THE LAW SOCIETY OF NEW SOUTH WALES
young LAWYERS

Communications, Entertainment & Technology Law Committee

Cyber White Paper

Connecting with Confidence – Optimising Australia's Digital Future

14 November 2011

Submission to the Department of the Prime Minister and Cabinet

NSW Young Lawyers
Communications, Entertainment & Technology Law Committee
170 Phillip Street
Sydney NSW 2000
www.younglawyers.com.au

About NSW Young Lawyers

NSW Young Lawyers is a division of the Law Society of New South Wales. Membership of NSW Young Lawyers is free and automatic for all NSW lawyers under 36 years and/or in their first five years of practice, and law students. Membership of its committees is voluntary.

The Communications, Entertainment & Technology Law Committee (CET) aims to serve the interests of lawyers, law students and other members of the community concerned with areas of law relating to:

- information and communication technology (including technology affecting legal practice);
- intellectual property;
- advertising and consumer protection;
- confidential information and privacy;
- entertainment; and
- the media.

As innovation inevitably challenges custom, CET promotes forward thinking, particularly about the shape of the law and the legal profession as a whole.

Contributors to our written submission included Stephen Chang, Ahmed Abbas, Leah Egiziano, Patrick Gardner and Matthew Tracey.

If you have any questions about our submission, please contact Heidi Fairhall, President of NSW Young Lawyers, at president@younglawyers.com.au or alternatively, Ju Young Lee, Chair of CET, at cet.chair@younglawyers.com.au.

Ju Young Lee
Chair, Communications, Entertainment & Technology Law Committee
NSW Young Lawyers

1. Introduction

1.1. We thank the Department of the Prime Minister and Cabinet for the opportunity to participate in an open discussion on how the government, industry and the community can work together to address the challenges and risks arising from greater digital engagement.

1.2. Our submission briefly addresses:

- suggested approaches for improved online security and resilience;
- a model of Internet governance that is in the best interests of all Australians;
- how to achieve a balance between Australia's social, economic and security needs when developing an Australian vision for the online environment;
- approaches to be taken to develop agreements on behaviour in the online environment; and
- new forms of government-industry cooperation and dialogue that are required to ensure the Australian cyber skills base is developed to meet Australia's broader national interests.

2. Security and resilience in the online environment

ISSUE: Much of the public discussion on cyber threats and risks to date has focused on national security issues. This important dimension has inadvertently hidden the reality that at its most basic level, security and safety online is reliant on the awareness of individuals. As a result, many businesses and consumers are not as mindful of cyber threats as they could be.

QUESTIONS:

(a) How can the Commonwealth, states and territories and industry effectively communicate the interdependent nature of individual and national cyber security? How can the importance of individual behaviour be highlighted in creating a secure, trusted and resilient online environment for all Australians?

(b) How can citizens better protect themselves from cyber threats?

(c) Are individuals adequately aware of cyber threats and the steps they should take to protect themselves? If not, why not?

Introduction

2.1. The Internet creates a limitless virtual world where participants are innately anonymous. This environment challenges the sovereignty of nation states, not only beyond their borders, but also within their borders.

2.2. The Internet hosts a thriving community of "netizens"[1]. A user's existence may be online only or predominantly offline. The online community includes social networkers, telecommuters, collaborators, shoppers, governments, entertainment seekers, information seekers, information disseminators, activists, dissidents, fraudsters and organised criminal syndicates.

2.3. According to the 2011 Norton Cybercrime Report[2], 24% of online adults consider that they cannot live without the Internet and 32% of social network users think they would lose contact with friends if they had to live without their social networks.

2.4. In Britain, the digital component of the economy is responsible for 10% of national production. Ninety per cent of retail purchases are transacted by credit/debit cards with the communications infrastructure of the digital economy. £50 billion of consumer purchases and sales occur entirely online[3]. These trends are being mirrored in Australia.

2.5. According to the British Cyber Security Operations Centre, by 2015, high-speed Internet access will be essential to everyday life, service interruptions will seriously

---

[1] Jay Hauben, 'On the History and Impact of the Net', <http://www.columbia.edu/~hauben/netbook/> at 3 November 2011.
[2] http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport/ at 8 November 2011
[3] Department for cuture, media and sport, '*Digital Britain : The Final Report*', (2009) < http://www.official-documents.gov.uk/document/cm76/7650/7650.pdf> at 3 November 2011.

impact the economy and public wellbeing. Unavailability of the Internet will stop people from purchasing goods and services, limit access to conduct financial transactions and curtail communications with family and friends. In an emergency, a lack of Internet access will limit the ability of people to access up to date information and co-ordinate their response appropriately[4].

Recent Trends

2.6. Software vendors and solutions providers provide storage, infrastructure and application services in 'cloud' infrastructures[5]. Concerns about such offerings include the cross jurisdictional nature of the offerings where data is distributed globally, the potential loss of data and the inability to control data. An advantage of these solutions for SMEs is they may gain access to an offering providing a security configuration, scalability and replication capability that might normally be beyond their skills, capability or budget.

2.7. Mobile devices are becoming increasingly important in the digital economy. These devices give their users the ability to access data anytime and anywhere. The first iPad was released in April 2010 and over 30 million have been sold. In Apple's Third Quarter Report, the sale of 9 million iPads during that quarter represented a 183 percent increase in sales. There are more mobile phones in Australia than people, 78 percent of households have computer access and 72 percent have Internet access[6].

2.8. Social networking is growing exponentially and is significantly impacting the way people communicate. It has been estimated that 'about half' of the Internet users in Australia are on Facebook. Social networking presents a ready source of personal data exposing Australians to fraud and identity theft. Alternatively a drive-by download may incorporate the individual as an unsuspecting participant in a botnet.

2.9. Social networking presents particular threats to children. Facebook has over 800 million active users: less than 12 percent are less than 18 years old and more than half are over 35 years old (although the fastest growing age group is between 40 and 60 years old.) Studies suggest that young people and adults use this technology in different ways. Dr McGrath concluded that adults do not organise their social lives using social networking sites, and often fail to understand this use of technology[7]. Parents in the US actively flout the Children's Online Privacy Protection Act and lie about their children's date of birth to enable them to join social networking sites[8].

What is security?

2.10. Security includes the physical and virtual protection of Internet infrastructure. It also includes the protection of personal data, market sensitive data, confidential information and data that may compromise national security.

---

[4] Peter Sommer (Information Systems and Innovation Group - London School of Economics) and Ian Brown (Oxford Internet Institute, Oxford University), '*OECD/IFP Project on 'Future Global Shocks' : 'Reducing Systemic Cybersecurity Risk*', (2011) <http://www.oecd.org/dataoecd/57/44/46889922.pdf> at 2 November 2011.
[5] Peter Sommer (Information Systems and Innovation Group - London School of Economics) and Ian Brown (Oxford Internet Institute, Oxford University), 'OECD/IFP Project on *'Future Global Shocks' : 'Reducing Systemic Cybersecurity Risk*', (2011) <http://www.oecd.org/dataoecd/57/44/46889922.pdf> at 2 November 2011
[6] ABS, 2009.
[7] Joint Select Committee on Cyber-Safety Commonwealth of Australia, *'High-wire act : cyber-safety and the young : interim report*', (2011) <http://www.aph.gov.au/house/committee/jscc/report/fullreport.pdf> at 2 November 2011.
[8] Danah Boyd, 'Why parents help their children lie to Facebook about ageUnintended consequences of the Children's Online Privacy Protection Act', (2011) First Monday 16(11); Joshua Warmund, 'Can COPPA work? An analysis of the parental consent measures in the Children's Online Privacy Protection Act', Fordham Intellectual Property, Media and Entertainment Law Journal', (2001) 11(1) <http://law.fordham.edu/fordham-intellectual-property-media-and-entertainment-law-journal/iplj.htm> 2 November 2011.

2.11. The Australian Internet infrastructure needs to be resilient and should be able to recover from deliberate attacks and events such as natural disasters.

2.12. Criminal activities associated with illegal access, illegal interception, data interference and the use of botnets require cross-jurisdictional cooperation.

2.13. The relationship between adware, spyware, spam, phishing, search engines, botnets, money mules, and organised crime in general is an inherently complicated structure[9]. Many of these activities are apparently legitimate but can be used in concert to facilitate crime. Policy and regulators need to focus on how these tools interact[10].

2.14. Malicious scripts may be injected into a webpage to steal session cookies, access otherwise protected content, collect usernames and passwords or redirect traffic.

2.15. The impact of security attacks on users is compromised authentication, unauthorised access to their personal data (enabling credit card fraud, identity theft and misuse of bank accounts), pop-up advertisement flooding, spyware installation, bot acquisition and data theft.

2.16. The impact on website owners of security attacks is that their content may be altered[11], the altered content may initialise malicious applications or customers may be redirected to other sites with malicious applications. Each of these scenarios erodes trust in the website owners and the Australian Internet.

2.17. The impact on government and statutory authorities of security attacks is that critical infrastructure may be compromised or shutdown[12], data involving issues of national security may be accessed or altered, personal data of citizens may be compromised or online government services may become unavailable[13].

Benefits of a Secure Digital Economy

2.18. There are numerous benefits of a secure digital economy:

(a) Australian Internet infrastructure will be perceived as safe and reliable, a place where criminals and data miscreants have difficulty operating and cannot shelter.

(b) Global and local businesses using Australian Internet infrastructure will benefit from a competitive edge.

(c) Australians will benefit as the volume of online transactions increases and the digital economy grows.

(d) Australians will have confidence and a higher level of satisfaction in government services provided online.

---

[9] House of Representatives Standing Committee on Communications, *'Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime : The Report of the Inquiry into Cyber Crime*', (2010).

[10] Alana Maurushat, '*Australia's Accession to the Cybercrime Convention: Is the Convention Still Relevant in Combating Cybercrime in the Era of Botnets and Obfuscation Crime Tools?*' [2011] UNSWLRS 20.

[11] Joint Select Committee on Cyber-Safety Commonwealth of Australia, *'High-wire act : cyber-safety and the young : interim report*', (2011) <http://www.aph.gov.au/house/committee/jscc/report/fullreport.pdf> at 2 November 2011 – cites an example of a popular website used by primary school children in Australia being altered to present images of pornography.

[12] Peter Sommer (Information Systems and Innovation Group - London School of Economics) and Ian Brown (Oxford Internet Institute, Oxford University), 'OECD/IFP Project on *'Future Global Shocks' : 'Reducing Systemic Cybersecurity Risk*', (2011) <http://www.oecd.org/dataoecd/57/44/46889922.pdf> at 2 November 2011 - SCADA devices which communicate over the Internet to avoid using a dedicated link have been compromised in the past.

[13] Many property transaction registrations and checks are conducted online and the Torrens system of indefeasibility makes transaction timing critical.

(e) Businesses involved in developing Australia's infrastructure will be able to export their expertise.

Security Challenges

2.19. Internet transactions inherently raise jurisdictional and evidential issues. Difficulties arise with identifying parties, the transaction platform and the ICT devices involved.

2.20. The simplest Internet transaction is between two identifiable entities using a known transaction platform in the same jurisdiction. Even in the simplest transaction, the transient nature of digital data may leave limited traces, making it impossible to reconstruct the transaction for evidentiary purposes.

2.21. Internet transactions are complex. A transaction is likely to be conducted between multiple end points in multiple jurisdictions via a conflagration of intermediary network nodes. Here, jurisdictional and evidentiary problems arise.

2.22. The anonymous nature of the Internet makes it possible for parties to a transaction to be unknown. In these circumstances, the transaction is between unknowable "netizens" of no identifiable jurisdiction via a transaction platform that can be associated with no nation state or at best, fleetingly associated with multiple nation states.

2.23. Data reconstruction can be challenging even in a controlled environment. The Internet cannot be described as a controlled environment. The intermediaries responsible for communicating a transaction may be comprised by thousands of devices having a variety of data retention periods. It may be impossible to reconstruct the transaction due to delays in identifying the necessary devices, finding the data on those devices or deciding to commence the reconstruction effort.

2.24. ICT systems incorporate compromises as they are designed and operated to answer multiple competing requirements. If the dominant purpose is for resilience then the design will be different from a design for performance, to facilitate data reconstruction or to minimise cost. It must be recognised that regulations imposed to improve security will be at the cost of other objectives.

2.25. The digital economy services virtual and physical world interests of "netizens". The present legal structures have developed over centuries in a world that did not contemplate the speed or ease with which events can occur online.

2.26. It is clear that interests outside of the online environment can be tainted by online events and activities. For example, defamation has been repeatedly recognised on the basis of Internet dissemination[14]. Online transactions may involve recourse to real world financial assets or may destroy the results of a significant time investment[15].

The Government's Role

2.27. Commonwealth and State governments need to lead by example with their own ICT implementations in the digital economy. Governments and taxpayers should benefit from these services as the process of information collection and dissemination is streamlined and reaches an increasing proportion of the population.

---

[14] David Rolph, *'Publication, Innocent Dissemination and the Internet After Dow Jones & Co Inc v Gutnick'*, (2010) UNSWLJ 33 562.
[15] Joshua Fairfield, '*Anti-Social Contracts: The Contractual Governance of Virtual Worlds*', (2008) McGill Law Journal 53 427.

2.28. Businesses and individuals can benefit from guidelines and codes of practice. These can be provided in the form of self regulation or by government agencies.

2.29. Each collector of information should be aware of what is expected of them in terms of:

(a) how they collect personal data;

(b) how they store such data;

(c) how long they retain the data;

(d) how they update the data; and

(e) how they share data.

2.30. Information collectors and disseminators should know when and how to obtain permission from an individual prior to making use of their data. For instance, whilst Australia has laws regarding opt in and opt out from direct marketing, there is no mandatory limitation on the use of cookies (although a voluntary code released by the Australian Association of National Advertisers titled "Australian Best Practice Guideline for Online Behavioural Advertising does exist). A website operator might decide to use cookies to gather information at the time of connection, continue to gather information after connection or make use of that information to influence the content delivered to an individual. For example, Facebook tracks users even after they have logged off that website. Cookies present a great opportunity for cybercriminals. Regulation of the use of cookies may be usefully included in the current privacy reform in Australia in relation to the protection of data[16].

2.31. In traditional media advertising, levies are applied to producing codes of practice and facilitate self regulation. In the Internet environment, advertising may not be a suitable source of funding. In the UK, data collectors and disseminators are compelled by law to register with the Information Commissioners Office. This allows information beneficiaries to bear the burden of ensuring information is collected in an ethically sound and publicly acceptable manner. They also carry the cost of implementing and managing the information collection framework.

2.32. Analysis of critical infrastructure shows Australia's communications networks are the most vulnerable component in an attack or natural disaster[17]. Some components are critical to carrying out essential functions. Australia needs to identify threats to critical communications infrastructure and manage vulnerabilities. Australia's sparse population presents challenges to building resilient systems with adequate redundancy and minimal points of failure.

2.33. Australia has a variety of emergency management plans[18]. An emergency plan specifically for the communications sector would be of immense benefit. The plan should reflect the latest understanding of the nature of any threat and lessons should be learnt from events that led to network problems. The communications plan should be tested and reviewed. It is important that the government understands the work undertaken to maintain and operate the communications network.

---

[16] Cyberspace Law and Policy Centre, *'OAIC should have more power'*, (2011) <http://www.law.unsw.edu.au/news/2011/09/oaic-should-have-more-power-cyberspace-law-and-policy-centre> at 2 November 2011.
[17] Desmond Ball, *'China's Cyber Warfare Capabilities'*, (2011) Security Challenges 7(2) 81.
[18] Attorney General's Department, 'Australian Government Emergency Management Plans', <http://www.ema.gov.au/www/emaweb/emaweb.nsf/Page/EmergencyManagement_PreparingforEmergencies_PlansandArrangements_AustralianGovernmentEmergencyManagementPlans< at 3 November 2011.

2.34. It is important to assure security where one provider's network connects with another. The new European Framework for the regulation of communications networks and services provides an example framework.

2.35. Cybercrime investigation requires a co-ordinated national and international approach. Australia has a number of policy makers, investigators and executioners in this area including the AUSCert, High Tech Computer Crime Centre, Cyber Security Operations Centre (CSOC), the AIC, the Office of the Privacy Commissioner, the Attorney General's Department, the ACCC, SCAMWatch, the ACMA, the Department of Broadband, Communication and the Digital Economy, and the Commonwealth Ombudsman. What Australia appears to be lacking is an agency responsible for co-ordinating the efforts of these authorities. The Council of Europe provides interesting guidelines for how this challenge might be addressed[19].

2.36. The Federal Trade Commission of the USA has a wide range powers including the ability to impose penalties for data breaches, ordering injunctions, mandating future behaviour and imposing reporting and compliance requirements. The ambit of the ACCC might be extended to bring these types of cases to court.

2.37. Cybercrime investigation requires particular skills for investigation. Law enforcement requires support to ensure they have adequate support and training. Law inherently struggles to keep up with technological change[20]. There are a variety of approaches that can be taken in recognising this struggle and attempting to ensure the best interests of government and the public are safeguarded[21].

2.38. A large number of gaps are apparent in Australia's domestic laws for successful accession to the Council of Europe Convention on Cybercrime[22]. Australia's trade relationship with the EU is likely to suffer if these deficiencies are not remedied. Recommendations for bridging these gaps have been the subject of a report by the Joint Select Committee on Cyber-Safety[23].

The Role of Businesses

2.39. Internet businesses perform many functions. They include Internet Service Providers, e-commerce companies, domain name registrars, software vendors and end users.

2.40. Each of these players has different objectives and motives. Some or all players could be crucial to tasks such as improving security and transparency, reconstructing data, discovering identity or deciding responsibility. Achieving these outcomes may translate to nothing more than a cost and complexity increase for some.

2.41. However, it is important to note that forcing players to adhere to certain rules may do nothing more than cause them to relocate to a jurisdiction where these rules may be avoided.

---

[19] Council of Europe, *Guidelines for the cooperation between law enforcement and Internet service providers against cybercrime*, (2008) <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567_prov-d-guidelines_provisional2_3April2008_en.pdf> at 2 November 2011.

[20] Lyria Bennett Moses, *'Recurring Dilemmas: The Law's Race to Keep Up With Technological Change*, [2007] UNSWLRS 21.

[21] Joe Herkert, Brad Allenby, and Gary Marchant (eds), *The Growing Gap Between Emerging Technologies and* Legal-Ethical Oversight (2011).

[22] Council of Europe, Convention on Cybercrime, ETS No. 185.

[23] Joint Select Committee on Cyber-Safety, *'Review of the Cybercrime Legislation Amendment Bill 2011*', (2011).

2.42. A lack of jurisdiction will make it inherently difficult to ensure costs follow the event. The only choice may be to compel a player within jurisdiction to supply information that more rightly should have been supplied by a player who is out of jurisdiction.

The Role of the Individual

2.43. Online crime is approaching the size of the global drug trafficking market. According to the 2011 Norton Cybercrime Report, 54% of online users surveyed have experienced viruses or malware on their computers.

2.44. Each Internet user has differing objectives and vulnerabilities. A user's existence may be online only or predominantly offline. A recent UK study showed different segments of the population are vulnerable to different types of fraud. Preferences and attributes including an individual's method of interaction with the Internet, online behaviours, financial knowledge, attitude to risk, fear of fraud and trust in authority[24] dictate risk.

2.45. According to the ACCC, online scams account for 45% of all reported scams in 2010[25]. Some scams could be prevented or minimised with improved security. Education is also an important factor in preventing Australians falling victim to scam attempts.

2.46. PCs, home networks and wireless networks can be secured with relative ease. Networks should be secured with encryption and secure passwords. A variety of anti-virus products are available at relatively low expense and security software should include a mechanism for regular updates. According to the 2011 Norton Cybercrime Report Norton survey, 41% of adults do not have up to date security software.

2.47. There appears to be an information gap or a sense of helplessness amongst individual Internet users. According to the 2011 Norton Cybercrime Report, 86% adults are concerned about cybercrime, but 51% say they would not change their online behaviour even if they became a victim. Individuals would benefit from awareness on topics such as computer optimisation, device set-up, software installation, parental control set-up, security and software installation and backup.

2.48. There have been a range of attempts at educating Australians in the use of the Internet and in ensuring security measures are implemented[26]. Some Internet exploits are not readily combated by education such as phishing and certain types of malware[27]. An important part of an education campaign is including a component to measure effectiveness. There is likely to be some benefit available from co-operation with global partners as many educational concepts will be globally relevant.

---

[24] National Fraud Authority, *'A quantative segmentation of the UK population: Helping to determine how, why and when citizens become victims of fraud.'*, (2011) <http://www.homeoffice.gov.uk/publications/agencies-public-bodies/nfa/national-fraud-segmentation?view=Binary> at 3 November 2011.

[25] ACCC, *'Targeting scams Report of the ACCC on scam activity 2010'*, (2010) .<http://www.accc.gov.au/content/item.phtml?itemId=972476&nodeId=82520eb0bf4bef0d78873f4f0680557a&fn=Targeting%20Scams%20Report%202010.pdf> at 2 November 2011.
<http://www.acma.gov.au/webwr/_assets/main/lib310665/galexia_report-overview_intnl_cybersecurity_awareness.pdf>
ACMA, *'An overview of international cyber-security awareness raising and educational initiatives : Research report commissioned by the Australian Communications and Media Authority'*, (2011) <http://www.acma.gov.au/webwr/_assets/main/lib310665/galexia_report-overview_intnl_cybersecurity_awareness.pdf>

[27] Alana Maurushat, '*Australia's Accession to the Cybercrime Convention: Is the Convention Still Relevant in Combating Cybercrime in the Era of Botnets and Obfuscation Crime Tools?'* [2011] UNSWLRS 20.

3. International partnerships and Internet governance

ISSUE: The attractions of the Internet in terms of openness, access to information (of all qualities) and informal governance are also creating tensions with traditional government responses to community interests.

QUESTION: What model of Internet governance is in the best interests of all Australians?

3.1. As outlined in the Discussion Paper, the Internet is an "*open, decentralised and universally available space*." In order to maintain this position, the model of Internet governance should be minimal in scope and only go as far as is necessary to ensure an open, decentralised and universally available space.

3.2. We submit that any potential model of Internet governance should acknowledge the limitations of regulating the online environment as it exists outside of Australia. Furthermore, policy makers should be wary of placing Australia in a position out of step with the rest of the world.

3.3. The consequences of regulatory forbearance could mean the online isolation of Australia consistent with its geographic isolation. The Internet which serves as Australia's most inexpensive and efficient connection with the rest of the world has the potential to satisfy the economic, social and security interests of Australia and its citizens. Regulation that puts Australia on an unequal footing with the rest of the world could lead to those interests being ignored.

3.4. In terms of the extent and breadth of regulation, governance should only go as far as to ensure the Internet is open, decentralised and universally available. Regulation beyond this position can have the potential to be overbearing, unnecessary, ineffective and suppressive.

3.5. In summary, there is no single model that can efficiently and effectively regulate all parties that exist in the online environment. The potential scope of regulation cannot be predicted in an online environment that is not yet fully developed and arguably will never be fully developed. Forming tangible and future-proof policy positions are necessarily difficult as a result.

3.6. Above all, required regulation should focus on the parties that are in the best position to secure its implementation, education and enforcement. Policy makers should be mindful of the most appropriate place for onus of compliance, whether that be on carriers, service providers, content hosts or end-users.

QUESTION: How can we get the right balance between Australia's social, economic and security needs when developing an Australian vision for the online environment?

3.7. The right balance can most readily be achieved through regulation that extends only to the point that it can ensure the Internet remains open, decentralised and universally accessible.

3.8. The risk of moving beyond what is necessary is a situation where unnecessary government control results in cultural censorship or a more restrictive commercial environment. In searching for an appropriate balance, policy authors should be determined to encourage innovation and promote competition. They should also form necessary regulation with the goal to provide a sufficiently secure online space for commercial enterprise or community engagement.

3.9. Ultimately, each aspect of regulation deserves its own assessment of how best to strike a balance between the three needs outlined above. An unnecessary adherence to one need over another is a potential danger in pre-determining policy priorities. Furthermore, policy makers should take a flexible approach to policy because there may be other needs that warrant attention and should be considered along with social, economic and security needs.

3.10. In lieu of additional stringent regulatory controls, the Government has the opportunity to promote self-regulation. Industry codes of conduct and voluntary standards can be highly effective. In terms of electronic transactions and the financial services industry, the Financial Services Industry Ombudsman has the opportunity to consider widely utilised standards such as the Payment Card Industry Data Security Standard (PCI-DSS) in making decisions.

3.11. A more concrete example for how this can apply to our broader digital economy comes in relation to the ongoing iiNet Court proceedings. The current position of the Full Federal Court seems to tentatively suggest that ISPs must take greater responsibility in this area.

3.12. An example of a legislative response to such circumstances which should be avoided are the Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet (HADOPI) laws in France. These laws were criticised as technologically unsound, unable to maintain consumer privacy and lacking procedural oversight mechanisms.

3.13. By encouraging industry dialogue, the Government has the opportunity to oversee the development of programs within industry that may more reasonably balance those interests of rights holders, alongside those of the community.

3.14. The Government could further supplement digital literacy programs within schools, by choosing to follow the EU in requiring public administrative bodies to implement open source software and formats, where there is no explicit reason to prefer proprietary software. Such software provides opportunities for software development of a scope and scale not often possible outside open source projects.

3.15. There are additional potential economic advantages to use of such software, in avoiding licensing fees, but a further key advantage would arise from data compatibility and open formats of data.

3.16. The Gov2AU program drew attention to the role of licensing and content structures in public data. Providing government data in accessible formats can lend itself to a range of applications that are of significant benefit to the community. Not for profit organisations such as the OpenAustralia Foundation currently operate a number of projects that make use of such data. They provide facilities for complex searches of Hansard information, along with email notifications for key terms. They additionally aggregate development applications to a range of Councils across Australia and provide alerts for applications based on geography.

3.17. The ease with which such projects can proceed and the benefit to the broader community is only amplified where Government chooses to actively make available more data to the public, in accessible formats, without the encumbrance of complex licensing arrangements or onerous regulatory control.

ISSUE: Increasingly, policy makers have turned to discussing what agreements governing behaviour in the online environment might look like, the principles they should be based on, the boundaries they would place on behaviour and how they can be promoted. This will be a gradual and long-term process, and varying stakeholders are likely to want different outcomes from any agreement process.

QUESTION: What sort of approach should be taken to developing agreements on behaviour in the online environment?

3.18. The Department of Broadband, Communications and the Digital Economy deserves praise for the manner in which they have conducted the Convergence Review. In an area of rapid technological and cultural change, the pace of legal review should be comparatively gradual and maintain a substantial emphasis on engagement with interested stakeholders. The progress of the Convergence Review to date represents a continual conversation with the community about important issues likely to affect them.

3.19. There are three main principles that should govern the development of agreements on behaviour in the online environment.

(a) In approaching and promoting an informed policy position on behaviour in the online environment, policy authors should exhaust all opportunities to engage with as many individuals, groups and body corporates as possible.

(b) Policy makers should be prepared to act purposefully but not carelessly when forming a policy position so as to consider all aspects of any potential regulation.

(c) The eventual policy position should be pragmatic and, to the largest extent possible, forward-looking in order to better accommodate further technological and cultural change.

3.20. Effective policy and regulation must remain platform and technology agnostic. Unnecessarily prescriptive regulation has the effect of creating unnecessary workload for regulatory bodies, without significant benefit to consumers or industry.

3.21. An example of such a burden is visible in the USA, where in relation to copyright, fair use provisions operate on the policy basis that the rights afforded to copyright holders should be balanced against those of broader society. However, beyond these particular provisions, the Library of Congress has the authority to make decisions about particular behaviour. A decision that garnered significant attention was that “jailbreaking” an iPhone was a practice protected by fair use. Such a decision is unnecessarily narrow in its specificity to one brand and one type of consumer device.

4. Investing in Australia's digital future

ISSUE: The demand for skilled cyber professionals in both the public and private sector will continue to grow at a rapid rate and it is likely that those companies - many of which will be based overseas - offering the best financial incentives will attract the best of Australia's ICT graduates. However, a purely market-led distribution of skilled cyber workers may not meet the broader digital needs of Australia as a nation.

QUESTION: What new forms of government-industry cooperation and dialogue are required to ensure the Australian cyber skills base is developed to meet Australia's broader national interests?

Protecting domestic law is in Australia's broader national interests.

4.1. Cyber technologies and data have in recent years become easier to distribute across the globe. This has posed concerns regarding the trans-jurisdictional nature of cyber technologies such as social media and cloud computing.

4.2. In commenting on Internet giants that were not responding to police investigations, Communications Minister Stephen Conroy recently cautioned against the potential for cyber organisations to take advantage of the trans-jurisdictional nature of their operations "Hiding behind the fact that they're American-based companies and the Internet is largely based in America is not good enough"[28].

4.3. A member of the European Parliament's civil liberties committee quite recently noted similar concerns "Does the [European] Commission consider that the U.S. Patriot Act thus effectively overrules the E.U. Directive on Data Protection? What will the Commission do to remedy this situation, and ensure that E.U. data protection rules can be effectively enforced and that third country legislation does not take precedence over E.U. legislation?"[29]

4.4. Whilst it may be possible, with international cooperation and partnerships, to hold criminals liable, it is still difficult to investigate such trans-jurisdictional matters due to inconsistencies in privacy and other related law across the world. The above concerns are amplified where an organisation has no established entities or employee-base within direct Australian jurisdictional reach.

It is in the national interests to maintain a balance of cyber technologies and skilled workforce.

4.5. Cyber technologies are increasingly marketed so that they appear to be cost effective or even free of charge. Rapid take up is also encouraged. If the substantial proportion of small businesses or even large enterprise takes up such apparently inexpensive offers, it would allow the major cyber service providers to centralise and manage powerful portions of entire economies. It would therefore be in the national interest to maintain a balance of cyber technologies and skilled workforce, so that they are developed and maintained within direct Australian jurisdictional reach.

---

[28] Nicola Berkovic, 'Internet giants put on notice', *The Australian* (Online), 27 May 2010 <http://www.theaustralian.com.au/politics/Internet-giants-put-on-notice/story-e6frgczf-1225871760378>

[29] Jennifer Baker, 'EU upset by Microsoft warning on U.S. access to EU cloud', Computerworld Inc. (Online), 5 July 2011 <http://www.computerworld.com/s/article/9218167/EU_upset_by_Microsoft_warning_on_U.S._access_to_EU_cloud>

4.6. Large enterprises such as banks have in the past also been tempted by the perceived lower costs of outsourcing their technologies internationally. In considering the storage of secure digital information, Michael Harte, Commonwealth Bank CIO in 2009 was quoted in an interview as stating "Commonwealth is in close discussion with several key parties across the world - both practitioners and possible service partners"[30].

4.7. It is important that dialogue between Government and industry be established to ascertain the motivations behind the distribution of cyber skills to overseas partners.

Balancing local and international social, economic and security needs should be in the national interest.

4.8. The impacts of commerce in a closed economy within Australia may not be as important as the impacts of commerce in an open international economy. Concerns surrounding this issue are noted in the Access Economics report on the *Household E-Commerce Activity and Trends in Australia* (Nov 2010) "International e-commerce purchases represent a leakage from the Australian economy as they are imports. The impact of this depends on whether e-commerce is displacing domestic production or sales of imported products by domestic retailers"[31].

4.9. In other words, a healthy balance needs to exist between international and domestic, and production and sales. Balancing such needs and interests should not be confused with comparisons/forecasts of exports and imports alone. In the same report, it is noted that the main reasons for the non-use of e-commerce by Australian consumers relates to privacy and security[32].

4.10. It is also worth noting other things, including the concerns of the Canadian Privacy Commissioner around the trans-jurisdictional nature of cyber computing and also the "*seeming* jurisdictional neutrality"[33] (emphasis added) of such technologies. Note that net neutrality does not seem to be politically in favour in the U.S. at the moment "there's essentially no prospect of a net neutrality bill passing anytime soon"[34].

4.11. Furthermore, it has been difficult for major technology providers to guarantee that data be protected against trans-jurisdictional effects as a result of such providers being based in the US. Gordon Frazer, managing director of Microsoft UK, has made statements that clarify the inability of data to be protected against the US Patriot Act and under the Safe Harbor Privacy Principles, where a company is also based in the U.S "Microsoft cannot provide those guarantees. Neither can any other company"[35].

4.12. This is a clear recognition that cyber computing may seem jurisdictionally neutral though in reality, may not be so. Depending on the locations of the cyber workforce or entities, cyber computing may pose unforeseen consequences.

---

[30] Fran Foo & Mahesh Sharma, 'Bank looks to cloud to blow away licence costs', The Australian (Online), 6 October 2009 <http://www.theaustralian.com.au/australian-it-old/cba-banks-on-cloud-computing/story-e6frgamo-1225783078913>

[31] Access Economics Pty Limited, (Report for the Department of Broadband, Communications and the Digital Economy), Household E-Commerce Activity and Trends in Australia, 17 November 2010, 22

[32] Access Economics Pty Limited, (Report for the Department of Broadband, Communications and the Digital Economy), Household E-Commerce Activity and Trends in Australia, 17 November 2010, 16

[33] Office of the Privacy Commissioner of Canada, *Reaching for the Cloud(s): Privacy Issues related to Cloud Computing* (February 2010) <http://priv.gc.ca/information/pub/cc_201003_e.cfm>

34 Chris Lefkow, "Republican victory in US election dooms 'net neutrality'", *The Age* (Online), 8 November 2010 <http://news.theage.com.au/breaking-news-technology/republican-victory-in-us-election-dooms-net-neutrality-20101108-17jmg.html>

[35] Zack Whittaker, 'Microsoft admits Patriot Act can access EU-based cloud data', *ZDNet*, 28 June 2011 <http://www.zdnet.com/blog/igeneration/microsoft-admits-patriot-act-can-access-eu-based-cloud-data/11225>

4.13. Therefore, the following forms of government-industry cooperation and dialogue are required:

- government led education on better understanding of how 'third country' jurisdictions can affect government or industry, technology and technology service providers;

- investigation of the motivations that are causing industry to send or consider sending cyber skills overseas; and

- reconfiguration of any forms of incentive or funding that the Government provides.

This will strategically encourage industry to establish intra-jurisdictional employment, skills and intellectual development in technology services. This could help to mitigate the security factors, encourage local economic and intellectual growth, while helping to balance an open online environment.

5. Conclusion

5.1. A minimalist approach to Internet governance is required to ensure the success of Australia's digital industry and our social, economic and security needs for the online environment. However, a level of Government intervention and investment is required for the success of Australia's digital future.