4. Where the wild things are: Evolving futures of communications regulation in the current national security context

ABSTRACT

In March 2008, the Australian Communications and Media Authority (ACMA) released a report dealing with the possible implications of the 'top six trends' in communications and media technologies, applications and services. The report highlights the fact that key regulatory elements in the communications environment are being conceptually 'stretched and pulled' by the accelerating pace of change in communications technologies, applications and services. The report also notes that in the longer term, there will be increasing overlapping developments in technology and increasing interconnections between people, databases and objects. This article will explore the evolving futures of communications regulation in the current national security context by focusing on the post-'9/11' regulatory response in Australia. Communications have long been regarded as 'the fundamental cornerstone of intelligence and law enforcement'. For this reason, in the current national security context, this article will argue that the evolving futures of communications regulation will be increasingly calibrated with national security policy.

Keywords: communications regulation, intelligence, media technologies

SUSANNE LLOYD-JONES
Macquarie University, Sydney

Introduction

IN MARCH 2008, the Australian Communications and Media Authority (ACMA) released a report dealing with the possible implications of the 'top six trends' in communications and media

technologies, applications and services (ACMA, 2008). The report highlights the fact that key regulatory elements in the communications environment are being conceptually 'stretched and pulled' by the accelerating pace of change in communications technologies, applications and services (ACMA, 2008, p. 1). The report also notes that in the longer term, there will be increasing overlapping developments in technology and increasing interconnections between people, databases and objects (ACMA, 2008, p. 3). Further, the report notes that 'while large companies are likely to continue to dominate the provision of infrastructure and many communications and media services, their business models are changing. Niche players, third parties, network collaborators, innovative business models and individual users are providing alternatives in internationalised markets' (ACMA, 2008, p. 3). The report also argues for a sustainable regulatory framework which is responsive to change and can accommodate new dynamics (ACMA, 2008, p.3). What is missing from the analysis of the 'top six trends' is an evaluation of the changes to the communications regulatory environment as a consequence of the post-'9/11' national security agenda.

This article will explore the evolving futures of communications regulation in the current national security context by focusing on the post-'9/11' regulatory response in Australia. Communications have long been regarded as 'the fundamental cornerstone of intelligence and law enforcement' (ACA, 2005, p.26; Hills, 2005, p.195). For this reason, in the current national security context, this article will argue that the evolving futures of communications regulation will be increasingly calibrated with national security policy. This article will also contend that the multi-layered communications regulatory environment complicates this calibration.

The article will briefly analyse some of the challenges and implications of the current national security context by reviewing the key legal and policy initiatives introduced by the Howard Government (and seemingly accepted by the new Rudd Government) since 11 September 2001 which affect the regulation of:

- *communications infrastructure* which comprises the cables, wires and airwaves over which data flows, and includes telecommunications services such as carriage or carriage services;
- *applications* which includes services such as search engines and social networking applications and software applications such as content filtering and encryption software; and

- *content* which includes, among other things, film and literature classification and broadcasting content.

This part of the article will also consider the impact and influence of communications stakeholders on national security law and policy.

It is commonplace to discuss the post-'9/11' national security legislation and policy in terms of the impact on democracy, freedom of speech and censorship. However before we can sensibly embark on a discussion of the ideological and political 'reach' of the new regulatory framework for communications industry stakeholders and citizens alike and the further changes that are envisaged, the technostructural underpinnings of the desired political objectives requires closer consideration. It is engagement with this practical dimension of regulation that is currently least developed in Australia. My concern is for what this might mean for broader debates about the surveillance society and for the future of Australian communications regulation.

Challenges of the security-communications regulatory interface

Communications have been undergoing unprecedented structural, institutional and regulatory change over the last decade (ACMA, 2008, p.3). The structural reality of the contemporary communications environment is that of a multilayered, trans and multinational regulatory environment serving many functions, not least of which is national security (ACMA, 2005, p.i). Rapid change in communications technology has ushered in a new era of trans and multinational regulation, both formal and informal (Bowrey, 2005, pp.19-21). The same rapid change has likewise guaranteed a shortfall between regulation and the communications networks they seek to regulate or to track (Berg & Tobin, 2007, pp. 32-36; Bronitt & Stellios, 2006, p. 414). This is nowhere more apparent than in the case of the internet which, with new and emerging technologies and applications, lies close to the heart of the battle against terrorism in the post-September 11 era (ACA, 2005, p. 14; Weimann, 2006, pp. 173 -202; Andrejevic, 2006, p. 442). This is a complexity that polarised debates focusing on the excess or dearth of anti-terrorist communications regulation have difficulty tracking.

In order to focus the analysis, the paper will concentrate on a selection of post-September 11 legislative amendments which attracted attention from the communications sector stakeholders. This part of the article will canvass the communications-related national security legislation as it relates to

licensing, provision of services which may be prejudicial to national security, interception and interception capability, and content regulation.

Licensing and national security

According to Raiche, the *Telecommunications Act 1997* provides the legislative basis for Australia's telecommunications industry (Raiche, 2004, p.1). Within this regulatory structure, licensing of services is a cornerstone of Australian telecommunications. Under the *Telecommunications Act* a person may apply to the Australian Communications and Media Authority (the ACMA) for a carrier licence so long as the person is a constitutional corporation, a partnership of such corporations or a public body (*Telecommunications Act 1997*). According to Senator Ian Campbell in his second reading speech on the *Communications Legislation Amendment (No. 1) Act 2004*, the pre-2004 licensing framework in the *Telecommunications Act* failed to take into consideration national security and law enforcement interests. No consideration of national security issues was required as part of the carrier licensing process.

From a regulatory perspective, Senator Campbell points out that the licensing authority, the Australian Communications Authority (now the Australian Communications and Media Authority (ACMA)) was under no obligation to consult with the relevant national security and law enforcement agencies prior to issuing a carrier licence to an applicant. It was regarded as a problem by the Howard Government that national security grounds were not expressly provided for in the carrier licensing approval process. Senator Campbell pointed out that the grounds for refusing a carrier licence are broad, but did not explicitly mention national security. The enactment of *Communications Legislation Amendment (No. 1) Act 2004* (the *Communications Act*) sought to remedy this perceived problem.

The security-focused amendments to the *Telecommunications Act 1997* in 2004 were justified on the basis that they would ensure that national security and law enforcement interests were considered in the carrier licensing process. Today, the Australian Communications and Media Authority (ACMA) must consult with the Communications Access Co-ordinator, the new regulator situated in the Attorney-General's Department, prior to granting a new carrier licence. The Communications Act gave the Attorney-General the power to direct the ACMA to refuse to grant a carrier licence on national security grounds. This direction can only be made in consultation with the

Prime Minister and relevant Minister. Senator Ian Campbell explained in the Second Reading Speech of the *Communications Act* that

> the package of amendments contained in [the *Communications Act*] will lead to more secure telecommunications networks and services and improved arrangements for the provision of assistance to law enforcement agencies by telecommunications carriers and carriage service providers.

However, such significant changes to the carrier licensing procedures attracted minimal attention from the telecommunications industry, arguably the industry most affected by the changes.

Provision of services—prejudicial to national security

Vodafone, the only telecommunications company to make a submission to the Senate Inquiry relating to the Communications Act, explained in its submission to the inquiry:

> [A]s a carrier and carriage service provider to [over 2.5 million customers in Australia], Vodafone is concerned that, as presently drafted, the Bill will confer very wide discretionary powers to restrict Vodafone's legitimate business practices, which powers appear to go well beyond what may reasonably be required to protect Australia's national security interests. (Vodafone, 2003, p. 1)

Vodafone was also particularly concerned about the effect of the power of the Attorney-General to 'direct carriers and carriage service providers not to use or supply, or to cease using or supplying (at all or to particular persons) a carriage service or all carriage services where such use or supply is considered to be prejudicial to national security' (Vodafone, 2003, p.1). Vodafone's concerns stemmed from the scope of the power to impact upon the livelihood of businesses and individuals working in the telecommunications industry. Vodafone further submitted that:

> As summarised in the Bills Digest to the Bill, the unacceptable consequence of the present drafting of section 581(3) is that:
> *...on a strict reading of the amendments proposed in the Bill, ... decisions by the Attorney-General affecting the business and livelihood*

> *of people in the telecommunications industry can be based on subjective judgments [sic] of the national security situation with little prospect of any successful review by the courts.* (Vodafone, 2003, p. 1)

In the same submission, Vodafone reiterated its support for the underlying policy objectives of the Bill and in doing so, identified one of the quandaries of the regulatory interface—how communications industry participants can reconcile their legitimate business interests with national security interests. Vodafone added that:

> Vodafone acknowledges that it is necessary and appropriate for Government to have adequate powers to protect Australia's national security, particularly given the current domestic and global security environment. Vodafone is committed to its statutory obligations to assist in this task, and already provides a very high degree of assistance to government agencies in this respect. (Vodafone, 2003, p. 1)

Historically, as noted by Jill Hills, national governments have always had the power to direct communications companies to cease the supply of communications services, such as the telegraph, for reasons of national security, most notably in times of war (Hills, 2006, p.197). The concept of carrier has a deceptive simplicity about it, particularly in the Australian communications environment where only a handful of licensed carriers operate. Before the deregulation of the telecommunications sector in the mid-nineties, the regulatory environment was even more uncomplicated as there was only one carrier, Telstra. However, thinking about this issue in terms of the 'top six trends' in the communications environment, how will this power be used in the future when niche players, third parties, network collaborators and individual users are providing alternatives to carrier services in internationalised markets? The issue is of practical concern—to whom will the power be directed and in what circumstances?

Interception and interception capability

Bronitt and Stellios have shown that the telecommunications interception regime has been expanding in both scope and scale since the 1980s (Bronitt & Stellios, 2006, p. 414). The telecommunications interception regime has been amended a number of times in the past decade to take into account advances in technology and the need for more responsive regulation to old and

new crimes using new and emerging technology (Bronitt & Stellios, 2006, p. 414). For example, the amendments introduced in 1999 were justified by then Attorney-General Daryl Williams on the basis that law enforcement and national security agencies needed tools to keep up to date with technological changes, organised crime, arsonists, child pornographers and terrorists. Bronitt and Stellios have tracked the regulation of telecommunications interception and have shown that the regulatory framework has shifted from being primarily that of an investigative tool to a national surveillance scheme for serious crime in the federal and state jurisdictions (Bronitt & Stellios, 2006, p. 414). They have characterised the 2006 changes to the interception regime as moving beyond 'function creep' (Bronitt & Stellios, 2006, p. 415) arguing that:

> [T]he amendments are a watershed in the history of interception law in Australia, heralding a major conceptual shift albeit under the guise of technical improvement. Under these reforms, the scheme moved beyond 'live' interception to include access to stored data. In simple terms, a warrant scheme originally devised to permit interception of communications has been extended into a power to search and seize stored communications data. (Bronitt & Stellios, 2006, p. 415)

Under the *Telecommunications (Interception and Amendment) Act 1979 (*as amended), a telecommunications network must be 'capable of interception'. The industry raised a number of issues associated with the interception capability requirements found in the *Telecommunications (Interception and Amendment) Amendment Act 2007*. The Australian Mobile Telecommunications Association (AMTA) noted in its submission that:

> The redefinition of Interception Capability, rather than using the term from the *Telecommunications Act 1997* has the potential for serious, even if unintended, consequences for Carriers and Carriage Service Providers. AMTA is concerned that the proposed definition includes any equipment connected to a telecommunications network. Provision of services in an Internet environment involves use of a variety of separate components that are clearly defined in the *Telecommunications Act* 1997, including customer equipment, carriage services, that is, the carrying of internet 'packets' across networks and

> internet applications and content services, such as instant messaging and web hosting. For the most part Internet applications, content services and customer equipment can be independent of the Carrier or CSP. (Australian Mobile Telecommunications Association, 2007, p. 2)

The point raised by the AMTA has practical consequences. The architecture of the internet with its multiple layers, protocols and generative processes make this independence possible (Zittrain, 2008, pp. 67-71). Further, the broad definitions now incorporated into the *Telecommunications (Interception and Access) Act 1979* may mean that many services may be classed as 'telecommunications services', such as Google and Microsoft's Suite of new and diverse offerings. Furthermore, there are also many new creators of 'telecommunications data', for example, social networking sites such as YouTube and MySpace. There are search engine services such as Google and platforms such as Microsoft, which provides a range of services from instant messaging to document management. The broad definition has the potential to capture these new services. The problem highlighted by the ATMA has relevance to the nature of the digital communications environment. Yet the current framing of the interception capability requirements means that the responsibility rests with the licensed carrier or nominated carriage service provider.

In February 2008, the newly elected Federal Labor Government, under the leadership of Kevin Rudd, introduced the *Telecommunications (Interception and Access) Amendment Bill 2008*. According to the explanatory memorandum, the Bill would, among other things, permit the interception of multiple telecommunications devices on the one 'named person warrant' (Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2008*).

The Bill was subject to a Senate Legal and Constitutional Committee Inquiry. The Bill was not without controversy despite assurances from the new Labor Attorney-General, Robert McClelland, that the Bill 'contains no new powers for security or law enforcement agencies in relation to telecommunications interception, stored communications or access to data.' The Attorney-General further explained that the amendments were necessary so that security and law enforcement agencies would have contemporary powers to deal with crime in an era of rapid technological change.

The *Telecommunications (Interception and Access) Amendment Act 2008* was passed in May 2008. Interestingly, no carrier, carriage service provider or relevant communications industry association made a submission to the Senate Committee Inquiry. The amended telecommunications interception framework now permits extensive lawful interception of Australian citizens across services, platforms, devices and data fields through a variety of warrant and authorisation processes. The complexity of the interception multiplies when considered in light of the current communications environment. Different carriers, devices and services are converging over multiple devices. By combining the devices and services with the 'telecommunications data' (which is produced in the environment) a monumental information flow results. Also, in the Internet environment, the regulatory line between access to the content of communications (which requires a warrant) and access to telecommunications data (which requires an authorisation) becomes somewhat blurred. It is surprising then, if not alarming, that no communications stakeholder made a submission to the Senate Committee about this Bill despite its obvious 'work generating' capacity.

Internet Protocols—interception capability and ownership

National security regulation occurs by way of telecommunications interception but only if a particular service can be intercepted at the physical layer or infrastructure level. This means that if a service uses network and transport systems which fall outside of the *Telecommunications (Interception and Access) Act* interception framework, such as an Internet Protocol based service, then those systems will not be subject to national security regulation from a telecommunications interception point of view. Yet, as the AMTA has noted, the responsibility for those services may end up falling with the carriers and carriage service providers for the reason that *their* services fall within the regulatory categories in the *Telecommunications (Interception and Access) Act*.

Internet Protocol based services, such as Voice over Internet Protocol (VoIP), exemplify the regulatory complexity in the regulation of internet protocols and the associated difficulties surrounding national security regulation. For example, in its submission to the Senate Inquiry into provisions of the *Telecommunications (Interception and Access Amendment) Bill 2007*, in its submission, the Attorney-General's Department hinted that 'RFC 2822', an Internet Protocol, (IETF, www.ietf.org/rfc/rfc2822.txt?number=2822,

retrieved 14 September 2007) may be used to determine the substance of 'telecommunications data' under the *Telecommunications (Interception and Access) Act 1979* (as amended) even though the RFC 2822 requirements are not included in any definition in the Act. The matter was raised in response to privacy concerns about the broad definition of 'telecommunications data' raised by Electronic Frontiers Australia and the Commonwealth Office of the Privacy Commissioner during the Senate Inquiry.

As explained by Bowrey, a 'request for comments' (RFC) is a voluntary standard and compliance with an RFC is about achieving 'the level of functionality that comes with adopting a tried and tested 'best practice' (Bowrey, 2005, p. 3). The International Engineering Task Force, an external non-government body, looks after the drafting, review and publishing of the RFCs (Bowrey, 2005, p.3). Bowrey explains that 'there is no law of the internet that says a site or network must be compliant' (Bowrey, 2005, p. 3).

It is quite possible that some telecommunications services are configured on the basis of the old RFC 822 or not RFC compliant at all. The important issue in respect of national security regulation will be the actual role of RFC 2822 and its relationship to the definition of 'telecommunications data'. Telecommunications data is not a defined term in the *Telecommunications (Interception and Access) Act 1979*. The *Telecommunications Act 1997* uses 'communications', which includes any communication:(a) whether between persons and persons, things and things or persons and things; and (b) whether in the form of speech, music or other sounds; and (c) whether in the form of data; and (d) whether in the form of text; and (e) whether in the form of visual images (animated or otherwise); and (f) whether in the form of signals; and (g) whether in any other form; and (h) whether in any combination of forms.

The Explanatory Memorandum provides the following explanation of 'telecommunications data':

> Telecommunications data is information about a telecommunication, but does not include the content or substance of the communication. Telecommunications data is available in relation to all forms of communications, including both fixed and mobile telephony services and for internet based applications including internet browsing and voice over internet telephony. For telephone-based communications, telecommunications data includes subscriber information, the telephone numbers of the parties involved, the time of the call and its duration.

> In relation to internet based applications, telecommunications data includes the Internet Protocol (IP) address used for the session, the websites visited, and the start and finish time of each session. Telecommunications data specifically excludes the content or substance of a communication. Currently, the use and disclosure of this data is generally prohibited under sections 276, 277 and 278 of the Telecommunications Act. Sections 282 and 283 allow access to this data for specific law enforcement and national security purposes.

The issue revolves around what actually constitutes 'telecommunications data' for the purposes of the Act. There is no guidance on whether RFC 2822 is a guideline or whether compliance will be mandatory. Nor does RFC 2822 necessarily provide the data which comprises 'telecommunications data' as described in the Explanatory Memorandum of the Bill, given that it is only a voluntary standard (despite the high level of compliance with the protocol (Bowrey, 2005, p. 3). The concept of 'telecommunications data' is an open-ended concept which provides little certainty for industry or citizens about what information will be comprised in 'telecommunications data'.

Data, as Bowrey explains, is 'used to identify us and speak for who we are' in a limited way:

> Data is collected, collated and transmitted. Data is used to identify us and speak for who we are. But our identity is only revealed through the databases largely generated by the records of our choices and actions. The related political concern here is that our agency or capacities as citizens have already become confined by and through these webs and networks. We cannot expect the state to intervene on our behalf, to address our other needs, interests or desires. The nation state will only identify us as consumers of services signified by the data that represents us, or see us as threats to the network, the state and ultimately other citizens, requiring a strategic, political response. (Bowrey, 2005, p. 179)

For this reason, an open-ended concept of 'telecommunications data' allows national security and law enforcement agencies access (for law enforcement and national security purposes) to an on-line universe of known, available or future (prospective) information which is being collected, collated and transmitted by telecommunications services. Moreover, the unique regulatory environment of the internet means that a voluntary standard such

as an RFC may determine what 'telecommunications data' means for the purposes of the telecommunications interception regime.

Communications applications—interception and service restrictions

Communications and media applications, such as the world wide web or social networking applications, such as FaceBook, can be indirectly intercepted through the telecommunications services or infrastructure owned and operated by a carrier or carriage service provider. The object of the interception is to capture the data flows. According to Zittrain, the applications represent the tasks which people are able to perform on the internet, such as searching for information or social networking (Zittrain, 2008, pp. 67-71). What an individual searches for and with whom they associate are relevant in the current national security context. The informal context of regulation of the internet means that many applications remain unregulated. In this respect, the effectiveness of the national security legislative framework is difficult to map. The tools of technology, such as steganography and encryption, allow anyone, for good or ill, to hide their activities and communications (Branch, 2003, p. 38).

The *Communications Act* provides the Attorney-General with the power to direct the cease of supply of a carriage service. The second reading speech explains that:

> Under the *Communications Act*, the Attorney-General, in consultation with the Prime Minister and the Minister administering the Telecommunications Act, may direct a person not to use or supply, or to cease using or supplying, a carriage service or all carriage services to itself or any other person on national security grounds.

The Second Reading speech notes, the direction is 'wide-ranging and may be issued with respect to particular individuals, groups or existing telecommunications industry participants, whose activities pose a risk to national security'.

As mentioned previously, governments have had the power to control communications in this manner since the St Petersburg Convention of the late 1800s (Hills, 2006, p. 197). According to Hills, this convention codified the powers of national governments with respect to telecommunications as a matter of national security (Hills, 2006, p. 197). For example, under Article 7 of the

St Petersburg Convention, the parties had the power to stop the transmission of any private telegram which may appear dangerous to the security of the state, or which may be contrary to the laws of the country, to public order, or to decency (Hills, 2006, p. 197).

In the current communications regulatory environment, this is a difficult power to define. From a practical perspective, which services does the government mean? How does one identify a service as a threat to national security and what happens if the threat does not originate with an Australian carrier? For example, would Google Earth or Google Map's Street View and its various other embodiments qualify? Does the power propose to stop the supply of the internet? Given the nature of the internet and its nodal, decentralised, structure, it would be difficult for the Australian government to order a cessation of supply without agreement in the international regulatory framework.

The international regulatory framework is beyond the scope of this article. However, important issues of ownership, access, use, interception and censorship play a role in this regulatory scenario and involve international state and non-state actors. The complexity of addressing this issue should be apparent from consideration of existing international debate about the existing use of powers over telecommunications and the Internet in authoritarian regimes.

Similar to the power to direct the ACMA to refuse a carrier licence on national security grounds, it was explained in the *Communications Act* second reading speech that the Attorney-General would exercise the power to direct a person to cease using or supplying a carriage service only in extreme circumstances where the risk to national security cannot be managed effectively through other mechanisms. With developments in the diversity of physical infrastructure flagged as a top six trend by the ACMA (AMCA, 2008, 4), reliance on the regulatory concept of carrier may have serious implications for the efficacy of this power to meet the policy objectives of the national security policy agenda.

Content regulation and national security

The national security legislative framework regulates content through film and literature classification, broadcasting content control, reporting restrictions on the media in respect of national security matters and the criminal offence of sedition. The criminal law will apply to communications and media content if the transmission of that content constitutes a criminal offence within the scope of the *Criminal Code Act 1995*, for example,

possessing and communicating child pornography using a carriage service (Fitzgerald, et.al, 2007, p. 681).

The rapidly evolving communications environment poses unique difficulties for carriers and carriage service providers in respect of content regulation for national security purposes. The responsibility for filtering criminal (which includes terrorist content) and offensive content is increasingly falling on the shoulders of communications industry stakeholders, such as Internet Service Providers and Internet Content Hosts. The development and implementation of new technologies will enable service providers to block, shape, monitor and prioritise internet traffic flows over their networks. The issues surrounding these kinds of activities range from the adequacy and efficacy of the filtering products to the appropriateness of communications industry stakeholders acting as 'rough censors' (Hills, 2006, p. 198) for the government.

The *Anti-Terrorism Act (No.2) Act 2005* introduced the revised and updated offence of sedition. Bronitt and Stellios have noted that 'the revival of the interest in sedition was a direct response to recent terrorist attacks, and was presented as part of a package of counter-terrorism measures by the Howard Government' (Bronitt & Stellios, 2006, p. 196). Before this revival, sedition had an unpleasant political history of being used against people, from artists to political opponents, who spoke out against the government (Bronitt & Stellios, 2006, p. 196). In 2007, the Howard Government successfully expanded the national security legislative framework into the film and literature classification regime by passing legislation which placed restrictions on access to 'terrorism-related materials' (*Classification (Publications, Films and Computer Games) Amendment (Terrorist Material) Act 2007)*.

Obligations currently exist where internet service providers must report users accessing criminal content, such as child pornography (Fitzgerald, et.al, 2007, p. 753). With improvements in content and network management capabilities, perhaps the future of communications regulation may tend towards even more 'rough censorship' by communications industry stakeholders, which may include the reporting of those who generate and access seditious content.

The *Broadcasting Services (Anti-Terrorism Requirements for Open Narrowcasting Television Services) Standard* 2006 restricts the broadcasting of certain content on open narrowcasting services. The standard resulted from an investigation into the broadcast of the Lebanon-based satellite television

channel Al Manar by the subscription television narrowcasting licensee Television and Radio Broadcasting Services Australia Pty Limited (TARBS) on 5 November 2003 (ACMA, 2004, Press Release). During the investigation, the Australian Broadcasting Authority (as it then was) considered whether:

> …certain material in programmes provided by Al Manar was in breach of Federal anti-terrorism laws, including material that appeared to solicit funds for organizations linked with terrorism. It concluded that if such material were broadcast with the intent to solicit funds and the broadcaster was reckless as to whether or not the funds would be used for terrorism purposes, it could constitute a use of the broadcasting service in the commission of an offence. (ACMA, 2004, ABA Investigation into Al Manar programming on TARBS, News Release, 22 October 2004, www.acma.gov.au, retrieved on 6 September 2006)

The investigation was never finalised, however, the *Broadcasting Services (Anti-terrorism Requirements for Open Narrowcasting Television Services) Standard 2006* was passed in March 2006. The object of the standard is to prevent the broadcasting of programs that encourage people to join or finance terrorist organisations (*Broadcasting Services* (*Anti-terrorism Requirements for Open Narrowcasting Television Services) Standard 2006*, s 3) The standard, among other things, does not prevent the licensee from reporting the news, expressing a political opinion or broadcasting a programme that merely gives information about, or promotes beliefs or opinions of, a terrorist organization (*Broadcasting Services (Anti-terrorism Requirements for Open Narrowcasting Television Services) Standard 2006*, ss 8 and 9).

Ordinary commercial and subscription television broadcasters are governed by their relevant Industry Codes of Practice and licence conditions as set out in the *Broadcasting Services Act 1992*. All broadcasting services are prohibited from using the broadcasting licence to commission an offence. The narrowcasting standard highlights the limitations of the regulatory framework to effectively regulate for national security purposes. The standard only applies to narrowcasting services licensed under the *Broadcasting Services Act 1992*. Internet Protocol based television (IPTV) reveal that certain services continue to remain outside the regulatory frameworks for content.

The shift towards security focused communications regulation

Taken together, the changes to communications regulation in the interests

of national security after 11 September, 2001, which include 'the almost constant pattern of revision of the telecommunications interception framework' (Bronitt & Stellios, 2006, p. 414), and the broader amendments covering telecommunications licensing, classification of terrorism-related content, sedition, restrictions on press freedoms, secrecy, terrorism advocacy and narrowcasting content standards, demonstrate a marked shift towards security-focused communications regulation. Yet there are multiple points of contact in the national security-communications regulatory interface running in parallel which get lost in a discourse which is focused on human rights, loss of privacy, press freedom and free speech.

The surveillance society?

Private and public activities, some of which are legal and others which are illegal, some of which are innocent and others that are dishonest, are undertaken with the help of communications and information technology systems, from the classroom to the café; from working-from-home to 'skyping' a friend in another country. The changes wrought by the communications and information technologies of the last decade are arguably unprecedented. The interconnectedness of life in the developed world and its impact on our lives has been well documented by a large number of scholars. The breadth and depth of scholarship is detailed and multi-disciplinary.

The regulation of networked communications and information technology systems is a contentious subject. The internet, in all its layered complexity, has seriously challenged the ability of national governments to regulate its uses and abuses. Bennett-Moses makes the point that technologies such as the Internet 'motivate legal change by their very existence'. (Bennett-Moses, 2007, p. 4) Bennett-Moses explains:

> Technologies such as railroads, genetic testing, *in vitro* fertilization, computing and the internet were not designed to evade the law or employ it for gain, but rather were created for independent reasons. Their relationship with the law is not intentional. (Bennett-Moses, 2007, p. 4)

The traditional means of regulating through the legislative silos of telecommunications, radiocommunications and broadcasting have been pushed to the limit by the internet and emerging technologies (Chapman, 2008, p. 2)

These new 'mediums' do not fit into the old regulatory categories. The regulatory body responsible for the communications environment, the Australian Media and Communications Authority (ACMA), operates as a semiconverged regulator and considers its legacy legislation in terms of 'broken concepts' (Chapman, 2008, p. 2). There are serious jurisdictional and structural issues still to be solved as each new technology comes online.

As a result of the enabling capability of communications and information technology systems, many participants in the current debate on the 'war on terror' believe that the communications environment has facilitated the introduction of unprecedented '*microregulation*', '*command and control*' technologies and solutions and *cradle to grave* surveillance (Michael & Michael, 2006, p. 360). Some view the developments of the last decade as a shift towards a surveillance society where privacy is traded for access to goods and services (Tregoning, 2006, p. 194).

Australians are subject to video surveillance in public places and private spaces. Australians leave digital tracks all over the communications environment. Our communications are able to be tracked and traced, stored and accessed with greater ease than perhaps any other time in history. This perspective is somewhat at odds with the values underpinning the regulation of the communications environment. Those values are partly based on competition, full and open access, efficiency and speed (Raiche, 2005, p. 1). The impact of technology based surveillance regulation on networks is thought, on one level, to be costly, intrusive and an impediment to network efficiency (Branch, 2003, p. 38). In some sectors, it is also thought of as an infringement of basic democratic, human rights, such as privacy and free speech.

Large media and telecommunications companies are strategically aligned with the Federal government over national security policy agenda through their involvement in the Business-Government Taskforce on Critical Infrastructure. Bull and Craig's research shows that all levels of government in Australia have recognised the need for critical infrastructure protection and identifies information technology and communications as critical infrastructure (Bull & Craig, 2006, p. 211). The strategic alliance between government and industry in the area of critical infrastructure protection seeks to strengthen the alignment of communications regulation with national security policy (Business-Government Taskforce on Critical Infrastructure Report, 2002, p. 2). The Business-Government Taskforce on Critical Infrastructure Report makes the following observation:

> Critical infrastructure protection is a complex issue with links to almost every industry sector. It is not possible to separate neatly the need to protect critical infrastructure from physical attack, and the need to assure the operation of the national information infrastructure. The Business/ Government Task Force has considered a wide range of issues, and has developed six recommendations. The recommendations are based on the principles of fostering a partnership between the public and private sectors, creating a culture of security addressing both IT and physical security concerns, and building on the work of existing security and consequence management arrangements. The Task Force recommends that a network of consultative groups be formed to address both policy and operational information sharing needs of business and government. (Business-Government Taskforce on Critical Infrastructure Report, 2002, p. 2)

There has been significant collaboration and co-operation at the level of infrastructure protection. However the public record of industry engagement over the post-9/11 expansion of telecommunications interception and surveillance powers demonstrates a far less dedicated level of interest. This however can be contrasted with the actions of the media entities who formed the 'Australia's right to know' campaign in an attempt to heighten community awareness and government responsiveness to their business concerns about the 'chilling effect' of the national security content regulation on free speech and access to information (Murphy, 2007, p.5; Moore, 2007, p.1).

The relationship between government and industry needs to be more fully appreciated and explored, in order for citizens and businesses to understand the impact of the national security legislative framework on Australian society and its governance. An understanding of the roles that are played by communications industry participants is crucial for a clearer picture of the regulatory landscape and its compliance and accountability framework. New technologies and innovations challenge the existing communications regulatory frameworks, including the relationships which many take for granted.

This is no easy undertaking. The regulatory framework must grapple with the live streaming of 'Big Brother' over the internet (Idato, 2006, p. 6) to pornography on hand-held communications devices; from social networking sites and other advanced internet technologies (Pascu et al., 2007, pp. 12-13) to off-shore gambling servers. Idato makes the comment that:

> Next-generation technology provides a range of solutions to the dilemma of managing controversial TV content and controlling who has access to it - smart-classification software that can control what can be watched and when, parental lock systems that can put entire channels out of the hands of children, and more. But rather than innovate, the government has hamstrung itself by kowtowing to the medieval fiefdoms that control our increasingly anachronistic broadcast TV sector. (Idato, 2006, p. 6)

Finally, the communications regulatory framework must grapple with the changed relationship between communications industry stakeholders and the state. There are many more creators and potential creators, facilitators and aggregators of 'telecommunications data' in a converged communications environment than the simple carrier/carriage service provider/content service provider categorisation of traditional telecommunications and broadcasting regulation. These developments open up issues of liability, compliance, criminal responsibility and cost, which are of concern to communications industry stakeholders (Nicholls & Rowland, 2007, p. 83). In relation to the post-9/11 amendments to the telecommunications interception regime in particular, communications industry stakeholders have felt obliged to accommodate the government and its national security policy objectives without questioning (or arguably, being able to question) the impact or potential long term impact on their customers or their businesses (Nicholls & Rowland, 2007, p. 83).

Conclusion

Since the terrorist attacks of 11 September 2001 in Australia and internationally, it is arguable that the paradigm of security, national security and its discourse have been 'waxing' to use the parlance often used in respect of the defence power under the Australian constitution.

Our technologically connected lifestyle enables pervasive, more accurate surveillance; less privacy; and direct targeting of political dissidence justified on the basis of 'national security' (which is as intangible and elusive and as difficult to safely define as 'terrorism') (Tregoning, 2004, p. 169). New services such as MySpace and FaceBook have seriously challenged the value of privacy in that context. Not only have those services opened up the potential for 'cradle to grave' surveillance (Michael & Michael, 2006,

p. 360), the cultural development moves the debate beyond privacy to the issue of communicative freedom, which is arguably a broader concept encompassing an individual's choices about the access, use and disclosure of their information (Bowrey, 2005, p. 178).

However, as for what this may mean for the future of communications regulation in Australia, Hills makes this point in respect of the UK and the US which is arguably true for Australia:

> Today, the internationalisation of communications has created a situation where, in the interests of security, the relation of government to citizens is focused on fear, suspicion and surveillance, not democracy and the protection of human rights.

In order to do something about this, this article, by highlighting the 'convergences and tactical linkages' at the interface of national security and communications regulation, has tried to provide some suggestions of policy areas requiring greater future consideration and discussion amongst citizens, business and government. National security deserves recognition amongst the other 'top six trends' in communications policy today, as it raises important matters about the future of a vibrant communications environment which is as Hills notes 'necessary in a democratic industrialised society for people to fulfill their roles as citizens' (Hills, 2006, p. 195).

References

Andrejevic, M. (2006). Interactive insecurity: The participatory promise of ready.gov, *Cultural Studies*, 20(4-5): p. 441-458.

Attorney-General's Department response to the Senate Legal and Constitutional Affairs Committee Inquiry into the *Telecommunications (Interception and Access) Amendment Bill 2007*. Retrieved on 14 September 2007, from: www.aph.gov.au/Senate/committee/legcon_ctte/telecommunications_interception/additional_information/amended_ag_answers.pdf

Australian Communications and Media Authority (2004). ABA investigation into Al Manar programming on TARBS. News Release, 22 October 2004. Retrieved on 6 September 2006, from: www.acma.gov.au

Australian Communications and Media Authority (2008). *Top six trends in communications and media technologies, applications and services – possible implications*. Canberra: Australian Communications and Media Authority.

Australian Communications Authority (2005). *Vision 20/20: Future scenarios for the communications industry—implications for regulation, final report*. Canberra: Australian Communications Authority.

Australian Mobile Telecommunications Association, Submission to the Senate Inquiry *Telecommunications (Interception and Access) Amendment Bill 2007*.

Bennett-Moses, L. (2007). Recurring dilemmas: The law's race to keep up with technological change. [2007] *UNSWLRS* 21, 18 May 2007, p. 4.

Berg, C. and Tobin, H. (2007). Big brother versus big brother: How politicians failed to understand reality television and in their confusion instead decided to regulate the internet. *Institute of Public Affairs Review*, 59(2): pp. 32-36.

Bowrey, K. (2005). *Law and internet cultures*. Cambridge: Cambridge University Press.

Branch P. (2003). Lawful interception of the internet. *Australian Journal of Emerging Technologies and Society*, 1(1): pp. 38-51.

Bronitt, S. and Stellios, J. (2006). Regulating telecommunications interception and access in the twenty-first century—technological evolution or legal revolution?' *Prometheus*, 24(4): pp. 413-428.

Bronitt, S. and Stellios, J. (2006). Sedition, security and human rights: 'unbalanced law' reform in the 'war on terror'. *Melbourne University Law Review*, 30: pp. 923-960.

Bull, M. and Craig, M. (2006). The problem of terrorism: balancing risk between state and civil responsibilities. *Current Issues in Criminal Justice*, 18(2): pp. 202-228.

Business-Government Taskforce on Critical Infrastructure Report, May 2002.

Campbell, Senator I. (2004). Second reading speech, *Communications Legislation Amendment (No. 1) Act 2004*. Hansard, Parliament of Australia.

Chapman, C. (2008). The flexibility and benefits of Australia's co-regulatory approach. Speech by Chris Chapman to the 14th European Conference of Postal and Telecommunications Administrations (CEPT), Strasbourg, France, April.

Electronic Frontiers Australia. Submission to the Senate Inquiry into the *Telecommunications Amendment (Interception and Access) Bill 2007*.

Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2008*.

Fitzgerald, B., Fitzgerald, A., Middleton, G., Lim, Y. F., Beale, T. (2007). *Internet and e-commerce law—technology, law and policy*. Pyrmont, NSW: LawbookCo.

Hills, J. (2006). What's new? War, censorship and global transmission: From telegraph to the internet. *The International Communications Gazette*, 68(3): pp. 195-216.

Idato, M. (2006, July 31). Bad taste, not war, is hell. *The Sydney Morning Herald*, p. 2.

McClelland, R. (2008). Second reading speech. *Telecommunications (Interception and Access) Amendment Bill 2008*, Hansard, Parliament of Australia.

Michael, K. and Michael, M. G. (2006). National security: The social Implications of the politics of transparency. *Prometheus*, 24(4): pp.359-363.

Moore, M. (2007, May 11). Media rally to defend free speech. *The Sydney Morning Herald*.

Murphy, K. (2007, May 10). Media unites on free speech. *The Age*, p. 5.

Nicholls, R. and Rowland, M. (2007). Message in a bottle: Stored communications interception as practised in Australia. In Michael, K. and Michael, M. G. (Eds.), *From dataveillance to uberveillance and the realpolitik of the transparent society*, The Second Workshop on the Social Implications of National Security, University of Wollongong, IP Location-Based Services Research Program (Faculty of Infomatics) jointly with the Centre for Transnational Crime Prevention (Faculty of Law), 29 October 2007.

Pascu, C., Osimo, D., Ulbich, M., Turlea, G., and Burgelman, J. C. (2007). 'The potential disruptive impact of internet 2 based technologies. *First Monday*, 12(3): pp. 12-13.

Raiche, H. (2005). The policy context. In Grant, A. (Ed.), *Australian telecommunications regulation*, [2nd edition] (p. 1). Sydney: UNSW Press.

RFC 2822 (2007). Retrieved on 14 September 2007, from: www.ietf.org/rfc/rfc2822.txt?number=2822

Telecommunications (Interception and Access) Amendment Bill 2007, Explanatory Memorandum, retrieved on 14 September 2007, from: parlinfoweb.aph.gov.au/piweb/Repository/Legis/ems/Linked/14060702.pdf

Tregoning, M. (2004). A new panopticon: Surveillance and privacy after September 11. 9 *Media & Arts Law Review* 169: pp. 169-198.

Vodafone Submission (2003) *Communications Legislation Amendment Bill (No.2), Senate Environment, Communications, Information Technology and the Arts Legislation Committee*, 22 September 2003.

Weimann, G. (2006). Fighting back: Responses to terrorism on the internet, and their cost. In *Terror on the internet* (pp. 173-202) Washington, DC: United States Institute of Peace Press.

Williams, D., Attorney-General (1999). Second reading speech, *Telecommunications (Interception) Amendment Bill 1999*, Hansard, Parliament of Australia.

Zittrain, J. (2008). *The future of the internet and how to stop it*. London: Allen Lane.

Susanne Lloyd-Jones is an associate lecturer in the Macquarie Law School at Macquarie University and a PhD candidate in the Faculty of Law at the University of New South Wales. She has practised as a solicitor in Sydney, and has worked as an in-house legal counsel for an Australian subscription television broadcaster, where she specialised in regulatory affairs. *The author would like to thank Professor Kathy Bowrey and Dr Andrew Lynch from the Faculty of Law at the UNSW for their comments on the draft of this paper. All errors and omissions are the responsibility of the author.*
Susanne.Lloyd-Jones@law.mq.edu.au