Australian contribution to the CWG-Internet

Ref CL-13/68

Introduction

Australia is pleased to provide this response to the question posed by the CWG-Internet in CL-13/68. That letter asked Member States to provide their positions on what actions have been undertaken by governments in relation to the international internet-related public policy issues identified in Annex 1 to Resolution 1305 (Council 2009). Accordingly, this response sets out the actions that the Australian Government is taking on a number of these identified issues. Where appropriate the Australian Government position on the issue more generally is also set out. Australia consulted widely both within and outside the Australian Government in the preparation of this response.

Australian internet related policy seeks to foster and reward innovation, drive productivity and empower individuals, while maintaining trust and confidence in Australia's digital economy and the online environment.

A common theme throughout this response is that while government plays an important role in responding to the range of issues identified - to provide the policy and legal frameworks, essential infrastructure and critical services - it cannot work alone. Effective responses require partnerships and shared responsibility through the active engagement and participation of the private sector, non-government bodies and citizens or in enabling them to respond to these issues within their own areas of expertise. Australia believes that developing a network of multi-stakeholder partnerships is central in ensuring a whole-of-nation approach to the development of internet policy.

International public policy issues pertaining to the Internet and the management of Internet resources, including domain names and addresses

Internationally, the global internet governance framework is based on a multi-stakeholder model, which brings together representatives from government, civil society, industry, non-government organisations, academia, and industry. Within this framework, stakeholders have different roles and responsibilities and it is difficult for any one group, including governments, to exercise undue influence in policy development.

The multi-stakeholder model has encouraged economic growth and innovation by maximising access – anyone anywhere can invent new applications, develop content, or create hardware or other standard-based technology and connect it with the global network. These arrangements underpin features that are crucial to the internet's success – its global nature, openness and dynamism – and ensure that it remains a global platform for economic and social innovation and development.

Governments have wide experience in public policy, and have an important role in any discussion about internet public policy, but they should not be the only voice. There is a broad range of public policy issues pertaining to the internet, such as security, privacy, access, and the administration of the technical protocols, which are often complex and interdependent. The multi-stakeholder model enables a full range of views to be expressed.

The Australian Government has been a strong supporter of this model, and actively participates in multi-stakeholder forums to encourage an open, secure and stable internet. Within the current multi-stakeholder framework, ICANN is a key decision-making forum for internet governance and domain name policy. ICANN's multi-stakeholder model brings together representatives from diverse sectors who work together to set the technical and policy framework for the stable and effective

operation of the global internet. The Australian Government has participated in ICANN's Governmental Advisory Committee since its inception, and will continue to work to improve and strengthen the multi-stakeholder model as the internet evolves.

Multilingualisation of the internet including Internationalised (multilingual) Domain Names

The multilingualisation of the internet will allow users to use the internet in different languages and scripts, which will assist in making the internet more culturally diverse. The ability to access and produce content in different in their own language will offer all internet users more choices in their avenues for communication, and help them to benefit from the opportunities that the internet provides. Governments have a role in supporting the progress of this important policy issue. The Australian Government is a strong supporter of ICANN's multi-stakeholder approach to internet-related policy development, and its ongoing work to introduce internationalised domain names (IDNs) into the Domain Name System.

The security, safety, continuity, sustainability, and robustness of the Internet

The Australian Government undertakes various programs to raise awareness amongst small-to-medium enterprises, along with the community more generally, of cyber security risks and the measures they can take to protect themselves and their business(es). The Stay Smart Online Program provides information targeted to individuals and small businesses to increase their online confidence and engagement by actively protecting their own, and others', personal and financial information online. The Australian Government has also partnered with industry in the implementation of the Internet Service Providers (ISPs) voluntary code of practice for industry self-regulation in the area of cyber security – better known as the icode. At present, more than 30 ISPs are signatories to the icode. This includes a number of small and medium ISPs and most of Australia's largest carriage service providers, representing up to 90 per cent of the home user market.

CERT Australia is the national computer emergency response team for Australia and the point of contact for international engagement with the global network of computer emergency response teams. It is the point of contact for operational cyber security issues affecting Australian businesses and is a trusted source of expert & actionable cyber security information.

Combating Cybercrime

Australia considers that ensuring an effective response to cybercrime is a priority for governments. Australia released its National Plan to Combat Cybercrime in July 2013. This plan represents a commitment from the Commonwealth, State and Territory governments of Australia to work together to address the threat posed by increasingly sophisticated cybercrime. The Plan provides an overarching strategic framework to better align the efforts of domestic agencies responsible for combating different types of online crime. The Plan is available online here: www.ag.gov.au/CrimeAndCorruption/Cybercrime/Pages/default.aspx

While the Plan focuses on the actions that governments will take, it also acknowledges the key roles played by industry and individuals and the importance of forging strong partnerships to deal with cybercrime.

The Plan identifies six priority areas for action, shaped around the critical contributions governments can make in strengthening our national response to cybercrime—areas where we must focus our efforts for the short to medium term in building our response to cybercrime. These include:

- educating the community to protect themselves
- partnering with industry to tackle the shared problem of cybercrime
- fostering an intelligence-led approach and better information sharing
- improving the capacity and capability of our agencies to address cybercrime
- strengthening international engagement on cybercrime
- ensuring our criminal justice framework keeps pace with technological change.

A key initiative under the Plan is the development of a national online reporting facility for cybercrime, to be called the Australian Cybercrime Online Reporting Network (ACORN). The ACORN will make it easier for the public to report cybercrime, get the information they need to protect themselves and ensure agencies can respond more quickly. The ACORN will also give a clearer picture of the scope and nature of cybercrime affecting Australians and enable better operational and policy responses. It is expected that the ACORN will be operational in the second half of 2014

The Australian Government considers the Budapest Convention on Cybercrime the most appropriate basis for international cooperation on cybercrime. Australia became a Party to the Convention on 1 March 2013. Acceding to the Convention has helped to make our domestic laws more robust, while access to reciprocal arrangements with other Convention countries has enhanced cooperation on law enforcement investigations.

Dealing effectively with spam

Spam is a global problem that requires a global solution. Governments can play a key role in the effective regulation of spam and the Australian Government takes a multi-layered approach in this regard. There is also a very important role for the private sector to play in the provision of anti-spam tools for consumers and businesses.

To respond to the economic and social impacts created by the spam, Australia introduced the Spam Act in 2003 prohibiting the sending of unsolicited commercial electronic messages.
Australia's spam legislation was one of the first of its kind against spam in the world. It takes an 'opt-in' approach to commercial electronic messaging which requires recipient consent before commercial electronic messages can be sent. This method is consistent with Australian Privacy Principles and considered best practice - given the large volumes of unsolicited electronic messages consumers would otherwise be required to respond to in order to opt-out. This approach has similarly been taken in other countries, such as Japan, Canada and Taiwan.

In administering Australia's spam legislation, the ACMA's goal is to promote confidence in electronic messaging as a form of commercial communication. To do this the ACMA uses:

- Traditional compliance and enforcement strategies, together with
- International engagement and cooperation
- Industry and citizen education programs
- Partnerships with industry
- Market intelligence.

Cooperation with international agencies and regulators ranges from providing information and assistance on specific matters to an ongoing involvement with international anti-spam bodies such as the London Action Plan, which encourage cross-border collaborations between regulators, law enforcement and industry.

Issues pertaining to the use and misuse of the Internet

The Internet and cyberspace are not without rules. Australia considers that existing international law applies to the Internet and cyberspace. In relation to the use of the Internet by states, we note the June 2013 consensus report of the UN Group of Government Experts on developments in the field of information and telecommunications in the context of international security (UN General Assembly document A/68/98) which concluded that international law, and in particular the Charter of the United Nations, is applicable to the use of ICTs by states. We also note Human Rights Council Resolution 20/8 of 5 July 2012, adopted by consensus, which affirms that the same rights that people have offline must also be protected online, in particular freedom of expression.

As the Internet is integral to the conduct of economic transactions and social interactions, it has inevitably attracted criminal activity seeking to manipulate and take advantage of these communications. One pervasive criminal industry that has emerged in the past decade is that of cybercrime perpetrated through malicious software (or malware). While the Australian government is combating this crime through a number of approaches, it is also focusing on reducing the impact of this crime on Internet users through a voluntary government sponsored program - the Australian Internet Security Initiative (AISI). The AISI provides daily alerts to Australian Internet providers of malware infections on their networks, and expects these providers to use this information to identify and alert their customers that their computing device(s) is compromised. The Australian experience to date is that a collaborative approach between the Internet industry, government and consumers is the most effective mechanism to combat malware infections, as it enables flexible and rapid responses to these infections in a constantly changing threat environment.

Availability, affordability, reliability, and quality of service, especially in the developing world

Reliability and quality of service continue to be very important aspects of consumers' use of communications services. Quality of service (QoS) has historically focused on the technical attributes of end-to-end service provision – especially for voice services. However, consumers increasingly have an expectation of a broader 'quality of experience', which includes not only the technical quality of the service, but also minimum (and consistent) download speeds and access to 'value added' broadband applications and services.

There is currently a wide array of VoIP services currently on the market, and end-users can choose different VoIP services on the basis of price, technical quality and other functional aspects. There is ongoing work in the ITU-T to develop end-to-end technical performance requirements for VoIP and other services (including data services). It should be noted that the technical parameters for 'carrier grade' VoIP derive from the quality of service parameters for circuit-switched voice services developed originally by the ITU, and which are contained in ITU-T recommendations. There is also working being undertaken in other standards development organisations (SDOs), including the Internet Engineering Task Force (IETF) and the European Telecommunications Standards Institute (ETSI) on IP quality of service and associated technical activities.

To assist end-users in making informed purchasing decisions, Australia supports the development of objective technical criteria that can be used by suppliers of communications services to describe the technical capabilities (and limitations) of those service. To that end, Australia supports the continuation of the ITU-T's QoS technical studies for both voice and data services, working in close collaboration with other SDOs including IETF and ETSI. However, such technical studies should not

unnecessarily limit the scope for innovation in the market, especially in the development of communications products and services.

Australia has funded a range of projects in the Asia-Pacific region with the aim of improving availability, affordability, reliability and quality of service, including for example, an ICT infrastructure project in Solomon Islands, where in conjunction with the World Bank, Australia supported the establishment of a Telecommunications Commission and the issuing of a second mobile telecommunication license. This financial assistance resulted in an increase in mobile phone coverage, a reduction in mobile calls costs and an increase in the number of mobile phone subscribers in Solomon Islands.

Contributing to capacity building for Internet governance in developing countries

The way the internet is governed will be important in shaping future economic and social developments. However, for many developing countries participating in internet-related policy processes presents a significant challenge. The Australian Government is supportive of measures aimed at enabling the effective participation of developing countries in internet governance, such as ICANN's Fellowship Program and its ongoing development of regional engagement strategies. The Australian Government looks forward to working with ICANN and regional partners in the development of ICANN's Oceania engagement strategy during 2014.

Respect for privacy and the protection of personal information and data

Australia considers that the Internet and other digital communication technologies provide an unparalleled opportunity for exercise of the fundamental freedoms of expression, peaceful assembly and association. Technological developments have also fostered opportunities for enhanced communication and connectivity, as well as improved access to health and education services for isolated communities.

Australia acknowledges that with these benefits also comes the risk that digital technologies can be used to undermine the protection of human rights. Accordingly, it is essential that it is ensured that the same rights and freedoms people should enjoy in their everyday lives are protected and promoted in the online environment.

Australia considers that support for and implementation of the International Covenant on Civil and Political Rights (ICCPR) remains as relevant and vital today, in the digital age, as it ever was.

Within Australia, the *Privacy Act 1988* (the Privacy Act) is the principal piece of legislation that regulates the collection, use, storage and disclosure of personal information. The Privacy Act is technology neutral. From 12 March 2014, reforms to the Privacy Act will introduce the Australian Privacy Principles, which will apply to both government agencies and certain organisations. These Australian Privacy Principles will replace the existing Information Privacy Principles and National Privacy Principles and set out the obligations for the handling of personal information.

Australian law provides additional protections for the privacy of the content of communications and for non-content telecommunications data on the Australian telecommunications network. The privacy protections created by Australian law comply with international law, including Articles 17 and 19 of the International Covenant on Civil and Political Rights, Article 12 of the Universal Declaration of Human Rights and Article 15 of the Budapest Convention on Cybercrime. In particular, warrants and authorisations permitting Australia's law enforcement and national security agencies to access the content of communications and non-content telecommunications data, which include

consideration of proportionality, ensure that access to content and non-content data is not arbitrary or unlawful.

In May 2013, the Australian Parliamentary Joint Committee on Intelligence and Security (PJCIS) recommended that the laws protecting the privacy of Australian telecommunications and permitting lawful access by law enforcement and national security agencies be 'comprehensively revised' and that the revision be undertaken in consultation with privacy advocates and practitioners. In December 2013, the Australian Senate Legal and Constitutional Affairs References Committee (Senate Committee) agreed to a further inquiry into the comprehensive revision of these laws. The Senate Committee is due to report by 10 June 2014. The Australian Government is considering the recommendations of the PJCIS and will consider any further recommendations made by the Senate Committee.

Protecting children and young people from abuse and exploitation

Computers and the internet have created unprecedented opportunities for social, commercial, recreational, and political interaction. The internet facilitates trade, commerce and communication and is an essential part of the global infrastructure. As with all types of advancement however, the threat of exploitation of those advancements and the risks associated with those threats are ongoing and persistent. For instance, the internet and mobile technologies are being used to facilitate the sexual abuse and exploitation of children globally.

The Australian Government recognises online safety of children is an important area of responsibility, especially for parents and teachers, and has committed to a range of policies to help protect Australian children online. These include establishing a Children's e-Safety Commissioner to take a national leadership role in online safety for children; implementing a legislative based complaints system for the fast removal of material from large social media sites that is harmful or distressing to a child; investigating options for a simplified cyber-bullying offence; consulting with industry to improve safety options and software for smartphones, other devices and internet access services; establishing an advice platform with guidelines for parents about appropriateness of individual media items for children; providing funding to support Australian-based research and information campaigns on online safety; and improving support for schools through a stronger online safety component within the National Safe Schools Framework, establishing a voluntary process for the certification of online safety programs to be offered in schools, and funding for schools for the provision of online safety programs.

The Government has also established an Online Safety Consultative Working Group to bring together representatives from industry, government and non-government organisations with an interest in child welfare to provide expert advice to the Government and the Children's e-Safety Commissioner (once established) in developing online safety policies and programs. In addition to these initiatives, the Government provides a number of online safety resources to help protect children and young people online, such as a *Cybersafety Help Button* which provides fast and easy access to online safety information and assistance, and *the Easy Guide to Socialising Online*, which provides tips and online safety information for using different social networking sites, search engines and online games.

The Australian Federal Police (AFP) seeks to combat the threat of exploitation of children online in partnership with State, Territory and International law enforcement agencies, government and non-government organisations and industry. The AFP's Child Protection Operations teams monitor, investigate and target those associated with these offences and in conjunction with relevant agencies. The AFP through its Cyber Crime Prevention Team is instrumental in implementing cybercrime prevention strategies aimed at educating and raising awareness of online risks and

empowering all online users on how to protect themselves online. The ThinkUKnow Cyber Safety program is one such example. This is a successful partnership between law enforcement (AFP, and Northern Territory Police), and Industry (Microsoft, Datacom and ninemsn) in raising awareness amongst carers, parents and teachers on how they can keep their children safe online (see www.thinkuknow.org.au).

The Australian regulator, the ACMA, administers a co-regulatory scheme for dealing with prohibited online content under Schedules 5 and 7 of the Broadcasting Services Act 1992 (that is, the ACMA Hotline for reporting offensive and illegal online content). The scheme provides a range of citizen and consumer protections, including a power to take-down prohibited content hosted in Australia, referral to law enforcement of illegal content and, under industry codes of practice, the availability of optional end-user filters for use by Australian families.

Under the scheme, Australian residents may make complaints about online content they believe to be prohibited, including child sexual abuse material. Prohibited content is defined in relation to the National Classification Scheme (NCC) that applies to films and computer games. It includes Refused Classification (commonly referred to as 'banned') material, X18+, and certain R18+ and MA15+ content. Child sexual abuse material falls under the Refused Classification provisions as it contains 'offensive depictions of children' (as defined by the NCC). The majority of complaints to, and investigations by, the ACMA regarding online content relate to child sexual abuse material.

When prohibited content is found to be hosted in Australia, a take-down notice is issued after the content has been formally classified by the Classification Board. When prohibited content is found to be hosted overseas, it is notified to industry accredited filter providers (filters are available from industry at or below cost and are optional for end-users).

Additionally, all content that is potentially illegal is notified to law enforcement in Australia, with one exception: where child sexual abuse material is found to be hosted overseas in an International Association of Internet Hotlines (INHOPE) member country, the ACMA reports it through the INHOPE network for rapid law enforcement notification and take-down in the host country. (Nearly all child sexual abuse material investigated by the ACMA is hosted in INHOPE member countries.) The mechanism to enable the ACMA to notify child sexual abuse material to INHOPE, rather than law enforcement in Australia, is provided by a formal service-level agreement with the AFP. This Memorandum of Understanding enables and provides a legal mechanism for the ACMA to report highly illegal content to an overseas body.

The ACMA's role, in conjunction with the effective operation of the international system, effectively acts as a frontline response to online child abuse material by assisting to:

- prevent inadvertent access to highly offensive illegal content by Australian citizens
- ensure such material is rapidly brought to the attention of law enforcement agencies around the globe
- help stop continued re-victimisation of child abuse victims through the removal of the evidence of their abuse
- disrupt access to content by paedophiles and others involved in criminal activity who wish to access child sexual abuse material.