

NEW ZEALAND

CWG-Internet: Response to invitation for Member States to provide their input on actions that have been undertaken or to be undertaken by governments in relation to various international Internet-related public policy issues.

Recognizing the scope of work of ITU on international Internet-related public policy matters, represented by the list of topics in [Council 2009 Resolution 1305 Annex 1](#) which was established in accordance with decisions of ITU membership at the Plenipotentiary Conference, the Council Working Group on International Internet Related Public Policy invites Member States to provide their position on following question:

Q1. What actions have been undertaken or to be undertaken by governments in relations to each of the international Internet-related public policy issues identified in Annex 1 to Resolution 1305 (adopted by Council 2009 at the seventh Plenary Meeting)?" (Annex 1 issues listed in table on following page)

POLICY AND REGULATION: Multilingualization of the Internet, International Internet Connectivity, International public policy issues pertaining to the Internet and the management of Internet resources.

InternetNZ, the New Zealand Domain name registrar, has actively supported the introduction and implementation of Internationalised Domain Names through the International Corporation of Assigned Names and Numbers (ICANN). The .nz domain introduced the use of macrons in 2010 to allow for Maori language strings.

International Internet Connectivity in New Zealand is managed on a fully commercial basis between private providers. The New Zealand Government does not regulate international Internet Connections.

The New Zealand Government participates in the discussions on international management of Internet resources, including domain names and addresses through regular attendance at the International Corporation for Assigned Names and Numbers (ICANN) Governmental Advisory Committee meetings, and through discussions with the New Zealand Domain Name Registrar.

New Zealand also has an annual multistakeholder conference, Nethui, which brings together internet stakeholders across New Zealand to discuss internet public policy issues. This event is based on the format of multi-stakeholder collaboration successfully introduced by the global Internet Governance Forum (IGF)

We support continued discussions in international fora regarding the process towards enhanced cooperation on Internet governance. We encourage the ITU to support developing countries to build capability so they can effectively participate on an equal footing, in multistakeholder discussions regarding international public policy issues pertaining to the Internet, as detailed in PP. Resolution 102 (Rev. Guadalajara, 2010).

NEW ZEALAND

CRIME: Combating cybercrime, dealing with spam, issues pertaining to the use and misuse of the Internet and protecting children and young people from abuse and exploitation.

Cybercrime and child protection

New Zealand is working with international organisations such as Interpol and the Virtual Global Taskforce to ensure cooperation on child protection, spam, and other criminal matters, in support of existing international justice agreements. The New Zealand Government has also entered into a partnership with ECPAT New Zealand, part of a global organisation the purpose of which is the elimination of child prostitution and pornography and trafficking of children for sexual purposes.

In 2006 the New Zealand Government passed the Crimes (Intimate Covert Filming) Amendment Act 2006. This Act makes it an offence to film people in intimate situations without their knowledge or consent, protecting privacy and potential misuse of the images obtained. This Act is similar to legislation in other jurisdictions such as the United States and Britain.

The New Zealand Government supports the non-profit organisations that promotes confident, safe, and responsible use of online technologies in New Zealand.

In addition, the New Zealand Government is also exploring opportunities to support capacity-building activities in the Pacific relating to combating cybercrime.

The New Zealand Government recognises the gap between supply and demand for cyber security capacity building internationally. New Zealand has delivered a number of capacity building initiatives in the ASEAN region over the last four years. We are committed to continuing to support our regional partners to boost their cyber capacity.

Spam

In 2007, the New Zealand Government passed the Unsolicited Electronic Messages Act, which came into effect on 5 September 2007.

The Act prohibit unsolicited commercial electronic messages ('spam') with a New Zealand link (i.e. messages sent to, from or within New Zealand), or address-harvesting software being used to create address lists for sending unsolicited commercial electronic messages.

The Act is also intended to encourage good direct marketing practice by:

- Requiring electronic messages to contain a functioning unsubscribe facility
- Ensuring electronic messages are sent only to customers who have consented to receiving it
- Restricting the use of address-harvesting software.

The Electronic Messaging Compliance Unit was established in September 2007 to enforce the Unsolicited Electronic Messages Act 2007 by investigating complaints about spam. In the first four years of operation, the anti-spam enforcement unit has issued three statements of claim, 18 infringement notices and 218 formal warnings under the Act.

NEW ZEALAND

Harm minimisation

In 2009, the New Zealand Government introduced the Digital Child Exploitation Filtering System, a filtering system operated by the Department of Internal Affairs in partnership with Internet Service Providers which blocks websites that host child sexual abuse images. This system is available for Internet Service Providers on an opt-in basis.

The New Zealand Government is currently considering the Harmful Digital Communications Bill, which introduces a range of measures to address damaging online communications and ensure perpetrators are held to account for their actions. This Bill puts in place a range of measures to both reduce harm from threatening behaviour online. In particular, this Bill seeks to provide protection for young people, who are bullied more easily, instantly, and anonymously online, by providing a civil enforcement regime to resolve issues in the most effective way possible.

NETWORK STABILITY: The security, safety, continuity, sustainability, and robustness of the Internet

The New Zealand Government undertakes a number of activities to support the stability of its national ICT infrastructure. New Zealand's Cyber Security Strategy was launched in 2011, with three priorities:

1. Increasing Awareness and Online Security
2. Protecting Government Systems and Information
3. Incident Response and Planning

This strategy recognises that as the use of the internet in New Zealand increases, so too does our vulnerability to cyber threats.

New Zealand established its National Cyber Security Centre in 2011. The Centre is a key element of [New Zealand's Cyber Security Strategy](#) released in June 2011, providing enhanced services to government agencies and critical infrastructure providers to assist them to defend against cyber-borne threats.

In 2012 the National Cyber Policy Office was established in the Department of Prime Minister and Cabinet to lead and coordinate cyber security policy for New Zealand. The NCPO provides policy advice to the government on cyber security issues, works on engagement with the private sector and the community, and leads New Zealand's international cyber policy work.

In partnership with the .nz domain name registrar, we also actively participate in relevant multistakeholder organisations to support the stability of the Internet and the services that run over these networks.

We encourage the ITU to progress actions in support of PP. Resolution 120, particularly the actions that support the ITU to:

NEW ZEALAND

- take a significant role in existing international discussions and initiatives on the management of Internet domain names and other Internet resources within the mandate of ITU; and
- to play an active and constructive role in the process towards enhanced cooperation as expressed in § 71 of the Tunis Agenda.

Furthermore, the New Zealand Government also assesses the sustainability and robustness of the telecommunications infrastructure that facilities use of the Internet in New Zealand through its National Infrastructure Plan. The Plan is designed to reduce uncertainty for businesses by outlining the Government's intentions for infrastructure development over a 20-year timeframe. The Plan sets out a vision that, by 2030, New Zealand's infrastructure is resilient, co-ordinated and contributes to economic growth and increased quality of life. Inputs into this plan include an assessment of the current state of the infrastructure, scenario and trend analysis, national resilience assessments, and projections for future investment.

DEVELOPMENT: Availability, affordability, reliability, and quality of service; developmental aspects of the Internet, and contributing to capacity building for Internet governance in developing countries

Transport and Communications Infrastructure, specifically improving connections for the Pacific to modern communications services, has been identified as a sector priority for the New Zealand Aid Programme (NZ Aid). NZ Aid is working in conjunction with the World Bank and other partners to provide support for connecting the Pacific to modern communications.

Capacity building activities relating to cybercrime and network stability are addressed above.

PRIVACY: Respect for privacy and the protection of personal information and data

Privacy and the protection of personal data is legislated in New Zealand through the Privacy Act 1994. This Act demonstrates a flexible, modern approach to managing privacy in the face of ongoing technological developments. Privacy obligations and processes for handling personal information are detailed through twelve privacy principles. The privacy principles, covering collection of personal information, storage and security of personal information, requests for access to and correction of personal information, accuracy of personal information, retention of personal information, use and disclosure of personal information, and using unique identifiers. These principles reflect internationally accepted standards for good personal information handling.

The Officer of the Privacy Commissioner has responsibility for monitoring proposed legislation to see if it affects the privacy of individuals, and commenting on any privacy problems. It also provides education about privacy, monitors technological developments that can affect privacy, issues codes of practice, which modify the privacy principles and which apply to a particular industry or topic, and investigating complaints about interferences with privacy.

The Officer of the Privacy Commissioner is actively engaged in discussions regarding technology and privacy, and regularly engages with Internet stakeholders both on an ad-hoc basis, and through

NEW ZEALAND

participation at Nethui, the annual New Zealand multistakeholder conference on internet public policy issues.

Private industry in New Zealand has also led the introduction of the New Zealand Cloud Code, a voluntary code for cloud service providers which requires signatories to declare what they offer so customers can make an informed decision.

The Code requires providers to make clear exactly what security precautions and back-up systems they have in place, where data is stored and a range of other disclosures, so customers can make an informed decision about which cloud service to use.