy and Security:
Identifying and managing the public policy risks.
A scoping workshop, 11 March 2011

Objectives

The objectives of the workshop were to:

> identify the privacy and security risks associated with social media and how best to manage these risks

> develop an agenda for evidence-based research that will assist government agencies to navigate the opportunities and challenges of social media

Presenters

Associate Professor Nick O'Brien, Centre for Policy Innovation, The Australian National University and Professor of Counter Terrorism, Australian Graduate School of Policing, Charles Sturt University

Dr Robert Ackland, Australian Demographic and Social Research Institute, The Australian National University

Adjunct Professor Mick Keelty, Centre for Policy Innovation, The Australian National University and Australian Graduate School of Policing, Charles Sturt University

Dr Mark Matthews, Executive Director of the HC Coombs Policy Forum, The Australian National University

Panelists

Mr John Sheridan, First Assistant Secretary, Australian Government Information Management Office

Dr Abbas Bigdeli, Senior Researcher and Project Manager, Advanced Surveillance Project, National ICT Australia

Professor Simon Bronitt, Director, Australian Research Council Centre of Excellence in Policing and Security (CEPS), Griffith University

Main themes

The main themes to emerge from the workshop were:

> there is a need to understand the risks to privacy and security posed by converging technologies

> developments in the area of social media are happening quickly and it is difficult to keep up with current developments, let alone predict future developments

> privacy concerns have the potential to diminish the value of social media to business and government

> little is known about people's attitudes to online privacy risks and how their attitudes affect their behaviour

> there is a lack of research in this area and more research is needed to understand the implications and identify ways of managing the risks.

First session: context and scene setting

Social media and information security: identifying and managing risk in a connected world

Associate Professor Nick O'Brien

This presentation focused on the information security implications of the following converging technologies:

- huge recent growth in social media and the practice of uploading and sharing photos on social media sites
- the use of facial recognition software in diverse contexts including marketing and photo tagging
- the increasing penetration of mobile devices such as smartphones and applications like foursquare – a location-based social networking site that enables users to interact with their environment
- huge increases in computing capacity.

Associate Professor O'Brien cited a range of statistics to illustrate the pervasive influence of Facebook as well as other social media sites such as Twitter and Foursquare (for more details, see Appendix 1). For example:

- Facebook was valued at $50 billion in the 7 years since starting up and in April 2011 was valued at $65 billion
- in 2010 Facebook announced that it had reached half a billion users (active users, using Facebook at least once a month)
- 100 million photos are uploaded each day, and even people who are not Facebook users can appear on Facebook in other people's photos
- users average 130 friends each
- Warner Bros is interfacing with Facebook to provide 48 hour windows to see a movie, three dollars a viewing
- President Obama referred to Americans as people of Facebook and Google in his 2011 State of the Union address
- smart phones are becoming ubiquitous and can pinpoint the user's location at any given time, including when taking a photograph
- 10,000 websites join Facebook every day – 3.65 million new websites
- more people now play games on Facebook than on combined other platforms such as X box, Wii etc
- there are now over 200 million Twitter users – around 30 million new users joined just in the two-month period September–October 2010
- there are 7.5 million foursquare users and 90 million LinkedIn users.

Another issue raised in this presentation was the use of mobile devices to access social networking sites like Facebook. Mobile devices, like social media, are being widely adopted at a fast rate. Facebook will be focusing on the mobile device market in 2011.

The rapid development of facial recognition software also has privacy and security implications. Such software can be used to identify people from photos (such as those uploaded onto social networking sites) and may be used to make tagging photos easier. Software such as iPhoto uses facial recognition software to help organise photos and Google is now adding this to its Picasa photo-sharing software.

Huge increases in computing power and different ways of accessing computing resources (such as cloud computing) provide much greater capacity to process huge amounts of data, as would be required to quickly search for people's faces on the internet, for example.

Web 2.0: context, uptake and implications

Dr Robert Ackland

This presentation considered:

- people's motivations for using social media
- the value to business and government of social media
- how privacy and security concerns might reduce the value of social media to business and government
- the need for research in this area given the lack of existing data on these phenomena.

Dr Ackland described his field of study as the interface between network science and web science. He explained that social media use leads to **vast digital repositories of searchable content** such as web pages, blog posts, newsgroup posts, Wikipedia entries. Such repositories can be thought of as **information public goods** that have economic value to business because they enable people to find information efficiently – for example, by using Google to search for answers to technical questions. For governments, the value of social media lies in the **potential for direct dialogue between citizens and government**, promoting participatory democracy (that is, broader participation in the direction and operation of government).

However, people are often not involved in social media for the instrumental reasons of creating information public goods or strengthening democracy but for social reasons and to express their individual or collective identity. Much of the time **people's use of social media is expressive** (like voting, or cheering at the football) **rather than instrumental** and people tend to be intrinsically motivated to participate – that is, for the inherent enjoyment of the activity – rather than being extrinsically motivated (for example, by the expectation of external rewards).

The presentation identified two issues that may reduce the value of social media to business and government by adversely affecting people's motivation to participate.

1. Game mechanics, was not covered in detail but refers to the use of rewards such as badges on foursquare, which may encourage some users but deter others, so may have the effect of selecting particular types of users to participate, and may also change the way in which people engage with online environments.

2. Privacy. The second issue identified as potentially diminishing people's motivation to participate in social media, and the issue of particular relevance in the context of this workshop, was privacy. Existing research is mostly survey research focusing on a particular demographic: youth. eg

- Sonia Livingstone found that younger teenagers use social media for creating 'identity through display' while older teenagers create 'identity through connection'. Different risks are associated with each of these behaviours.
- Zeynep Tufecki's quantitative study of US college students looked at how privacy concerns affect students' willingness to disclose information online. This research suggested that 'treating privacy within a context merely of rights and violations, is inadequate for studying the Internet as a social realm'. Full details of these journal articles are provided in Appendix 1.

Further research needed. Most existing research has focused on youth in wealthy countries but there is a need for research on other demographic groups. For understanding how people's participation in Government 2.0 might be affected by privacy and security concerns, for example, it will be important to include demographic groups more relevant to these initiatives as youth tend not be involved in political activities online.

Dr Ackland drew attention to a study of older Australians and their social media use (funded by an ARC Linkage Grant) being undertaken by the Australian Demographic and Social Research Institute at The Australian National University in partnership with National Seniors Australia. He noted that research into privacy and Government 2.0 is generally not based on data and is mainly speculation at this stage. Little is known about people's attitudes towards the potential for governments to use their data for purposes other than policymaking, such as surveillance and law enforcement.

Developments in network science and mining social graphs (that is, the social connections between people or organisations). Social media use leads to digital traces of activity that are permanent, searchable and cross-indexable. The presentation highlighted some research drawing on the online behaviour of people or groups (such as Australian groups focused on abortion, or US political bloggers) illustrating how people (or organisations) sort themselves into groups by linking to like websites. (Full details of the research presented are provided in Appendix 1.) New tools are being developed to support this type of research through data mining, network visualisation and analysis, including:

- the Virtual Observatory for the Study of Online Networks (VOSON) System (http://voson.anu.edu.au) developed by Dr Ackland
- SAS Social Media Analytics
- NodeXL, which enables social network data such as that gathered by VOSON to be imported into Excel.

It was noted that there is an important difference between individual privacy and social graph security. Network scientists increasingly have the ability to mine social graphs and place people in groups by identifying clusters in

social networks and predicting the existence of social connections. Protecting the social graph is more important – and more difficult – than protecting personal data.

Dr Ackland concluded by drawing attention to the Master of Social Research course run by the Australian Demographic and Social Research Institute at the Australian National University. The Social Science of the Internet specialisation taught by Dr Ackland as part of this course covers the interface between network science and web science as well as tools and methods for conducting online research.

Panel discussion

Mr John Sheridan, Dr Abbas Bigdeli, Professor Simon Bronitt

Mr Sheridan talked about the push from the Australian Government to use social media to get a range of benefits and referred to the Declaration of Open Government made in July 2010. Releasing datasets to make information more accessible is part of this initiative.

Government is increasingly using social media to seek information from individuals and industry. The initial response from public servants has been slow but is gradually increasing.

Social media is being successfully used to quickly correct information in the public domain that is incorrect. Public servants can comment in their professional capacity and their contribution to debates can be picked up quickly by the media.

Mr Sheridan suggested that the challenges raised earlier in the workshop about identifying people actually make the security job easier in some ways. He also noted that no amount of technology can address the issue of security breaches by individuals, for example by leaking – firewalls cannot stop someone photocopying material and carrying it out of the office.

Dr Bigdeli talked about the third generation of video surveillance technology, in which each camera is a website and in theory could be accessed anywhere in the world.

He described the huge increases in computing power over recent decades by noting that the computing power of the iPhone is equivalent to a supercomputer of 30 years ago.

Dr Bigdeli also mentioned that there are ways of tracking identity using poor quality images, eg from video surveillance and that not only face recognition, but clothing and gait can be used to track identity across multiple surveillance networks. He also referred to iris-on-the-move technology. He said these technologies have both customs hall and street use.

Professor Bronitt drew attention to the work of the Centre of Excellence in Policing and Security (CEPS), which is a research partnership between The Australian National University, Griffith University, The University of Queensland and Charles Sturt University. The Centre also brings together a range of industry partners (refer to the CEPS website for a full list) who are committed to innovation and evidence-based research in policing and security.

The Centre's goal is 'to gain a better understanding of the origins, motivations and dynamics of crime and security threats. Its objectives are to create significant transformations in crime, crime prevention and security policies, and to bring about evidence-based reform in the practices of policing and security to enhance Australia's social, economic and cultural wellbeing.'

Professor Bronitt discussed the issues of vulnerability and resilience. In relation to infrastructure, he noted that much vulnerable infrastructure is in the hands of private companies and it will be necessary to engage with policymakers and private companies before starting research.

He noted that social media can make you vulnerable but also resilient. For example, in the Brisbane floods social media was used for self-organising.

Professor Bronitt referred to the speed of developments in the area of social media, observing that social media catches every strategist and futurologist off-guard. He sees a key role for 'foresight forums', which have not previously been used in Australia much.

He said that as a criminal lawyer he sees that some of the issues are regulatory and legal ones. Laws and regulations don't yet cover all aspects of what is now appearing in social media – eg video. He noted that privacy in the modern context clearly goes into the realm of the public – physically and virtually – related to human dignity. Social media has no borders but laws are tied to territory, so addressing interjurisdictional issues poses significant challenges.

Social Media and Information Security: Identifying and Managing Risk in a Connected World
Adjunct Professor Mick Keelty

Adjunct Professor Keelty's presentation started by asking: **Is the rise of social media a problem?**

He identified some of the concerns for **covert policing:**

- the increasing difficulty of protecting assumed identities for undercover police and in the witness protection program
- occupational health and safety
- the implications for the cost to government of these programs.

Adjunct Professor Keelty presented some results from a survey that he and his colleagues are undertaking to understand the social media exposure of new police, intelligence and other related recruits and the associated identification risks. Some of the survey results relating to social media usage were, for example:

- 85 per cent of respondents were using at least one of the listed social network sites (90 per cent for women, 81per cent for men)
- Women aged between 45-65 did a lot of photo-sharing, emulating their role in the real world
- The use of social network sites was much higher among younger people
- The majority used one or two social network sites
- Facebook was overwhelmingly the most popular social networking site, used by 86 per cent of female recruits and 74 per cent of male recruits.

The survey also addressed issues more specifically related to the risk of identification. For example:

- 85 per cent of respondents said someone else had uploaded their photograph
- 42 per cent thought it would be possible to identify their relationship with others on the internet
- 23 per cent thought it would be possible to identify their network of associates by surfing the internet
- 21 per cent thought it would be possible to associate their personal details with their photo on the internet; another 36 per cent had not checked or were not sure
- Only a small percentage (16 per cent had considered the implications of facial recognition software
- 28 per cent said their survey answers had caused them to be concerned about their profile on the internet.

It was noted further that:

- Facebook is not a publicly listed company and they own any photographs on Facebook – so who can be asked to remove photos?
- There is data showing that over a five year period the average amount of time young people in the US spent consuming media increased by over an hour a day, mostly due to the widespread adoption of mobile devices.

The presentation looked at examples of how personal details that people had disclosed on the internet had been exposed, and some of the websites that enable this, for example by enabling people's whereabouts to be tracked via their phone number. The ability to source so much information about a person and their family from the internet raises other concerns, for example:

- the security of people such as immigration officers dealing with difficult cases
- disclosure of location information on the internet by individual defence force personnel could jeopardise national security
- evidence of past misbehaviour could be used to embarrass people in later life, eg Google Chief Executive Eric Smith's advice to people who were concerned about this to 'change your name' was irrelevant as facial recognition technology would enable people to be identified anyway
- the risks of a particular Facebook feature, Facebook Groups. Such groups may expand to include people that other members don't even know, including the person who started the group
- the use of Facebook by government was also questioned – while government websites are strictly regulated, private websites like Facebook are not.

Adjunct Professor Keelty's presentation concluded with a list of other issues:

- matters before courts involving family law and apprehended violence orders
- further testing of witness credibility based on social network entries
- subversion of anti discrimination legislation
- witness credibility and jury selection
- aborting of trials where material posted on social networking sites
- loss of privacy for public officials (and all citizens)
- Brand/reputation damage
- people tracking (juries, witnesses, officials)
- increased security risks/public safety
- risks associated with financial institution security checks – date of birth, favourite pet, mother's maiden name etc
- Gen Y and younger have a different attitude to privacy
- issues are building (eg consider a 15 year old today and their level of exposure by 2016).

Implications for public policy
Dr Mark Matthews

Dr Matthews talked about **the geo-strategic implications of social media**. He noted that:

- in this innovation environment there is a lot of potential for illicit activity and suggested that OECD nations are not really keeping up with this
- potential for a Richardson process or "arms race" between the illicit and licit domains as each tries to keep ahead of the other
- a whole of government response is needed to these geopolitical issues and that it will be important to raise awareness, as well as identifying problems and responses
- legislation at the national level would not be sufficient and that international responses would be required.

Second session: Workshop discussion

Points made from the floor in discussion responded to the presentations outlined above and also ranged widely in subject and point of view. They have been left as individual remarks to capture the range of viewpoints. They have been grouped here under four themes: identity and privacy; legislation and regulation; education and public awareness of risk; and policing and security.

Identity and privacy

Some comments placed the debate in a broader cultural and historical context and question how big a problem social media really is to individuals:

- Different countries have different values – eg in content regulation. Privacy, content and identity are linked issues in user-generated content. There are varying community attitudes about materials going up on the web.
- The distinction between public and private life is dated. There is the capacity for private data to be used to access your public life capacity and a blurring of work device and private device. If you put facial recognition on top of that, there are huge implications.
- Perhaps in general social media is not a problem for society at large.
- It is like a return to village life where everyone knew everything about everyone. This is an interim period.
- One observer was struck by the idea of identity and culture. Thinking of Venice and masks, or the Islamic burkha – identity masking may once again be necessary in this new environment.

Other comments reinforced earlier concerns for the protection of people's identity and privacy:

- If we know there is a risk and threat we need some response, and the commonsense approach is: how do we mitigate the negative effects? Online identities are like virtual tattoos – still there 20 years later.
- A lot of what is going on now is happening to people beginning their careers, not prominent people and information about their activities and preferences, eg what books they read when they were younger, can affect their recruitment. There are risks that doors get closed. Think about tomorrow's politician, CEO of an organisation, is this what we want?

- We all have multiple identities. There is a risk that where you appear the most is what others think you are the most – which may not be actually the case. There is the potential for misinterpretation of people's online representation. People can present multiple identities in various areas of their lives, as a normal thing – analytics is forcing one identity for each person and it tends to be the worst identity.

Legislation and regulation

- Traditional methods of regulation and international agreement won't work – eg child pornography – 94 countries have not signed.
- We can still assume that it is easier to build up international consensus on what is bad – can start to build up momentum for an international approach.
- Can't hold industry back with regulation when they have global competitors. Need to have industry on board. If industry does not cooperate nothing will happen. Microsoft and now Google have become more concerned about these things than used to be. Big stick can't work.
- Potential for legislation – adhered to by those willing to do so. Large criminal networks have already been allowed to become very strong – need affirmative action against those groups before any legislation.

Education and public awareness of risk

- Changing the concept of trust – strong blurring of private and public trust. Average person is naïve of the consequences. Regulation does not work, eg cannabis and heroin – regulation has not been a success. Education is more important than regulation.
- When do you do regulation, when education? Behavioural issues are really hard to deal with by regulation, eg cyber stalking and bullying. How do you decide what tools to use for what problems?
- People need a driver's licence for the internet.
- Education – general community information about the risks is not that good.
- We need to give people more control tools for it. People are learning to balance public and private domains, people choose to get involved in social networks, quite deliberately.

Policing and security

- Security clearances – will processes for recruiting the average public servant change if something you did ten years ago shows up which you have forgotten about?
- Seeing a picture on the net may be more accurate than what people write into security applications.
- New techniques in place of covert operations can be used and developed. How do we change our practices to fit this new world rather than trying to fit it back into old boxes?
- Niche area was undercover policing. Is it dead? It is at least increasingly difficult.
- Difficulty of intelligence and policing identity when you can have back-to-childhood photos.
- We are in a new world – best we can do with crooks is to try to catch up.
- Policing issues are real and costly for government. These things are happening now. People are putting their lives on line – with what long term effects?
- Policy of Public Service Commission in relation to public servants being more available and known online – are they protected? Response: Agencies that have those concerns are less likely to have their staff publicly available.
- Naivety – IT people often feel they have a policing role in a department – when it is not their job.

Where to from here?

- There is a lot of unfinished business here.
- There is a lot of potential for people to be disadvantaged quite critically.
- The challenge is having the research knowledge, wisdom and judgement to harness the opportunities and deal with negatives.

Appendix 1 – Useful references

The following references include those cited in workshop presentations as well as other selected references that may be of interest.

ABC (2011). Can social media compromise crime fighting?, accessed 28 April 2011.

Australian Communications and Media Authority (2010). Trends in media use by children and young people: Generation M2 2009 (USA), and MCAF 2007 and CPCLA 2009 (Australia). Retrieved from http://www.acma.gov.au/scripts/nc.dll?WEB/STANDARD..PC/1001/pc=PC_312174, accessed 28 April 2011.

Asia Pacific futuregov (2010). Will Facebook profiles replace govt web sites? Retrieved from http://www.futuregov.asia/articles/2010/mar/19/will-facebook-replace-govt-web-sites/, accessed 28 April 2011.

BBC (2010). US Air Force warns Facebook 'may reveal location'. Retrieved from http://www.bbc.co.uk/news/world-us-canada-11782352, accessed 28 April 2011.

BBC (2010). Facebook hits 500m user milestone. Retrieved from http://www.bbc.co.uk/news/technology-10713199, accessed 28 April 2011.

CNN (2011). Report: Egyptian dad names child 'Facebook'. Retrieved from http://edition.cnn.com/2011/WORLD/meast/02/21/egypt.child.facebook/

Daily Telegraph (2010). Facebook trials 'facial recognition' technology to make tagging photos easier. Retrieved from http://www.telegraph.co.uk/technology/facebook/7868875/Facebook-trials-facial-recognition-technology-to-make-tagging-photos-easier.html, accessed 28 April 2011.

Daily Telegraph (2010). Facial recognition software to go public. Retrieved from http://www.telegraph.co.uk/technology/news/7958511/Facial-recognition-software-to-go-public.html, accessed 28 April 2011.

Facebook Penetration by country. Retrieved from http://www.economywatch.com/economic-statistics/economic-indicators/Facebook_Penetration_Rate/, accessed 28 April 2011.

Facebook Press Room Statistics (2011). Retrieved from http://www.facebook.com/press/info.php?statistics, accessed 28 April 2011.

Gartner (2010). Gartner Highlights Key Predictions for IT Organizations and Users in 2010 and Beyond. Retrieved from http://www.gartner.com/it/page.jsp?id=1278413, accessed 28 April 2011.

Gartner (2010). Gartner Says Social-Networking Services to Replace E-Mail as the Primary Vehicle for Interpersonal Communications for 20 Percent of Business Users by 2014. Retrieved from http://www.gartner.com/it/page.jsp?id=1467313, accessed 28 April 2011.

Government 2.0 Taskforce Report (2009). Retrieved from http://www.finance.gov.au/publications/gov20taskforcereport/index.html, accessed 28 April 2011.

Huffington Post (2011). My dad un-friended me on facebook – baby boomers and social media, Retrieved from http://www.huffingtonpost.com/meagan-johnson-and-larry-johnson/babyboomers-facebook-_b_853756.html, accessed 28 April 2011.

Livingstone, S (2008) Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. New media & society, 10(3), pp. 393-411.

Magid, L (2010). Facebook Groups Can Jeopardize Privacy. Retrieved from http://www.cubagreenscreen.com/forum/showthread.php?tid=10731, accessed 28 April 2011.

Mail Online (2011). MI6 chief blows his cover as wife's Facebook account reveals family holidays, showbiz friends and links to David Irving. Retrieved from http://www.dailymail.co.uk/news/article-1197562/MI6-chief-blows-cover-wifes-Facebook-account-reveals-family-holidays-showbiz-friends-links-David-Irving.html#ixzz1KmVfGmb7, accessed 28 April 2011.

Mail Online (2011). Minority Report-style shopping? The billboard that profiles you and then flashes up ads tailored to your tastes/ Retrieved from http://www.dailymail.co.uk/sciencetech/article-1361490/Minority-Report-style-shopping-The-billboard-profiles-flashes-ads-tailored-tastes.html, accessed 28 April 2011.

Mail Online (2010). The facial recognition software that will put a name to every photograph in the internet. Retrieved from http://www.dailymail.co.uk/sciencetech/article-1305191/Facial-recognition-software-allow-ability-identify-people-photographs-internet.html, accessed 28 April 2011.

Mail Online (2011). Saucy Facebook-style party picture comes back to haunt Congresswoman four years later. Retrieved from http://www.dailymail.co.uk/news/article-1345253/Facebook-style-party-picture-haunts-Congresswoman-Mary-Bono-Mack-4-years-later.html#ixzz1KmU88GY6, accessed 28 April 2011.

Mail Online (2010). Special investigation: It took just one hour for internet experts to find out almost every private detail of this woman's life. Retrieved from http://www.dailymail.co.uk/news/article-1310965/Special-Investigation-It-took-just-hour-internet-experts-private-womans-life.html, accessed 28 April 2011.

Mashable (2010). A Glimpse at the Future of Foursquare. Retrieved from http://mashable.com/2010/11/03/future-of-foursquare/, accessed 28 April 2011.

Mashable (2010). 10,000 Websites Integrate with Facebook Every Day. http://mashable.com/2010/10/26/10000-websites-integrate-with-facebook-every-day/, accessed 28 April 2011.

Mashable (2010). Facebook Brings Facial Recognition to Photo Tagging. Retrieved from http://mashable.com/2010/12/15/facebook-photo-tag-suggestions/?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+Mashable+%28Mashable%29, accessed 28 April 2011.

MEMRI TV (2011). Excerpts from an address by Seif Al-Islam Al-Qadhafi, the son of Libyan leader Mu'ammar Al-Qadhafi. Retrieved from http://www.memritv.org/report/en/5027.htm, accessed 28 April 2011.

NetworkWorld (2011).Facebook unveils security tools after Zuckerberg's page hacked. Retrieved from http://www.networkworld.com/news/2011/012611-facebook-security-tools.html, accessed 28 April 2011.

NetworkWorld (2010). HPC experts look past petaflop to the exascale. Retrieved from http://www.networkworld.com/news/2010/111810-hpc-exascale.html, accessed 28 April 2011.

Obama, B. (2011). Remarks by the President in State of Union Address. Retrieved from http://www.whitehouse.gov/the-press-office/2011/01/25/remarks-president-state-union-address, accessed 28 April 2011.

PC World (2010). The Facebook Data Torrent Debacle http://www.pcworld.com/article/202167/the_facebook_data_torrent_debacle_qanda.html, accessed 28 April 2011.

PEW Internet (2010). Reputation Management and Social Media, Retrieved from http://www.pewinternet.org/Reports/2010/Reputation-Management/Part-2/Managing-identity-through-social-media.aspx, accessed 28 April 2011

Slyvisions (2011). Facebook Users Uploaded 750 million Photos On New Year's Eve. Retrieved from http://slyvisions.com/2011/01/04/facebook-users-uploaded-750-million-photos-on-new-years-eve/, accessed 28 April 2011.

Sydney Morning Herald (2010). Google on privacy: change your name. Retrieved from Sydney Morning Herald http://www.smh.com.au/technology/technology-news/google-on-privacy-change-your-name-20100817-127xj.html, accessed 28 April 2011.

Sydney Morning Herald (2011). Spy on your kids' Facebook without being their friend. Retrieved from http://www.smh.com.au/technology/security/spy-on-your-kids-facebook-without-being-their-friend-20110427-1dw6k.html#ixzz1KmgUHBaY, accessed 28 April 2011.

TechCrunch (2010). Foursquare Hits 2 million check-ins, 25K New Users Daily. Retrieved from http://techcrunch.com/2010/12/08/foursquare-hits-2-million-check-ins-25k-new-users-daily/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Techcrunch+%28TechCrunch%29, accessed 28 April 2011.

TechCrunch (2009). Picasa Adds Facial Recognition And Geo-Tagging To Its Desktop App. Retrieved from http://techcrunch.com/2009/09/22/picasa-adds-facial-recognition-and-geo-tagging-to-its-desktop-app/, accessed 28 April 2011.

TechCrunch (2010). Twitter Added 30 Million Users In The Past Two Months. Retrieved from http://techcrunch.com/2010/10/31/twitter-users/, accessed 28 April 2011.

Tufekci, Z (2008). Can you see me now? Audience and disclosure regulation in online social network sites. Bulletin of Science, Technology and Society 28:1, pp. 20-36.

Mashable (2010). Stipple Secures $2 Million to Build Photo Tagging Tools for Publishers. Retrieved from http://mashable.com/2010/11/18/stipple/?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+Mashable+%28Mashable%29, accessed 28 April 2011.

World Facebook connections (2010). Retrieved from http://mashable.com/2010/12/13/facebook-members-visualization/?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+Mashable+%28Mashable%29, accessed 28 April 2011.

Yahoo Finance (2011). Apple slammed over iPhone, iPad location tracking, accessed 28 April 2011.

Contact

Paul Harris
Deputy Director
HC Coombs Policy Forum
The Australian National University

T +61 2 6125 6983
E paul.harris@anu.edu.au

The Australian National Institute for Public Policy and the HC Coombs Policy Forum receive Australian Government funding under the 'Enhancing Public Policy Initiative'.