Submission No 41

Inquiry into potential reforms of National Security Legislation

Name: Andrew Brunatti & Neveen Abdalla

Organisation: Brunel Centre for Intelligence and Security Studies
Brunel University, UK

Inquiry into Potential Reforms of National Security Legislation

Submission to the
Parliamentary Joint Committee on Intelligence and Security
Parliament of Australia

Andrew Brunatti and Neveen Abdalla

Brunel Centre for Intelligence and Security Studies
Brunel University, UK

August 2012

Authors' Information and Affiliation

Neveen Abdalla
MA Candidate (Intelligence and Security Studies)

Andrew Brunatti
PhD Candidate (Politics and History)

Brunel Centre for Intelligence and Security Studies (BCISS)
Brunel University
Kingston Lane
Uxbridge, Middlesex
UB8 3PH
UK

Submission Summary

This submission examines current trends in digital communications and the use of warrants under the lawful access regime to maintain a balance between privacy and security in Australia. It illustrates that a fundamental challenge facing the current lawful access regime is the non-existence of verifiable individual identity in the use of communications in cyberspace. The submission then proposes the creation of a National Digital Identification Regime to reinforce the long-term integrity of both an individual's online identity and the effectiveness of the lawful access regime.

Introduction

There are few issues that will have a more lasting effect on the national security environment than the growth of cyberspace, and particularly the growing complexity of communications infrastructure associated with the digital realm. While cyberspace is not, in itself, a new concept, the rate of its growth and complexity is demanding a much more vigorous policy response that democratic populations rightly concerned with privacy, but at the same time increasingly willing users of cyberspace, have already found unsettling.

This is a particularly acute issue within the security and law enforcement sector where traditional capabilities are in danger of eroding more quickly and efforts at modernization are faced with new complexities. Responses by the state to this environment must be balanced and effective, for at one extreme is the potential infringement of privacy and at the other, the failure to adequately protect a state's population from threats.

The Parliamentary Joint Committee on Intelligence and Security's[1] *Inquiry into Potential Reforms of National Security Legislation* comes at a critical time. Australia's domestic and regional environments are facing consistent threats including terrorism, organized crime, espionage and cyberattack. None of these threats reflect traditional geographic boundaries; all are agile and fluid by nature and all have a well-developed presence in the digital environment. Indeed, as citizens move more of their lives online, threats will inevitably continue to follow. Cyberspace has come to suit the criminal more than the traditional telecommunications environment. This is partly due to gaps in the capability of law enforcement or security agencies. More basically, this is also because fundamental concepts such as verifiable individual identity, signified in the physical world in such mundane forms as drivers licenses or tax file numbers, are seen to be inapplicable in our digital lives.

[1] Hereafter referred to as PJCIS, or simply 'the Committee.'

This submission seeks to show that one of the foundational issues in the modernization of the lawful access[2] regime is how the concept of identity has been diluted within the digital environment and that this must be remedied for any lawful access regime to prove effective in the long-term.

Subsequently, alongside the proposed immediate changes there is need to consider the creation of a digital identification regime, supported in legislation and with appropriate safeguards and information security measures. This would provide for individual identification in cyberspace much the way a drivers license provides identification on Australia's roadways. While this is ultimately a larger endeavor than the reforms currently proposed, the authors believe that the need to systematize accurate means of individual identity in cyberspace underlies the long-term efficacy of many of the proposed reforms relating to lawful access in the discussion paper prepared by the Attorney General's Department (AGD). [3] Additionally, without such a regime the state's efforts to maintain public safety will have increasing trouble catching up to the expansion of cyberspace. *Ad hoc* reforms have led to inconsistent thresholds and a multiplicity of processes, as the AGD's discussion paper points out,[4] and this may only serve to increase the risk to privacy. Delaying a more strategic response makes viable solutions more complex, expensive, and politically sensitive for both public and private sector actors.

While the submission touches on aspects related to many of the Committee's terms of reference, it particularly addresses the following:

Term of Reference 2

"The inquiry should consider the effectiveness and implications of the proposals to ensure law enforcement, intelligence and security agencies can meet:

---

[2] For the purposes of this submission, 'lawful access' refers to the ability of law enforcement and intelligence agencies to access communications content and data through interception, stored data, and subscriber information through the use of legislatively supported special powers.

[3] Attorney General's Department, *Equipping Australia Against Emerging and Evolving Threats*, (Canberra: Australian Government, 2012)

[4] *Ibid*. p.17: "The pace of change in the last decade has meant [the TIA Act] has required frequent amendment resulting in duplication and complexity that makes the Act difficult to navigate and which creates the risk that the law will not be applied as Parliament intended."

a) the challenges of new and emerging technologies upon agencies' capabilities

b) The requirements of a modern intelligence and security agency legislative framework, and to enhance cooperation between agencies, and

c) The need for enhancements to the security of the telecommunications sector."

Term of Reference 3

"The Committee should have regard to whether the proposed responses:

a) contain appropriate safeguards for protecting the human rights and privacy of individuals and are proportionate to any threat to national security and the security of the Australian private sector

b) apply reasonable obligations upon the telecommunications industry whilst at the same time minimizing cost and impact on business operations in the telecommunications sector and the potential for follow on effects to consumers, the economy and international competition, and

c) will address law enforcement reduction of capabilities from new technologies and business environment, which has a flow-on effect to security agencies."

The Digital Environment and Individual Identity.

The global rate of fixed and mobile network operators, VoIP,[5] satellite and internet service providers has grown exponentially over the course of the last several decades, and in the current climate it is highly likely that demand for additional global-reach services will increase. By 2016, it is estimated that there will be over 10 billion mobile phones in the world, carrying 130 exabytes of data annually (equal to 33 billion DVDs). [6] Smartphones, which have the capability of a mobile computing platform, currently account for 12% of the world's global phone market and make up 82% of global handset traffic. The rapidly increasing rate of electronic services develops in tandem with the increasing complexity of capabilities. Whereas in the 1970s the primary means of long distance communication was through fixed telephone lines or postal mail, today, the introduction of broadband has introduced a **"Unified Communications System"**

[5] 'Voice over Internet Protocol' services, such as Skype.

[6] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2011–2016
http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html

(UCS): real time (or near-real time) communication which is an amalgam of instant messaging, telephony, video conferencing, data sharing, interactive white boards, voice-mail, e-mail, SMS, MMS, and fax,[7] which serves to unite communications both nationally and transnationally faster than at any point in the past.

The increased use of digital communication brings a concurrent increase in cyber threats globally. Key findings of a recent study commissioned by Detica and BAE Systems suggest that the global community is entering an "age of digital crime" as online and offline worlds converge. The study states:

- 80% of digital crime originates in some form of organized activity.
- 43% of organised digital crime group members are over 35 years of age, whereas only 29 % are under 25.
- Half of groups comprise six individuals or more, with one quarter comprising 11 or more. However, group size does not correlate with the impact or scope of offending – in the digital era, a small number can inflict large damage.
- 25 % of active groups have operated for less than six months.
- Offline groups are increasingly using digital tools in ways that further 'traditional' criminal behaviour, such as gang member recruitment or newer activities such as pin code theft.[8]

In addition to security risks, the economic cost of these cybercrimes, whether initiated by groups or individuals, is rising. A 2011 study conducted by Norton estimates that the annual global cost of cybercrime is USD 114 billion,[9] and the cost of combating cybercrime in the UK was came to GBP 27 billion

---

[7] "What UC Is and Isn't." What UC Is and Isn't. N.p., n.d. Web. 29 July 2012. <http://searchunifiedcommunications.techtarget.com/feature/What-UC-is-and-isnt>.

[8] John Grieve Centre for Policing and Security at London Metropolitan University. Rep. N.p.: n.p., 2011. *'Organised Crime in the Digital Age'*. BAE Systems, Detica, 29 Mar. 2012. Web. 30 July 2012. http://www.baesystemsdetica.com/resources/organised-crime-in-the-digital-age/

[9] http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02

(approximately USD 40 billion) between 2010-2011.[10] To put this into perspective, the total value of the world's cocaine market in 2011 was USD 85 billion, and the total cost of the heroin trade was USD 61 billion.[11]

While crime committed in cyberspace is a rapidly growing concern, of equal and possibly more pressing concern is the use of more complex, and widely accessible, digital communications to plan criminal acts in the offline world. The ability of security intelligence and law enforcement agencies to intercept digital communications or monitor online venues under lawful authority has been integral to the successful dismantling of significant terrorist plots, such as Operation PENDENNIS in Australia, Project O-SAGE in Canada, and Operations CREVICE and OVERT in the United Kingdom. However new technologies such as VoIP communications have opened up gaps in interception and monitoring capability.[12] These services are widely available and, more importantly, can be utilized with no verifiable form of identification. Subscriber information can be easily falsified, leaving usernames connected to ghost identities.

The difficulty in securing warrants enabling law enforcement and security agencies (hereafter referred to LE/S agencies) to investigate online criminality, or offline crimes planned online, is two-fold: cyber crimes are often trans-jurisdictional, and those who wish to commit a crime can remain anonymous within the realms of cyberspace. Individuals can generate unidentifiable or 'dead-end' e-mail addresses, use aliases within the context of social media, pay cash for a no-check 'pay-as-you-go' mobile phone, acquire access to transnational internets using multiple or hidden IP addresses, and incite crimes ranging from 'hacktivism' to identity theft by using crowd-sourcing or channeling through victimised systems. In short, a cyber-savvy individual can develop a completely anonymous identity with little or no connection to his actual identity, making a warrant application, which requires robust identification of the subject, increasingly difficult.

---

[10] John Grieve Centre for Policing and Security at London Metropolitan University. *'Organised Crime in the Digital Age'*.
[11] http://www.unodc.org/unodc/en/data-and-analysis/WDR-2011.html
[12] See for instance, Hines, N. 'Skype Opens Private Line to Security Snoopers' *The London Times*, July 27 2012; 'Italy: Govt Probes Suspected Mafia Use of Skype' *Adnkronos International*, Feb 18 2009.

Because the increasing rate of a population's use of cyberspace correlates to the escalating rate of cybercrime or crimes planned in cyberspace, there is an urgent need to streamline lawful access to communications and data that correlates to a specific person. However, any system which is put in place must also be adequately protected by INFOSEC[13] measures and ensure privacy safeguards for citizens. This generates a need to reassess the way individuals and nations perceive and utilise the Internet. Currently, individuals have the ability to sever themselves from their online identity. Ultimately, it is necessary to construct a system where online identity is directly correlated to actual identity. This then allows tools such as named person warrants, which are flexible but infused with necessary safeguards, to adequately address all aspects of an individual's digital activity. Conversely, victims of cybercrime would also have a means of tracking and reporting inconsistencies in their data via the use of a standardized online identity system.

The Digital Identity Deficit and Lawful Access Warrants.

The need for LE/S agencies to obtain special-powers warrants for intrusive investigatory methods is fundamental to the balance between security and privacy in a democratic system. The O'Connor and Major Commissions in Canada drew a distinction between propriety-based oversight (the ability to ensure security agencies operated within the law) and efficacy-based oversight (the ability to ensure that security agencies are able to operate efficiently).[14] While it may not seem so at first glance, these goals are complimentary and the warrant regime is fundamental to both.

Warrant applications subject the agencies' investigatory plans to external scrutiny by legal or elected actors ensuring lawful compliance and political

---

[13] Information security.

[14] O'Conner, D. *A New Review Mechanism for the RCMP's National Security Activities*, Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar (Ottawa: Government of Canada, 2006); Major, J. *Final Report, Volume 3: The Relationship Between Intelligence and Evidence and the Challenges of Terrorism Prosecutions*, Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 (Ottawa: Government of Canada, 2010)

accountability. This aspect of the regime is obviously critical to maintaining propriety-based oversight and is the principle reasoning behind warrants.

Just as importantly however, warrants force agencies to identify specific subjects of investigations,[15] ensuring their capability is targeted and formalizing the links with private sector actors that are operationally necessary. The introduction of 'named person warrants'[16] increased the operational efficiency of the agencies by allowing flexibility in the *breadth* of interception (adding or subtracting new services to be intercepted as the target of the warrant changed methods of communication) as long as the interception was concretely tied to a *specific target*. The model of the named person warrant is even more important as the array of services available to the subject of an investigation becomes wider and their ability to easily switch between services grows.[17] Indeed, the concept underpinning named person warrants is increasingly important in maintaining the operational effectiveness of the agencies. In a sense, the named person warrant provides the target-specific enclosure under which agencies' lawful access activities can expand and contract as demanded operationally. Given the digital environment described previously, and also outlined in the AGD's discussion paper, this is a key capability. In short, the robustness of the warrant regime is critical to both proprietary and efficacy concerns.

With the growing importance of the named person warrant model,[18] and the continued general importance of the warrant regime in maintaining both privacy and efficiency, the decline of verifiable individual identity in cyberspace presents a fundamental challenge. Warrant applications have, under statute, the

---

[15] See *Australian Security Intelligence Organisation Act 1979*, Part 3 Sec.17(1)(e) and the *Telecommunications (Interception and Access) Act 1979*, Part 2-2, Sec.11A-D

[16] See Sherman, T. *Telecommunications (Interception) Act 1979: Report of Review of Named Person Warrants and Other Matters*. (Canberra: Commonwealth of Australia, 2003)

[17] It is important to note that the named person warrant was introduced to deal with the growth of easily transferrable SIM cards in telecommunications, as well as the growth of mobile, fax and email services. The concept however is actually more applicable in today's environment where a subject may switch between landlines, mobiles, email, VoIP and several other forms of communications almost seamlessly.

[18] Exemplified by the proposal within the current reform package to create a named person warrant provision within the ASIO Act. See Attorney General's Department, *Equipping Australia Against Emerging and Evolving Threats*, (Canberra: Australian Government, 2012), p. 9, 47.

requirement to identify the subject of the warrant. Part 2-2 Sec.9(2) of the *Telecommunications (Interception and Access) Act 1979* (hereafter referred to as the TIA Act) states that:

> *A request by the Director-General of Security for the issue of a warrant in respect of a telecommunications service:*
>
> *(a) shall include a description of the service sufficient to identify it, including:*
>
> *(i) the name, address, and occupation of the subscriber (if any) to the service; and*
>
> *(ii) the number (if any) allotted to the service by the carrier; and*
>
> *(b) shall specify the facts and other grounds on which the Director-General of Security considers it necessary that the warrant be issued and, where relevant, the grounds on which the Director-General of Security suspects a person of being engaged in, or of being likely to engage in, actions prejudicial to security.*[19]

More stark is the requirement under Sec.9A(2) regarding named person warrants, which states:

> *A request by the Director-General of Security for the issue of a warrant in respect of a person:*
>
> *(a) must include the name or names by which the person is known; and*
>
> *(b) must include details (to the extent that these are known to the Director-General of Security) sufficient to identify the telecommunications services the person is using, or is likely to use;*[20]

It must be noted that these requirements, particularly in the case of 'single service warrants' (the traditional form of warrant) covered in Sec.9, were put in place at a time when investigations were principally subject-generated. That is to say that the LE/S agencies would determine a subject of interest, obtain their identity, and subsequently expand their investigation to determine the subject's activities. However, in the current environment the LE/S agency is just as likely to be monitoring an online chat room or file transfer site. Here, the initial investigative lead is likely to be the *activity* itself, with the subjects hidden behind usernames connected to false subscriber information. The LE/S agency may detect there is a subject, or several subjects of interest, based on the activity,

---

[19] *Telecommunications (Interception and Access) Act 1979*, Part 2-2, Sec.9(2).
[20] *Telecommunications (Interception and Access) Act 1979*, Part 2-2, Sec.9A(2).

but are unable to determine the necessary identities to obtain subject-specific warrants to further their investigations.

As already noted, the ability to hide one's identity is much greater in cyberspace. This is due in large part to the fact that the new digital environment has grown up without requirements for verifiable identification that are commonplace in the offline world. Without a strategic approach to identity within cyberspace, it will become increasingly difficult to maintain the sophisticated tools, such as the warrant regime for lawful access, which balance security and privacy. Without the ability to verify digital identities, both privacy and security risks increase, including but not limited to:

- the risk of innocent citizens' privacy being infringed upon if there is incorrect identification in warrant applications;
- the risk of LE/S agencies becoming risk-averse and losing investigatory capability;
- the risk to privacy inherent in resorting to less targeted methods of authorizing access in order to maintain capability.

Given these risks, it is necessary to support the long-term effectiveness of the lawful access regime with a larger strategic initiative that reinforces verifiable individual identification within cyberspace. This initiative could be termed a 'National Digital Identification Regime.'

A National Digital Identification Regime

In order to maintain a robust yet efficient warrant system and to protect the integrity of individual identity in cyberspace, consideration should be given to the creation of a single point of access which would act as an individual's unique gateway to multiple digital communications services. It would also act as the single point of reference for LE/S agencies to accurately determine what online services an individual was associated with. In terms of security or criminal investigations, an issued warrant could therefore encompass multiple communications services but remain strictly limited to the individual targeted by

the warrant. In order to do this, an opportunity lies in the creation of a unique digital identifier for each individual.

The development of a **National Digital Identification Regime (NDIR)** would create the ability to streamline warrants while providing increased security to individual users at almost every access point in the UCS. Under the NDIR, as it pertains to citizens, the government would provide each citizen with a unique number which must be used when making purchases, including fixed and mobile phones, SIM cards, and computers or computing items. Similarly, that **National Digital Identifier (NDI)** would be entered at any public Internet access point, or entered on a family computing device and updated on a monthly or bi-monthly basis to ensure the computing device has not changed hands without notice. It is important to note that this does not affect an individual's ability to generate an online "alias" for social media or e-mail addresses; rather, it serves as a "behind-the-scenes" identifier for security purpose. For instance, in addition to streamlining LE/S security access, a web user who forgets their password may be asked to enter their NDI and answer a security question to gain access into a specific site.

For current Australian citizens, this identifier could "piggy-back" on an existing infrastructure (for example, assigned along with Medicare numbers or birth certificates), or it could coincide with existing identifiers, making, for instance, one's Tax File Number and NDI the same.

For visitors coming to Australia for a limited amount of time, a small fee could be included in the purchase of a holiday, school, work, or other visa to obtain a temporary NDI, or **Digital Visa (DV)**. This DV will allow visitors to access the Internet, and if necessary, purchase of mobile phones or computing devices. Digital Visas could have an identifying code that first classifies the nationality of origin for entering civilians. For example, John W. Smith, visiting from the United Kingdom, may be issued with UK-JWS-123-456-789. In this manner, it is also easy to detect increases in unusual activity stemming from visitors in a particular region or nation.

Within the NDIR lies the premise that users must register an NDI number to create an e-mail address or obtain a telephone number. For citizens with

existing e-mail addresses, a page could be developed in which a user registers and verifies an e-mail address or addresses with their NDI. For a limited period of time, pages requiring submission of an e-mail address to access content could require NDI verification as well. Thus, when a person logs into a social media account such as Facebook by using their e-mail address, there is a record of ownership of that email account, eliminating much of the risk for anonymous pages or dead-end e-mail links.

Likewise, multi-national businesses or corporations who have commerce with public or private sector organizations must adhere to the NDIR standards. This includes non-Australian business advertising on a .au extension, or businesses with a .com, .org, or other extension which allows advertising from Australian organizations.

Under NDIR, any computing device or telephone system, e-mail address or social media account, which is linked to an individual's NDI, is eligible for access under a warrant, and data can be collected from access points such as CSPs, web hosting sites, or web pages, to link a user to a specific location or computer. In the event of the user accessing the Internet through a hidden IP address, a de-cloaking engine can be used to determine the actual IP address of a specific mobile phone or computing device.

For the purpose of security, storage and maintenance, digital services, such as registered mobile phone operators, CSP data, VoIP services and other "top-layer" data is to be kept on record under and individual's NDI, *but not content*. If a user chooses to obtain a new e-mail address, they will submit their NDI number and that e-mail address will be associated with their NDI number. However, *content and data can only be accessed by warrant* through C/CSPs, website hosts, or other sources which maintain a consistent record of user activity. As is already an aspect of the Committee's deliberations, requirements should be established to determine the length of time these activities must remain available for access under warrant.

Management of the NDIR would require efforts on the part of both public and private sector organizations; each would be required to establish a system for NDI verification and content storage within guidelines, as defined by

legislation. The principal public and private sector actors would be responsible, likely through the Interception Consultative Committee, for determining a central location for content uploads on a daily or weekly basis to the NDIR, ensuring that the database remains current, while sweeping content that goes beyond the statute of limitations on a daily or weekly basis. Flagged data or content that is preserved under a named person or NDI warrant should be identified and stored in a unique database.

In order to establish the NDIR in a timely manner, corporate tax incentives could be issued to companies that meet defined technical and administrative capabilities within a given timeframe. Conversely, organizations that fail to meet guidelines would receive a tax penalty or a fine, and be required to meet minimum standards within a certain period. Organizations should be tested on an annual or semi-annual basis do determine adherence to guidelines, and those responsible for the administration of the NDIR must remain alert to new methods of circumventing the system while developing further tools to stay abreast of new technologies or services.

It is recognized that a system such as the National Digital Identification Regime would be controversial, but when one considers, in perspective, the unquestioned requirements for identification in our offline lives, an identification regime in cyberspace becomes more understandable. If one of the core responsibilities of the democratic state is to maintain the security of its people, and indeed this is a provision that the citizenry expects from its government, then it is necessary to approach the security of our online lives with the same realism that we approach the security of our offline lives.

Within a citizen's offline existence, the need for verifiable identification is accepted as commonplace. In the United States, the Social Security Number provides a unique individual identifier across dozens of different services. The United Kingdom, Canada, and New Zealand employ unique identifiers for healthcare services, tax administration and other core government functions.[21] While Australia has not adopted a national identification number, the need to

[21] See, for instance, the Canadian Social Insurance Number (SIN), UK's National Insurance Number (NIN), and New Zealand's Inland Revenue Department number (IRD number) and National Health Index number (NHI number).

administer comprehensive services at a national level has already driven the creation of similar identification regimes including **Medicare numbers** and **Tax File Numbers**.

More generally, the ability to produce verifiable identification as a prerequisite for the use of infrastructure or services is a widely accepted concept. Driver licenses identify an individual as approved to utilize the nation's roadways, and vehicle identification numbers (VIN numbers) provide unique identifiers for the vehicles they drive. Individual identifiers are required for the provision of healthcare, and passport numbers grant access to international travel. Existing forms of identification, such as a driver's license or passport, are also required either directly or indirectly for many other purposes such as the acquisition of a bank account, the renting of accommodations, or simply the purchase of alcohol.

The concept of verifiable individual identity also has widely accepted precedent within cyberspace. The use of one's credit card, itself a form of verifiable identity, is necessary to engage in the vast majority of e-commerce and is reinforced by further safeguards provided by '3-D Secure' services such as Visa's *Verified by Visa* or Mastercard's *SecureCode*.

Yet while there is public acceptance of these existing verifiable identification regimes, a similar concept has not been applied to the multitude of digital communications services. It is useful to keep in mind that many of the identification regimes previously mentioned actually safeguard the integrity of the individual, combatting crimes such as identity fraud. An NDI regime would serve similar purposes, while also enabling a more sophisticated approach to cyberspace by LE/S agencies.

Concluding Points

Australia is at a turning point in its technological infrastructure; a turning point that supports the creation of the National Digital Identification Regime. The construction of the National Broadband Network (NBN) will bring exponentially greater Internet capacity to the doorstep of every Australian citizen. The NBN

endeavor will also create technological and administrative infrastructure that could support elements of the NDIR, such as centralized data storage. The country's robust response to cybersecurity and INFOSEC issues, signified by the international recognition of the Defence Signals Directorate as a leader in cybersecurity innovation,[22] indicates that Australia is well placed to ensure the security of information contained within the NDIR.

The current package of proposed reforms outlined in the AGD's discussion paper must be viewed not as a disproportionate expansion of government surveillance capability, but instead as the necessary and proportional response to the much larger expansion of our online lives. Indeed, as we have shown, there is a strong case for even more fundamental reform if the balance between security and privacy is to remain healthy as we move further into cyberspace.

As the pace of technological development increases, the difficulty and cost, in both time and money, associated with providing necessary security also increases. In 2005, the Blunn Review highlighted that the decreasing ability to identify targeted users and services for lawful access had, particularly in the case of SIM cards and GSM[23] handsets, already outpaced any foreseeable solution.[24] Blunn subsequently recommended that, "priority be given to developing a unique and indelible identifier of the source of telecommunications and therefore as a basis for access."[25] In Oceania, Internet usage has jumped from 7.6 to 23.9 million users between 2000 and 2011.[26] Globally, in 2011, the number of email accounts reached 3.1 billion.[27] The explosion of social media, combined with the already staggering number of digital communication services lends new

---

[22] SANS. 'Australian Defence Signals Directorate Wins US National Cybersecurity Innovation Award,' SANS Institute press release, October 24, 2011. https://www.sans.org/press/australian-defence-signals-directorate-national-cybersecurity-award.php

[23] Global System for Mobile communications.

[24] Blunn, A.S. *Report of the Review of the Regulation of Access to Communications*. (Canberra: Commonwealth of Australia, 2005) pp.45-46

[25] *Ibid*. p.46

[26] "World Internet Usage Statistics News and World PopulationStats." *World Internet Usage Statistics News and World PopulationStats*. Miniwatts Marketing Group, 29 July 2012. Web. 02 Aug. 2012. <http://www.internetworldstats.com/stats.htm>.

[27] "Internet 2011 in Numbers." *Internet 2011 in Numbers*. Pingdom, 17 Jan. 2012. Web. 02 Aug. 2012. <http://royal.pingdom.com/2012/01/17/internet-2011-in-numbers/>.

urgency to Blunn's 2005 recommendation. The growth, in scale and complexity, of digital communications intensifies the need to rectify our previous *laissez faire* approach to identity in cyberspace in a way that reinforces both the integrity of the lawful access regime and the integrity of an individual's online identity. While the Committee considers the proposed package of reforms, it should also consider recommending that these reforms be supported by a more strategic approach to maintaining verifiable individual identity in the digital environment of the 21st Century, potentially through the creation of the National Digital Identification Regime.