

A Strategic Consideration of ICT Security and Confidence in New Zealand

Discussion Paper for Key Agencies/Organisations

Resources and Networks Branch

March 2006

ISBN 0-478-28470-5

Contents

INTRODUCTION.....	1
BACKGROUND	2
A STRATEGIC APPROACH.....	3
A Culture of Security and Safety.....	3
Principles.....	3
Roles of Various Participants in the ICT Sector.....	4
Roles of Government.....	4
Roles of Business and Industry Associations	5
Role of the General Public, Communities and User Groups	5
CURRENT ICT SAFETY AND SECURITY ISSUES	6
PRIORITY AREAS FOR FURTHER WORK.....	31
SCHEDULE 1 – RELEVANT LEGISLATION	33

Introduction

1. Information and communications technologies have become indispensable to modern society. Their continued development is revolutionising business, government, education, and communities generally through the benefits that they bring. Technological development and increased interconnectivity means, however, that information and communication systems and networks are now exposed to a growing number and a wider variety of threats and vulnerabilities. This raises new issues for security and suggests a need for greater awareness and the taking of new security measures by all participants in the information society.

2. This discussion paper seeks to apply a strategic framework and guiding principles to Information and Communications Technology (ICT) security and confidence in New Zealand, considers the respective roles of government, business and the general public, identifies current ICT safety and security issues and policies, and considers possible further actions for government. It follows on from the work of the Ministry of Economic Development on a Digital Strategy for New Zealand and the State Services Commission through various e-government projects.

3. The paper raises a number of questions on which feedback is sought from key agencies and groups to guide the development of government policy and the establishment of priorities for future action. It is proposed that following the receipt of submissions a number of key ICT security and confidence actions and projects will be identified and established with agreement on the lead agency and participating agencies.

4. Feedback by way of submissions should be provided by **13 April 2006** and can be provided in writing to:

Information Technology and Telecommunications Policy Group
Resources and Networks Branch
Ministry of Economic Development
PO Box 1473
WELLINGTON
or by email to ictsubmissions@med.govt.nz

Background

5. The Government released in 2005 its Digital Strategy in order to guide government action in helping to ensure that all New Zealanders are able to enjoy the benefits of ICT. In particular, the development and widespread use of ICT is considered to be a key factor in fostering economic growth.
6. One of the key enablers of the Digital Strategy is “confidence” as threats such as viruses, internet fraud and identity theft undermine the confidence of users and their willingness to use ICT. There are also threats to networks such as denial of service attacks. The Internet and telecommunications infrastructure are considered to be critical infrastructure for New Zealand.
7. In November 2004 the E-government Unit (now the ICT Branch) in the State Services Commission produced a report entitled *Trust and Security on the Internet* which assessed threats on the Internet as they relate to e-government. It provides a useful guide to many of the current threats arising from information and communication technologies.
8. In recent years the government has sought to make legislative changes which take account of changes in information and communications technology. Examples of this are the Electronic Transactions Act 2003 (clarifying the legal position around electronic commerce), amendments to the Crimes Act 1961 (changes to the definitions of “property” and “document”, provision for crimes involving computers, and extending the application of communication interception offences), proposed changes to the Copyright Act to address the implications of digital technologies, and the introduction of the Unsolicited Electronic Messages Bill to address the problem of spam.
9. Government agencies have also responded to the increased importance of information and communication technologies through the creation of specialist units to deal with technology-based policy and threats such as the Information Technology and Telecommunications Policy Group in the Ministry of Economic Development, the ICT Branch in the State Services Commission, the E-crime unit in the New Zealand Police and the Centre for Critical Infrastructure Protection.
10. Business has been active in the area of ICT security. New ICT security products and services have been developed, businesses have incorporated ICT security planning and processes into their operations and systems, and codes of practice have been developed in order to support good safety and security practices by the ICT industry in the provision of its services.
11. There has also been a growth in specialist ICT sector organisations such as the Internet Safety Group, InternetNZ, and the New Zealand Computer Society. These organisations are able to advise and coordinate on ICT security issues.
12. The general public has become more aware of ICT safety and security issues as a result of the widespread adoption of new ICT technologies and increased publicity on the threats to which users and infrastructure are now exposed.

A Strategic Approach

A Culture of Security and Safety

13. A strategic approach to ICT security and confidence issues is important to ensure that there is a clear overall vision to underpin and guide planning and to harmonise actions by government and other participants.

14. The Organisation for Economic Cooperation and Development (OECD) sets out a global vision for ICT of developing and promoting a culture of security amongst all participants, namely government, business, other organisations and individual users. This means that security is factored into the development of information and communication systems and networks and that the actions and behaviours of all participants in the ICT area take account of security issues.

15. This paper focuses on safety and security issues because threats to safe use of information and communications technologies undermine confidence in their use.

16. It is proposed that the development and promotion of a culture of security and safety amongst all participants be a key strategy for building and maintaining confidence in ICT in New Zealand consistent with the objectives of the Digital Strategy.

Principles

17. To support the development of a culture of security, the OECD established nine principles to guide the actions and behaviour of participants in the ICT sector. It is proposed that the principles to guide the actions and behaviours of participants in the ICT sector in New Zealand include the nine OECD principles (with some additions and modifications).

18. The following principles are proposed:

- **Currency** in that public policy and legislation impacting on ICT safety and security is up-to-date with current and emerging ICT technologies;
- **Awareness** by participants of the need for security of information and communication systems and networks and what they can do to enhance security;
- **Responsibility** being taken by all participants for the security of information and communication systems and networks;
- **Responsiveness** in that all participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents;
- **Ethics** in that participants should respect the legitimate interests of others;
- **Constitutionally and legally sound** in that the security of information and communication systems and networks should be compatible with New Zealand's constitutional and legal protections and freedoms;

- **Risk assessments** should be conducted by all participants and factored into risk and security management practices;
- **Security design and implementation** in that participants should incorporate security as an essential element of information and communication systems and networks;
- **Security management** in that participants should adopt a comprehensive approach to security management, including the adoption of security practices as part of the governance framework of organisations;
- **Reassessment** in that participants should regularly review and reassess the security of information and communication systems and networks, and make appropriate modifications to security policies, practices, measures and procedures;
- **Education and expertise** in that government and business should promote education of good ICT practices and ensure that there is sufficient technical and professional expertise in ICT security available to support the required actions;
- **Co-operation** in that the security of information and communication systems and networks should be supported by international co-operation and co-operation within government, between government and business, and between businesses and specialist ICT organisations.

Roles of Various Participants in the ICT Sector

Roles of Government

19. Government has the task of providing for the development of a culture of ICT security and safety. It can provide for this in each of its roles, including the development of public policy, the administration and enforcement of legislation, as owner and operator of systems and networks, as the provider of services, and as a user of such systems and networks.

20. The objective for government in developing public policy is the promotion of the security of information and communication systems and networks to engender confidence in their use and better ensure economic growth and overall security. In its public policy role government should respond to the need for a comprehensive policy and institutional infrastructure to ensure public safety, security and economic well-being in response to the threats and vulnerabilities associated with globally interconnected information and communication systems and networks. In addition government should assist with education and awareness-raising, the development of guidelines, and support and facilitate efforts by all participants to address ICT security and confidence issues.

21. As the administrator and enforcer of legislation it is important that government sufficiently resource and support these tasks to ensure good decision-making to support security and effective enforcement action against cyber-crime and ICT security threats generally. As owner and operator of information and communication systems and networks, government shares a role with businesses and other organisations and should lead by example by effectively applying the principles of risk assessment, security design and implementation, security management, and reassessment. As a user of information

and communication systems and networks government shares the responsibility with businesses, other organisations, and individuals for ensuring use of the system and network consistent with a culture of security and safety.

Roles of Business and Industry Associations

22. Most information and communications systems and networks are owned or operated by private sector businesses. In addition, businesses are users of these networks and systems.

23. In their role as owner and operator of information and communication systems and networks businesses have an important role in ensuring the security of ICT infrastructure through the adoption of best practices, the meeting of industry standards, and applying the principles of risk assessment, security design and implementation, security management and reassessment.

24. As a user of information and communication systems and networks, business has a responsibility to ensure that its use is consistent with security management principles and good security practice. Industry associations can often have a role in educating and encouraging their industries to adopt good practice.

Role of the General Public, Communities and User Groups

25. Individual and organisational users of information and communication systems and networks have a responsibility to ensure that their use is consistent with good safety and security practice. User groups such as InternetNZ and the Internet Safety Group have important roles in educating and promoting to users these good safety and security practices.

Questions for Discussion

1. What is the best strategy for promoting confidence in the use of ICT in New Zealand?
2. Are the proposed guiding principles right and, if not, what changes should be made?
3. Are the suggested roles of government, business, specialist ICT organisations, and the general public and communities right and, if not, what should they be?

Current ICT Safety and Security Issues

26. Security of information and communications infrastructure:

- a. *Issue:* The information and communications infrastructure comprises both fixed line and wireless networks that interlink to enable the transmission of information and communications between users (e.g. the Internet). Threats to the secure operation of this infrastructure include:
 - i. Cyber-attacks affecting the operation of ICT infrastructure (e.g. viruses/worms, denial of service attacks, hacking, deliberate sabotage);
 - ii. A lack of robustness or protection against ICT network faults or failures leading to network outages;
 - iii. Physical damage to key parts of the ICT infrastructure.
- b. *Policy:* The policy objective is to ensure that key ICT infrastructure continues to be operational and support ICT services through protection from security threats, sufficient network robustness and appropriate contingency planning. New Zealand made international commitments at the APEC Leaders meeting in Mexico in 2002 to:
 - i. Endeavour to enact a comprehensive set of laws relating to cyber security and cyber crime that are consistent with the provisions of international legal instruments;
 - ii. Identify national cyber crime units and international high-technology assistance points of contact and create such capabilities to the extent they do not already exist;
 - iii. Establish institutions that exchange threat and vulnerability assessment (such as Computer Emergency Response Teams).
- c. *Regulatory framework:*
 - i. The Crimes Act 1961 (ss 249 – 252) prohibits unauthorised access, damage and interference to computer systems and data held on computer systems.
 - ii. The Radiocommunications Act 1989 – prohibits the transmission of radio waves except in accordance with a licence or regulations made under the Act, requires licences issued under management rights to be certified as to non-interference before being registered and puts in place interference resolution mechanisms.
- d. *Institutional framework:*
 - i. New Zealand Police – enforces the Crimes Act provisions relating to e-crime;
 - ii. The Centre for Critical Infrastructure Protection (CCIP - part of the Government Communications Security Bureau) – CCIP provides advice and support to protect New Zealand's critical infrastructure from cyber threats – it has three main roles:

- Providing 24 hour/7 day “watch and warn” advice to owners of critical infrastructure;
 - Analysis and investigation of cyber attacks;
 - To work with critical infrastructure organisations and other sectors nationally and internationally to improve awareness and communications regarding information technology security;
- iii. The IT and Telecommunications Policy Group (part of the Ministry of Economic Development) – develops ICT policy for New Zealand with a particular emphasis on economic benefits;
- iv. The Radio Spectrum Management Group (part of the Ministry of Economic Development) – administers and enforces the Radiocommunications Act;
- v. The Government Inter-departmental Internet Security Working Group – this group has representatives from a number of government departments involved in Internet security issues – it considers and provides feedback on Internet security policy issues where they involve cross-departmental interests;
- vi. The State Services Commission (ICT Branch) – considers e-government issues and implements policies aimed at promoting effective and secure e-government practices;
- vii. The Telecommunications Carriers Forum – comprises a group of telecommunications carriers who consider telecommunications sector issues and develop policies and codes of practice to address these;
- viii. InternetNZ – engages in self-regulatory consensus-driven policy development relating to its operation of the .nz domain name space and other public policy advocacy and codes of conduct relating to protection of the Internet.
- e. *Comment:*
- i. From a legislative perspective New Zealand has responded to one of its commitments made at the 2002 APEC Leaders Meeting by enacting sections 249 – 252 of the Crimes Act regarding unauthorised access, damage to and interference with computer systems and data held on computer systems. There may be value, however, in reviewing New Zealand’s cyber security laws for the purpose of determining their consistency with international cyber security laws and whether further legislative measures may be required.
- ii. In New Zealand e-crime investigations are carried out by the appropriate Police District, with the forensic component conducted by a centralised forensic unit (the Electronic Crime Lab, which has three locations across the country). Electronic crime poses particular challenges because of its virtual and cross-border characteristics and its specialist nature. There may be merit, therefore, in considering whether the current Police structure and capability is sufficient to meet the growing challenges involved in e-crime investigations.

- iii. In other countries there have been established institutions that exchange threat and vulnerability assessment information. No computer emergency response team (CERT) or domestic computer security incident response team (CSIRT) has been set up for New Zealand but CCIP does carry out some of the functions of a CERT (it provides advisories in relation to cyber-threats). In addition some New Zealand organisations subscribe to the Australian Computer Emergency Response Team (AusCERT – an independent not-for-profit organisation based at the University of Queensland). There is a concern, however, that many computer security incidents in New Zealand are going unreported because of the lack of a single national contact point to address these as well as a mechanism for anonymous reporting. There is, therefore, a lack of effective communication with private sector organisations concerning threats, and prevention and mitigation measures.
- iv. There do not appear to be any requirements on business or ICT infrastructure providers to ensure that minimum security requirements are met in terms of network design and implementation or in terms of network robustness and security management practices.
- v. For business to put in place good ICT security measures there need to be sufficient incentives from a business and/or regulatory perspective. Care would need to be taken to minimise any unnecessary compliance costs. Facilities based competition can have an incentive effect to promote better security because it can provide a competitive advantage. In addition, the development of telecommunications infrastructure alternatives assists in mitigating against the effects of network outages.
- vi. There are security standards available to the private sector (ISO/IEC 17799:2000, ISO 27001:2005) which some businesses use as benchmarks for their security. These standards could be promoted to the private sector by government with a view to obtaining their wider use.
- vii. In the government sector there is the *Security in Government Sector (SIGS)* manual, which sets out the minimum standards of protective security that must be met by government departments and agencies, including standards relating to communications and systems security management. This is supplemented by NZSIT 400 which provides additional technical guidance.
- viii. There is a concern that there is a lack of expertise being developed in the area of ICT security and a lack of dedicated ICT security courses at our tertiary education institutions. There appears to be a need for the area of ICT skills development and training to be examined further to ensure future needs are catered for.
- ix. GCSB and CCIP appear to be the government agencies best placed to take the lead within government on the issue of ICT infrastructure security. In the business sector there is a need for a business-related group to take the lead in this area.

Questions for Discussion

4. What measures or actions should Government be taking to promote secure and resilient ICT infrastructure security within New Zealand, particularly within the private sector?
5. Is there value in reviewing New Zealand's cyber security laws for the purpose of determining their consistency with international cyber security laws and whether further legislative measures may be required? If so, who should lead this work, and what would be the priority issues?
6. Is there a need to review whether the current Police structure and capability is sufficient to meet the growing challenges involved in e-crime investigations?
7. Is there a need to prescribe minimum security standards for infrastructure operators?
8. Is there a need for changes in ICT education and skills development to be made to develop expertise in ICT security? Should ICT security be a mandated component of government funded ICT courses? Should there be an ICT security qualification or professional standard developed for New Zealand ICT security professionals?
9. What agencies or groups should be taking the lead on the issue of ICT infrastructure security and on the issue of the education of ICT infrastructure security?
10. What role or actions should ICT infrastructure operators and business be taking on this issue?

27. ICT network construction, repair and maintenance:

- a. *Issue:* In order to provide secure and modern information and communications infrastructure operators need to be able to construct, repair and maintain such infrastructure without undue impediment and need to incorporate security as an essential element in the design of such infrastructure. Issues arise where:
 - i. Security is not incorporated as an essential element in the design and construction of ICT infrastructure;
 - ii. There are difficulties or delays in getting the required landowner or council consents or where the terms and conditions attaching to consents are unreasonably restrictive;
 - iii. There is a lack of national standards or guidelines for councils to streamline consent processes;
 - iv. It is unclear whether the terms and conditions of a consent to construct and operate a power line allow that line to also be used for telecommunications purposes;
 - v. There is poor infrastructure redundancy (i.e. insufficient investment in upgrades, repairs and maintenance).

- b. *Policy:* The policy objective is to balance the need for ICT infrastructure development, repair and maintenance with the rights and interests of land owners as well as social and environmental considerations.
- c. *Regulatory framework:*
 - i. The Telecommunications Act 2001 (Part 4) provides for the declaration of network operators and for rights of access for the construction, repair and maintenance of lines and equipment for telecommunications purposes;
 - ii. The Electricity Act 1992 provides for the rights of access for the construction of electricity transmission infrastructure;
 - iii. The Resource Management Act 1991 requires that consents from local authorities be obtained for the use of land.
- d. *Institutional framework:*
 - i. The IT and Telecommunications Policy Group (part of the Ministry of Economic Development) takes the lead on telecommunications sector legislation and infrastructure issues;
 - ii. Ministry for the Environment – administers the Resource Management Act and is responsible for the development of national guidelines under that Act;
 - iii. Regional and territorial authorities – consider applications to use land and develop local planning guidelines;
 - iv. Telecommunications Carriers Forum – develops industry codes of practice for telecommunications carriers;
 - v. Utilities Advisory Group – comprises central and local government agencies and utility providers – discusses and coordinates actions on issues relating to the development and operation of utilities such as telecommunications, gas and electricity (particularly as they relate to roads).
- e. *Comment:*
 - i. Some stakeholders have expressed concerns that compliance costs and delays associated with obtaining the required consents for network construction are impeding the provision of modern and secure information and communication infrastructure. A review of and amendment to the Resource Management Act has sought to address these concerns by promoting nationally consistent standards and streamlined procedures. Work to develop national environmental standards for low impact telecommunications facilities is currently underway. This work is being led by the telecommunications industry, with MED and MfE taking an advisory and decision-making role.
 - ii. There are also concerns that the separation of legislative provisions addressing the rights to construct different types of networks (e.g. telecommunications and

electricity) does not easily allow for the application of new technologies to existing networks to enable a multiplicity of uses.

Questions for Discussion

11. What measures or actions should the Government be taking to ensure that the development of ICT infrastructure in New Zealand is able to take place without undue impediment and with security built into its design? What additional guidance on the development of ICT infrastructure can be provided?

12. Does the issue of the use of infrastructure for different purposes require any legislative action such as widening the land use and access rights of operators?

13. What role or actions should ICT infrastructure operators be taking to ensure security is an important consideration in the development of ICT infrastructure?

14. What roles or actions should ICT infrastructure operators and government be taking to ensure that national infrastructure is protected from failure?

28. Internet Governance:

a. *Issue:*

- i. Internet governance is both a national and an international concern. Nationally, management of the .nz domain name space is the responsibility of InternetNZ through the Office of the Domain Name Commissioner. Internationally Internet governance, including the Domain Name System (DNS), is the responsibility of ICANN, a non-profit body set up by the US Government to oversee the management of the core root services of the Internet. The DNS is the facility which converts website address names into addresses of actual machines. The DNS uses a database of names which is distributed across the world. It relies on "root servers" which are centrally operated, although they are geographically diverse and are duplicated in several locations.
- ii. IP addresses are also managed internationally by ICANN, and regionally in Asia Pacific by APNIC based in Australia. IP numbers are also a crucial aspect of DNS resolution, and aspects of national sovereignty are ignored in the existing model.
- iii. The issue from a New Zealand safety and security perspective is that decisions affecting the use of the Internet by government, business and the general public are taken by organisations (InternetNZ at a national level and APNIC at an Asia-Pacific regional level in relation to IP addresses) neither of which have any formal accountability to interested parties such as the government. Decisions affecting international aspects of security are taken by ICANN and the US Government.

b. *Policy:* The Government's policy objective for Internet governance is to represent the interests of New Zealand's stakeholders by participating in international discussions on decisions affecting the operation of the Internet.

c. *Institutional framework:*

- i. InternetNZ (a non-profit organisation fostering coordinated and cooperative development of the Internet in New Zealand – it also has the delegation from ICANN for the .nz Country Code Top Level Domain and operates the Office of the Domain Name Commissioner);
- ii. The IT and Telecommunications Policy Group (MED) takes the lead on IT policy issues;
- iii. State Services Commission (ICT Branch) – has an interest in Internet issues as they relate to e-government;
- iv. CCIP – has an interest in Internet issues as they relate to critical information infrastructure security;

d. *Comment:*

- i. At the international level recent discussions on proposals to revise the arrangements for Internet governance to promote a more inclusive approach for international stakeholders and greater accountability resulted in the status quo being maintained.
- ii. Internationally there has been a debate around issues such as the role that governments should play in the governance of the Internet, which is currently managed within the private sector. The New Zealand Government has contributed to these discussions through the World Summit on the Information Society and the Government Advisory Committee of ICANN. However, these issues are seen as being beyond the scope of this paper except and insofar as they affect the relationship between the Government and InternetNZ.
- iii. At the domestic level the operation of the Domain Name System for New Zealand appears to be proceeding relatively smoothly at present. In the past, however, there have been a small number of calls for greater Government involvement in Internet governance. At present the Government carries out a policy oversight role in relation to internet issues.
- iv. A recent phishing attack using a domain name registered in New Zealand and very similar to a New Zealand bank's website raised the issue around whether the Domain Name Commissioner (DNC) should carry out a check based on certain agreed criteria before registering a domain name for a website. The Fair Trading Act contains a general prohibition against misleading and deceptive conduct. This could include carrying on business under a name that is misleading or deceptive. However, the courts determine the question of whether a name is misleading or deceptive, and therefore the DNC does not vet names for this purpose. However, the Registrar of Companies which performs a similar function to the Domain Name Commissioner, is able to, under the Companies Act 1993, decline to reserve a name that:
 - Contravenes an enactment;

- Is identical or almost identical to another company name (the key words and/or the order in which they appear make that name virtually indistinguishable from another);
 - Is offensive.
- v. Registering of domain names using false information, while not permitted under the terms and conditions of the agreement between registrars and registrants who use their services, is not checked by the registrars. This is the same as with the registering of a company name – checking of registrant details are not undertaken nor are required by law.
- vi. Given the resources and time required to verify all applicant details and the likelihood of only a very small number of fraudulent applications, a check of the domain name against criteria similar to that used for company name registration may be much simpler and more effective.

Questions for Discussion

15. Should the government establish a more formal relationship with InternetNZ around the issue of the administration of the Domain Name System?

16. Should the Domain Name Commissioner be required to check applications for domain names against criteria similar to those applied to the registration of company names?

17. Should domain name registrars be required to verify applicants' details?

29. Protection of information assets and individual privacy:

a. *Issue:*

- i. The increasing capabilities and use of information systems and technologies to track, store and analyse personal information pose potential threats to people's individual privacy and confidence in using ICT. All governments and many organisations are engaged in the collection of detailed personal information on their citizens and customers. Information and privacy must therefore be protected from possible misuse and invasion while ensuring that information obtained for bona fide purposes, including providing for a safe and trusted internet, is permitted.
- ii. Issues relating to privacy and information security include:
- a. "Dataveillance" – tracking of information on individuals (e.g. via databases, spyware and cookies). This can sometimes occur as a result of users assenting to end-user licence agreements which give providers wide-ranging access to users' personal information.
 - b. Obtaining personal information, passwords and pin numbers through hacking or the use of software such as keystroke loggers on publicly used computers (e.g. obtaining internet banking passwords from internet café computers).

- c. Data matching, sharing and profiling -
 - This is a technology that assigns people to categories on the basis of personal information that has been collected, stored, processed and shared between organisations or different divisions of an organisation;
 - Sometimes referred to in privacy literature as "panoptic sorting", some uses of this technology could be considered unethical and discriminatory because, unlike a traditional investigation on an individual which is triggered by some evidence of wrongdoing or specific query, data matching and profiling is initiated because his or her category is of interest to the organisation;
 - To some extent this activity already exists in commercial organisations such as credit agencies, financial institutions and marketing companies;
 - To ensure that the privacy concerns surrounding this technology are considered and managed in government information matching programmes, the Privacy Act requires such programmes to go through an authorisation process.
 - d. Authentication - the e-Government strategy objective of delivering services and information via the Internet requires authentication of a person's identity. This plus the Government's demand for greater border security through passports with microchips and biometric information have increased people's concern that these may be the first steps towards a national identity card. The Government has addressed these concerns in the Cabinet-approved policy principles which any authentication system adopted within Government must follow.
 - e. Surveillance – tracking people's movements (e.g. via webcams, rfid, GPS computer chips in cellphones).
 - f. Identity theft and identity spoofing.
 - g. Covert filming and the taking of images of people in private situations.
- iii. Privacy and confidentiality can be protected through the following measures:
 - a. Security - the range of administrative, technical and physical mechanisms that aim to preserve privacy and confidentiality, by restricting information access to authorized "knowers" for authorized purposes, for example, passwords, encryption and authentication. Security is the responsibility of both the collector and owner of personal information.
 - b. Privacy enhancing technologies (PET) - those software programs or hardware devices that can help a user regain some of their privacy that has been lost on the Internet (e.g. programs that allow users to manage the cookies that web sites place on their hard drives, applications that

provide the ability to surf on the Internet anonymously so that advertisers cannot track a user's shopping habits).

- c. Data protection - the range of legal, regulatory and institutional mechanisms that guide collection, use and disclosure of information (e.g. the Privacy Act).
- b. *Policy*: The policy objective is to achieve the right balance between protection of information assets, private property and individual privacy and competing values such as freedom of information and expression, preventing and punishing crime, and the efficient operation of business and government.
- c. *Regulatory framework*:
 - i. The Privacy Act 1993 and its related codes (e.g. Health Information Privacy Code) provide rules and guidelines to:
 - a. Ensure that individuals have a right to control information about themselves, and to prevent its use without their consent for purposes unrelated to those for which it was collected.
 - b. Set out the Privacy Commissioner's central requirement to seek balance and have regard to the human rights and social interests that compete with privacy, desirability of free flow of information and the right of government and business to achieve their objectives in an efficient manner.
 - c. Establish a regime to permit data matches between government agencies after Parliamentary scrutiny and with monitoring and reporting back to Parliament, for example, requiring government agencies to identify those circumstances where information matching is most clearly justified, that the benefits outweigh the costs and data matching is undertaken in such a way that minimises the effect on privacy through careful data management.
 - ii. The New Zealand Bill of Rights Act 1990 protects against unreasonable search or seizure. It could be argued that data matching or profiling would violate this right because the technique of matching unrelated databases is designed as a general search. The search is not based on any pre-existing evidence to direct suspicion of wrongdoing to any particular person.
 - iii. Specific legislation, for example, the Land Transport Management Act 2003 includes a clause to prohibit a toll operator from using personal information for purposes other than the collection and enforcement of tolls.
 - iv. If passed, the Crimes (Intimate Covert Filming) Amendment Bill will assist in addressing some of the covert filming concerns. The Bill forbids the making, possession, publication, importation, exportation and sale of an intimate visual recording (IVR). An IVR is defined as the making of a surreptitious visual record of another person without that person's knowledge or consent and in circumstances that the person would reasonably expect to be private.

- v. The Privacy Commissioner encourages government agencies and other organisations proposing to introduce new laws, policy or technology to undertake a Privacy Impact Assessment. A PIA is an assessment of actual or potential effects that the activity or proposal may have on individual privacy and the ways in which any adverse effects may be mitigated.
 - vi. Industry codes of practice, for example, *Code of Practice for Direct Marketing, Electronic Product Code (EPC) / Radio Frequency Identification (RFID) in Retail Consumer Code of Practice*.
- d. *Institutional framework:*
- i. The Ministry of Justice (Public Law Group) - responsible for privacy law policy and the New Zealand Bill of Rights Act;
 - ii. The Office of the Privacy Commissioner – responsible for the operation of the Privacy Act;
 - iii. The IT and Telecommunications Policy Group (MED) – responsible for IT policy and its relationship to privacy issues;
 - iv. State Services Commission (ICT Branch) – responsible for e-government issues and their relationship to privacy;
 - v. New Zealand Police – responsible for the investigation and enforcement of criminal offences;
 - vi. Industry associations (e.g. Direct Marketing Association, New Zealand Bankers' Association);
 - vii. The Internet Safety Group (an independent non-profit organisation which is focused on providing cybersafety education for all New Zealanders), InternetNZ, and other user groups.
- e. *Comment:*
- i. New Zealand is generally thought to have one of the most comprehensive national privacy law outside Europe. Some New Zealand industry associations have also been proactive with regard to privacy concerns and have instigated self-regulation. However, there are other industries or services where more work is being done or could be done in the area of security and confidentiality, for example, codes of practice for internet banking and internet cafes.
 - ii. Advances in, and the decreasing cost of, tracking and monitoring technologies are raising increasing concerns about surveillance and misuse of the data/images collected and whether current policies and legislation are adequate to deal with the potential ethical issues which extend beyond privacy to ones of dignity.

Questions for Discussion

18. Are current measures and legislation adequate to minimise the threats to information security and individual privacy that have emerged through developments in information and communications technologies (e.g. spyware)? If not, what action should the government take?

19. Is enough being done in educating organisations, especially SMEs, as to their responsibilities regarding protection of information and privacy?

20. Is enough being done in educating the public as to their rights?

21. Is protection of information assets and privacy being sufficiently considered by those developing these technologies and applications? If not, what actions can be taken?

22. Is there a need for regulatory or self-regulatory measures to be introduced to address privacy concerns over passwords and pin numbers used for internet banking?

30. Abuse of information and communications technology services by users:

a. *Issue:* Abuse of ICT services can take many forms but they all contribute to an undermining of public confidence in the use of such services. Forms of abuse include:

- i. Abuse of email and other ICT messaging services by the sending of spam, "phishing" messages, messages promoting Internet-based scams and frauds generally, bullying or harassment by way of emails or text messaging, the sending of illegal or age restricted images by way of email or texting;
- ii. Abuse of internet and phone chatroom services by sexual predators and others with dishonest or malicious motives;
- iii. Abuse of ICT services by the transmission of objectionable material such as child sexual abuse images;
- iv. Abuse of Internet services by the posting of defamatory, offensive or objectionable material;
- v. Abuse of Internet search engine services by the creators of websites hosting "adult" or obscene material using "acceptable" but misleading website subject information in order to appear on a website search result list for such information;
- vi. The publication or distribution of images obtained covertly and in breach of privacy rights;
- vii. Illegally accessing other peoples bank accounts to commit fraud by the unauthorised transfer of funds;

b. *Policy:* The policy objective around the use of ICT services is to adopt a multi-tiered strategy aimed at minimising abuse and promoting a high degree of public confidence in the use of such services.

c. *Regulatory framework:*

- i. The government has taken and is taking a number of steps to address the abuse of ICT services including:
 - the passing of the Crimes Amendment Act 2005 to address the problem of sexual predators involved in the sexual grooming of children using the Internet;
 - the introduction of the Unsolicited Electronic Messages Bill to address spam;
 - the introduction of the Crimes (Intimate Covert Filming) Amendment Bill;
 - the support of ICT safety initiatives undertaken by the Internet Safety Group;
 - the application of the Crimes Act and the Fair Trading Act by the Police and Commerce Commission to Internet-based scams and frauds; and
 - the policing of objectionable and restricted material by the Department of Internal Affairs under the Films, Videos and Publications Classification Act 1993.
- ii. The government is also encouraging the development of industry codes of practice to address areas such as chatrooms and spam (the Telecommunications Carriers Forum and InternetNZ have been involved in this).

d. *Institutional framework:*

- i. The IT and Telecommunications Policy Group (MED) – responsible for IT and telecommunications policy, including the regulation of services;
- ii. The Ministry of Justice (Crime Prevention and Criminal Justice Group) – responsible for criminal justice and censorship policy;
- iii. The Ministry of Consumer Affairs – responsible for consumer policy issues;
- iv. Department of Internal Affairs (Censorship and Compliance Group) – responsible for the enforcement of New Zealand's censorship laws;
- v. New Zealand Police responsible for the investigation and prosecution of criminal offences;
- vi. The GCSB (as the national INFOSEC authority) and CCIP – monitoring the cyber-threat environment;
- vii. Commerce Commission – responsible for the enforcement of the Fair Trading Act and, if required, telecommunications industry codes;

- viii. Ministry of Education – responsible for safe practices within schools;
 - ix. The Internet Safety Group – promotes the safe use of ICT services and good user practice;
 - x. The Telecommunications Carriers Forum (TCF) and InternetNZ which are both involved in the development of codes of practice to address the abuse of ICT services;
- e. *Comment:*
- i. The enactment of the Unsolicited Electronic Messages Bill supported by anti-spam codes of practice developed by the TCF and InternetNZ for service providers and enforcement by the Department of Internal Affairs will assist in mitigating the growth of spam.
 - ii. The Crimes (Intimate Covert Filming) Amendment Bill has been considered by Select Committee and, if passed, will help address concerns over intimate covert filming.
 - iii. The TCF has developed a draft code of practice for mobile service providers to address mobile content issues, including the abuse of chatroom services.
 - iv. Investigating and enforcing laws around ICT-based scams and frauds and threats to child safety requires specialist expertise and resources and needs to be supported by a legal system that has trained and knowledgeable lawyers and judges. Concerns have been raised that there is currently a lack of sufficient specialist expertise and resources within or available to the New Zealand Police and a lack of sufficient lawyers and judges trained in this area.
 - v. The resourcing of both public education campaigns and government agencies involved in enforcement is an issue that will need to be closely monitored and adequately addressed. The Ministry of Consumer Affairs is seeking to promote a fraud awareness campaign around the concept of Fraud Awareness Month (an international campaign coordinated by ICPEN) but for such campaigns to be effective they require sufficient resourcing.
 - vi. The Internet Safety Group has a valuable role to play in public education and awareness of the abuse of ICT services but also requires adequate resourcing for this task (government departments and agencies such as the Ministry of Education, State Services Commission, CCIP and the New Zealand Police currently contribute funding to support its work along with private sector sponsors). Its website provides information on a wide range of Internet safety issues.
 - vii. Businesses also have a valuable role to play in promoting ICT safety and good practice through staff education and training.

Questions for Discussion

23. What additional actions or measures should government be taking to address the abuse of ICT services and what are the areas of highest priority?

24. What additional actions or measures should the ICT industry be taking to address the abuse of ICT services and what are the areas of highest priority?

25. Is there a need for additional programs to develop more expertise and knowledge in the investigation and enforcement of ICT-based scams and frauds?

26. How can the education and awareness-raising of users on how they can best protect themselves against the abuse of ICT services be most effectively achieved? Should businesses be taking a more active role in educating and training their staff?

27. How should the specialist requirements of investigating and addressing ICT safety and security issues be best met by the Police, and do judges and lawyers require additional training in the area of cyber-crime?

31. Security of computers and computer systems against misuse:

- a. *Issue:* Computers and computer systems can be compromised by viruses/worms and Trojans which enable computers to be commandeered for noxious purposes such as sending spam or for denial of service attacks. In order to mitigate against this threat there needs to be education of users, installation of appropriate defences, and effective ISP management and law enforcement.
- b. *Policy:* The policy objective is to ensure that there is effective prevention and detection of, and redress against, abuse of computers and computer systems which undermine the effectiveness of and confidence in the use of information and communication technologies.
- c. *Regulatory framework:* As noted above, the Crimes Act 1961 (ss 249 – 252) prohibits unauthorised access, damage and interference to computer systems and data held on computer systems.
- d. *Institutional framework:*
 - i. The New Zealand Police – responsible for the investigation and prosecution of criminal offences;
 - ii. The GCSB as the National INFOSEC Authority;
 - iii. The CCIP – monitors and provides warnings of cyber attacks;
 - iv. The State Service Commission (ICT Branch) – advises on Internet security in relation to e-government;
 - v. The IT and Telecommunications Policy Group (MED) – responsible for IT policy and promoting confidence in the use of information and communication technologies;

- vi. The Ministry of Justice – has policy responsibility for criminal policy, including e-crime policy;
 - vii. The Internet Safety Group – promotes the safe use of computers and communications technology;
- e. *Comment:*
- i. Experience has shown that with the increased uptake of broadband, computers are more vulnerable to misuse in that they are always “connected” and can be targeted for use as part of a “zombie” network for the purposes of spamming or carrying out a denial of service attack. This means that it is important for users to put in place effective security measures on their computers such as firewalls and anti-virus software.
 - ii. The Internet Safety Group provides valuable information in this area and other organisations such as the CCIP, software suppliers, computer security companies, major ISPs and the online auction company Trademe, also promote the security of computers and computer systems.
 - iii. In Australia the Australian Communications and Media Authority is proposing to launch an Internet Security Initiative (ISI). The aim of the ISI is to reduce spam by remotely and automatically scanning computers for compromise or vulnerability and to pass this information onto ISPs so that they can take action (which could include quarantining or disconnection if the problem is serious) and to encourage the public to secure their own machines. A similar initiative could be undertaken in New Zealand once the anti-spam legislation has been enacted.
 - iv. Despite attempts at user education, it would appear much of the public is unaware of ICT security issues or lack sufficient incentive to put in place preventative measures. One measure that could assist in promoting ICT security is to require that all new devices sold must meet minimum security standards.

Questions for Discussion

28. What additional measures or actions should government be taking to address the security of computers and computer systems against misuse and what are the areas of highest priority? Should New Zealand adopt a similar initiative to the Internet Security Initiative taken by Australia?

29. What additional measures should equipment, software and network suppliers be taking to address the security of computers and computer systems against misuse?

30. What compliance measures are required?

32. Security of and access to communications between users:

a. *Issues:*

- i. Communications between users in the form of emails, text messages and voice communications can be intercepted or accessed by persons without authorisation if proper security measures are not in place.
 - ii. Electronic communications, as well as providing many benefits, also serve as a means to aid criminal activity. For this reason, access by law enforcement authorities to records of electronic communications can be an important element in conducting a criminal investigation.
 - iii. Unlike many other countries, New Zealand does not require telecommunications service providers and Internet Service Providers to retain certain levels of information that may be relevant to law enforcement agencies. Increasingly, however, there appears to be a reluctance on the part of the service providers to retain this information voluntarily, and therefore there may be a need to consider the imposition of data retention obligations or the development of a code of practice to address this issue.
- b. *Policy:* The policy objective is to ensure that effective privacy and security measures for electronic communications are implemented and balanced against the interests of law enforcement agencies in carrying out criminal investigations.
- c. *Regulatory framework:*
- i. The Crimes Act 1961 (ss 216A – 216F) prohibits the use of interception devices to intercept private communications and the disclosure of information obtained from such interception (subject to exceptions for law enforcement and maintenance of service purposes).
 - ii. The Radiocommunications Act (s 133A) prohibits the disclosure of the contents of a radiocommunication received by a person knowing that it was not intended for that person (subject to exceptions for law enforcement purposes).
 - iii. The Telecommunications (Interception Capability) Act 2004 (s 7) requires network operators to ensure public telecommunications networks and telecommunications services are interception capable (this is for the purpose of enabling law enforcement and security agencies to continue to carry out interception activities notwithstanding developments in technology).
 - iv. The State Services Commission ICT Branch has developed a Secure Electronic Environment project for government which includes the implementation of the “Secure Electronic Environment Mail” or “SEEMail”. SEEMail is used by many government agencies as a means for the secure exchange of email and attachments using the Internet. This is likely to be replaced by the Government Shared Network, currently in development by the SSC ICT Branch. SSC is also working on the implementation of a shared workspace initiative.
- d. *Institutional framework:*
- i. New Zealand Police – responsible for carrying out criminal investigations involving the use of interception warrants and enforcing the Crimes Act;

- ii. Ministry of Justice – responsible for criminal justice policy and the interception capability legislation;
 - iii. Radio Spectrum Management Group (MED) – responsible for enforcing the Radiocommunications Act;
 - iv. The IT and Telecommunications Policy Group (MED) – responsible for IT and telecommunications policy;
 - v. State Services Commission (ICT Branch) – responsible for the security of government communications;
- e. *Comment:*
- i. Technology providers have developed solutions to address the issue of the security of communications between users through technologies such as encryption and authentication.
 - ii. The imposition of data collection and retention obligations on service providers for law enforcement purposes has occurred in countries such as Australia and those in the European Union. These obligations are likely to involve the imposition of significant compliance costs and therefore the mechanism for and extent of such obligations needs to be carefully considered.

Questions for Discussion

31. Is the matter of the security of communications between users an issue that requires additional government action or is technology able to provide the solutions in this area?

32. Is there a need to consider the imposition of data collection and retention obligations for law enforcement purposes on service providers?

33. Security of and confidence in transactions entered into using information and communications technologies:

- a. *Issues:*
- i. Research studies have identified the following major impediments to the broader use of the Internet for commercial activities:
 - ii. Transactions are not always secure and not always conducted by authenticated parties (security). Surveys have concluded that theft is the major deterrent to shopping online and identity theft is recognised as the world's most menacing and fastest growing means to perpetuate fraud;
 - iii. Personal details are not always kept private, stored safely, and used as agreed (privacy). Users have a desire to avoid unsolicited advertising and other intrusions into their personal privacy;
 - iv. Levels of service are not always as specified or up to an acceptable standard (this may include non-delivery of items purchased) and there may be no easy

access to effective systems for complaint handling and redress, especially where the business is overseas (service); and

- v. There is an apparent lack of a "value proposition", as perceived by customers, to warrant taking the risks.
 - vi. An issue has arisen concerning the application of existing product safety requirements to online publishers, such as Trademe, who promote and facilitate product dealings between other parties. The issue is whether the online publisher should have responsibility for ensuring compliance with the product safety requirements applying to goods sold by parties using their sites.
 - vii. The ability to take legal redress against another party to a transaction when things go wrong is also an issue. This is particularly the case in cross-border transactions, such as transactions over the Internet with someone from another country, and for Internet transactions generally where the personal details of the other party may not be known.
 - viii. In the case of transactions between parties connected through online sites, such as Trademe, the organisation operating the site may have the required personal information to enable an application to the Disputes Tribunal or court to be filed, but requests for such information can give rise to privacy concerns, particularly where it may be difficult to ascertain whether the "proposed court action" is the genuine reason for the request (the divulging of personal information where court proceedings are reasonably in contemplation is allowed by the Privacy Act).
 - ix. The sharing and storing of information or data by ICT service providers assists in the process of investigating cyber-crime. Accordingly it is arguable that ICT service providers should be required to store, and provide law enforcement agencies with access to, certain levels of information.
- b. *Policy:* To ensure that consumers trust in the security, privacy and service fulfilment of e-commerce.
- c. *Regulatory framework:*
- i. Crimes Act 1961 (provisions re fraud and theft);
 - ii. Electronic Transactions Act 2002 (clarifies the legal validity of transactions entered into by electronic means);
 - iii. Fair Trading Act (re misleading or deceptive conduct in trade and product safety);
 - iv. Privacy Act 1993 (provides rules relating to the collation, holding and disclosure of personal information);
 - v. The OECD *Cross-Border Fraud Guidelines* and the OECD *Guidelines for Consumer Protection in the Context of Electronic Commerce* (implemented in

New Zealand through the *Model Code for Consumer Protection in Electronic Commerce*).

d. *Institutional framework:*

- i. New Zealand Police – investigation and prosecution of criminal offences;
- ii. IT and Telecommunications Policy Group (MED) – IT policy and the promotion of e-commerce;
- iii. State Services Commission (ICT Branch);
- iv. Office of the Privacy Commissioner – provides a complaint mechanism and dispute resolution process for privacy issues;
- v. Ministry of Justice – criminal justice and privacy policy and dispute resolution;
- vi. Ministry of Consumer Affairs – consumer protection policy;
- vii. Commerce Commission – enforcement of the Fair Trading Act;
- viii. Businesses that rely on ICT to facilitate or enter into commercial arrangements (e.g. Online traders and retailers, banks);

e. *Comment:*

- i. The risks associated with e-commerce or online transactions can be significantly mitigated by parties adopting sensible business practices and by vendor businesses adopting sound security management practices around the commercial information of its customers.
- ii. Some industries have developed codes of practice setting out principles to address the major concerns of e-commerce (e.g. the Code of Practice for Direct Marketing in New Zealand and the draft internet banking code of practice). The Electronic Marketing Standards Authority, with support from the Ministry of Consumer Affairs, has also developed the Trustmark accreditation. Businesses trading goods or services on the Internet can gain this accreditation by meeting specific good practice requirements.
- iii. The Ministry of Consumer Affairs has been working on the issue of taking legal redress against another party to a cross-border transaction when things go wrong. This work has focused on the OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders, and membership of the International Consumer Protection Enforcement Network (ICPEN).
- iv. There has been a proposal that where legal proceedings are contemplated following an online transaction and the parties do not know each other but a third party that connected them does, that the claimant file the application and the Disputes Tribunal obtain the personal information from the third party. The purpose of this is to address privacy concerns. The Ministry of Justice is

concerned that such a proposal compromises the independence of the Tribunal or Court. It suggests that the claimant could, at the time of requesting the information from the third party, provide some sort of evidence to support the genuine nature of the claimant's request, such as a "verified" copy of an application to the Tribunal with the personal details of the respondent "to be completed".

- v. Consumer and business education and the provision of security management tools promote the security of online transactions. In particular, the education of consumers/users on the requirements for secure online transactions mitigates against the occurrences of online frauds and scams.

Questions for Discussion

33. Should the codes of practice go further and specify minimum standards in some areas, for example, a minimum level of security, security system or authentication?

34. Should there be a code of practice for all e-commerce activities?

35. How should court and dispute resolution processes take account of the different nature of e-commerce compared to ordinary commercial dealings and the privacy concerns around the disclosure of personal information?

36. Should there be a review of the responsibilities of online publishers for compliance issues involved in the sale of products facilitated by their sites, such as product safety?

37. Should the collection and storing of IP data by ISPs to assist in the prevention and detection of e-crime or fraud be required?

34. Security of intellectual property rights:

- a. *Issue:* The development of digital technologies has had major implications for the protection and management of intellectual property rights, especially copyright associated with written works, images, and audio and visual recordings. Digital rights management technologies have been developed as a way of protecting intellectual property rights but there has been controversy about the limitations these can place on the rights of consumers/users of copyright protected works.
- b. *Policy:* The policy objective is to ensure that intellectual property laws provide the necessary incentives for the development and creation of new works and inventions, including works and inventions created using information and communication technologies, while taking account of public interest considerations relating to dissemination, use and access.
- c. *Legislation:*
 - i. Copyright Act 1994 (governs the scope of protection of original works) – a Copyright Amendment Bill to address the implications of digital technologies as they relate to copyright has been developed by the Ministry of Economic Development and is ready for introduction;

- ii. Patents Act 1953 (provides for the protection of inventions by registration as a patent) – there have been issues around the registration of patents for commonly used e-commerce processes and whether these patents are justified on the basis of novelty or not. A review of the Patents Act has led to a proposed amendment Bill to tighten the patent examination process by ensuring patents are justified and not overly broad. There is also a proposal to make the process for challenging a patent easier;
- d. *Institutional framework:*
- i. Intellectual Property Policy Group (MED) – intellectual property law policy;
 - ii. IT and Telecommunications Policy Group (MED) – IT policy issues;
 - iii. State Services Commission (ICT Branch) – management of government information;
- e. *Comment:*
- i. The issues arising from the development of new technologies as they relate to New Zealand’s intellectual property legislation are largely being addressed through the proposed Copyright Amendment Bill and a review of the Patents Act;
 - ii. There are practical application issues arising from the development of Digital Rights Management technologies, particularly to prevent the unauthorised copying of works developed using software that incorporates DRM. There are concerns in particular around the ability of the person originating the work being able to retain control over the work. DRM also has the potential to lock up works and prevent the exercise of permitted acts. The State Services Commission is currently considering issues relating to DRM as they apply to government documents and government held information;
 - iii. The infringement of intellectual property rights is an ongoing issue and new technologies provide greater scope for infringements. These technologies also offer new business models and ways to lock up works. Education of users on intellectual property issues assists in mitigating against infringement of rights. The MED Intellectual Property Policy Group and Intellectual Property Office of New Zealand will undertake various education and awareness raising projects in 2006.
 - iv. Recently there was an incident involving the use by Sony of “rootkit” technology in its DRM software with the consequent creation of a security risk for users.

Questions for Discussion

38. What measures, if any, should government implement to address the issues arising from Digital Rights management technologies?

39. What intellectual property issues should be addressed in future education and awareness-raising campaigns?

35. Safety of content:

a. *Issues:*

- i. With the development of the Internet in particular there is now a much greater ease of accessibility to images and information which is generally considered to be indecent, offensive or harmful. Some of these images or information is “objectionable” while others are considered to be “adult” content that should have restricted availability.
- ii. With the convergence of technologies for broadcasting and telecommunications there is likely to be a greater use by broadcasters of different telecommunications-related platforms, such as the Internet, for the distribution of its material. The issue is whether the broadcasting standards regime should apply to this material.

b. *Policy:* The policy objective is to develop a regulatory and institutional framework that supports protection from exposure to “harmful” and “offensive” content balanced against the interests of freedom of expression.

c. *Regulatory Framework:*

- i. Films, Videos and Publications Classification Act 1993 (indecent and objectionable material);
- ii. Broadcasting Act 1989 (broadcasting standards and content);
- iii. Crimes Act 1961;
- iv. Advertising Standards Authority Code of Practice (advertising standards and content);

d. *Institutional framework:*

- i. Department of Internal Affairs (Censorship and Compliance Group) – enforces New Zealand’s censorship legislation;
- ii. The CCIP;
- iii. Ministry of Justice - has policy responsibility for censorship and the Crimes Act;
- iv. Ministry for Culture and Heritage – responsible for broadcasting standards and content;
- v. Ministry of Education – responsible for the safety of content in schools;
- vi. New Zealand Police – responsible for enforcement of the Crimes Act;
- vii. New Zealand Customs - responsible for the legality of material that comes into New Zealand;

- viii. IT and Telecommunications Policy Group (MED) – responsible for content issues from an ICT policy perspective;
- ix. Internet Safety Group – provides information on how users can protect themselves and their children from “harmful” content;
- x. Telecommunications Carriers Forum and InternetNZ – develop industry codes of practice to promote good industry practice around the provision of content services;
- xi. InternetNZ.

e. *Comment:*

- i. The Internet is a largely uncensored place which means that indecent, offensive and adult content is easily accessible. For children in particular this represents a risk. For this reason user education and the development of safety tools are considered to be important in mitigating the risks of exposure to harmful material.
- ii. The New Zealand Police, Customs and Department of Internal Affairs work together to help ensure a coordinated approach to enforcing New Zealand’s laws relating to the safety of content. A coordinated approach assists in promoting effective enforcement action.
- iii. The Ministry for Culture and Heritage is likely to be considering the question of what the role of the Broadcasting Standards Authority, as a complaints body, should be in relation to broadcasting-like material appearing on different platforms.
- iv. There is a concern that age verification procedures for restricted material or activities, such as online gaming, is not sufficiently robust and should be improved.
- v. Some countries, such as Australia, place legal obligations on ISPs to remove offensive content hosted by them unless they have signed up to and complied with an approved code of practice. While InternetNZ is developing a draft code of practice for ISPs the issue of content safety is largely unaddressed.
- vi. The recent consideration and enactment of the Films, Videos and Publications Classification Amendment Act 2005 prompted consideration of the issue of what obligations ISPs should be subject to in relation to the hosting of “objectionable” material. It was determined that ISPs should not be liable for distribution offences without the requisite mental elements. It was considered that ISPs could not reasonably monitor all the electronic material on the Internet because of the volume and changing nature of material subscribers can access, limitations placed by privacy legislation, and the unreliability of automated filters. Sections 122 and 122A of the Films, Videos and Publications Classification Act set out the legal position concerning the distribution of publications, including electronic publications via the Internet.

- vii. In the area of mobile content, the Telecommunications Carriers Forum has developed a code of practice to promote the responsible provision of mobile content.
- viii. The development of the Internet and satellite television has resulted in an explosion in cross-border advertising. The Advertising Standards Authority will adjudicate on a complaint made by a New Zealand consumer in relation to advertising originating in another country. In other words, it adopts the country of reception principle, but takes account of a number of factors such as the primary audience for the advertising. In dealing with the issue of cross-border advertising there is a huge reliance on international liaison and cooperation between the regimes in different countries. This international element means that there are a number of issues to be worked through between various countries such as which codes of practice apply (for further discussion see the article on this subject on the Advertising Standards Authority website [www.asa.co.nz]).

Questions for Discussion

- 40. Should ISPs be subject to legal obligations regarding the hosting of offensive or indecent content or should they be encouraged to sign up to a voluntary code of practice?
- 41. Should age verification procedures for restricted material or activities be made more robust?

Priority Areas for Further Work

36. The outline and discussion of the above issues concerning ICT security and confidence is for the purpose of promoting feedback and discussion on the priority areas for further work for government in terms of both government-led actions and the actions of business and users which can be supported by government. In some areas work is already being undertaken to address the implications of new technologies from a security and confidence perspective but in other areas there are clear gaps that need to be addressed. There is also a need for agreement on which agencies should have primary responsibility for new issues and which agencies have an interest.

37. One of the concerns that arises from an analysis of ICT security and confidence issues is that while there is informal liaison and cooperation between various agencies there is a lack of formal coordination and strategic oversight of the work of the many different government and non-government agencies that are involved in this area. Accordingly one issue that may need examining is whether or not there is a need for a dedicated group which carries out this function.

38. Areas for further work would appear to include the following:

- Reviewing the need for the establishment of a national computer emergency response team (CERT) and a mechanism for anonymous reporting of security incidents;
- Reviewing the consistency of New Zealand's cyber-security laws with international laws;
- The development and application of security standards for ICT infrastructure;
- The promotion of ICT network and systems security within businesses, including educating staff on good workplace practices;
- Professional and technical education requirements to support ICT security and safety;
- The review of InternetNZ policies concerning the registration of domain names and whether there is a need for it and the Government to establish a more formal relationship regarding Internet management issues;
- A review of threats to information security and individual privacy from developments in information and communications technologies, including consideration of the issues of spyware, identity theft and internet banking security;
- The promotion of ICT safety/security awareness;
- The establishment of a specialist unit or units in the police to investigate cyber-crime and safety issues arising from information and communication technologies;
- Consideration of data retention obligations on telecommunications and Internet service providers to assist criminal investigations;

- Consideration of the need for minimum security requirements to apply to ICT devices;
- The education and support of police, judges and lawyers on the methods and consequences of cyber-crime and abuse of ICT services;
- The development of an initiative aimed at scanning computers for compromise and vulnerability and seeking the assistance of ISPs in taking action to address this;
- The review of court and dispute resolution processes to take account of the different nature of e-commerce compared to ordinary commercial dealings;
- The review of the responsibilities of online publishers for compliance issues involved in the sale of products facilitated by their sites, such as product safety;
- Reviewing what legal obligations regarding content safety should apply to Internet service providers and other providers of digital content services.

Questions for Discussion

42. Does the above list correctly identify the work areas for ICT security and confidence and, if not, what should they be?

43. Which work areas are the most important?

44. Which agency should have the lead responsibility for these work areas and which agencies have an interest?

Schedule 1 – Relevant Legislation

- The Telecommunications Act 2001 (administered by the Ministry of Economic Development) regulates the terms and conditions of access to designated services (e.g. interconnection with Telecom's fixed PSTN), the provision of telecommunications service obligations, and issues relating to network construction, connection, maintenance and use.
- The Radiocommunications Act 1989 (administered by the Ministry of Economic Development) provides for the management of the radio spectrum, including the creation and allocation of rights to manage and use radio frequencies.
- The Telecommunications (Interception Capability) Act 2004 (administered by the Ministry of Justice) requires telecommunications networks to have interception capability.
- The Broadcasting Act 1989 (administered by the Ministry for Culture and Heritage) provides for the maintenance of programming standards in broadcasting in New Zealand, establishes the Broadcasting Standards Authority and the Broadcasting Commission, and enables political parties to broadcast election programmes for parliamentary elections free of charge.
- The Films, Videos and Publications Classification Act 1993 (administered by the Ministry of Justice) regulates the provision of offensive and indecent material.
- The Crimes Act 1961 (administered by the Ministry of Justice and enforced by the Police).
- The Privacy Act 1993 (administered by the Ministry of Justice with complaints dealt with by the Office of the Privacy Commissioner).
- The Electronic Transactions Act 2002 (administered by the Ministry of Economic Development).
- The Fair Trading Act (administered by the Ministry of Consumer Affairs and enforced by the Commerce Commission).
- The Copyright Act 1994 and the Patents Act 1953 (administered by the Ministry of Economic Development).