CYBERLIBERTIES IN THE WAKE OF A NATIONAL SECURITY "PUSH"

Background Briefing Paper prepared by Oz NetLaw: internet law practice of the Communications Law Centre on behalf of the Baker & McKenzie Cyberspace Law and Policy Centre

Contents

PART 1

Terrorism and National Security - Australian Legislation and Policy

Two factors have been the driving force behind a number of recent Acts and Bills before Parliament:

- the events of September 11; and
- the increased flow of asylum seekers to Australian shores epitomised by the Tampa crisis.

These measures address popular concerns of border protection, terrorist threats and national security. This symposium is concerned with the effects of the new legislation on the internet and other communications media. However, to place this legislation in context, the background paper will set out a summary of some of the recent legislation that has been introduced into Parliament with respect to these issues. The new legislation can be broadly grouped into 3 types, with some overlap between issues:

- border protection;
- intelligence and enforcement powers; and
- anti-terrorism.

The most important pieces of recent legislation that the Government has introduced to address these issues is set out below, accompanied by some of the policy considerations which the legislation raises. Other Australian legislation that relates to terrorism is set out at Appendix A.

A number of overseas jurisdictions have also responded legislatively to the events of September 11 and the threat of increased terrorist activity. For purposes of comparison, we have summarised and annexed some of the legislation introduced in the United Kingdom (**Appendix B**), the United States of America (**Appendix C**), and Canada (**Appendix D**) as well as a Proposal of the European Union (**Appendix E**).

Border Protection Legislation

(a) **Migration Amendment (Excision from Migration Zone) Act 2001 (Cth)**

This Act excises certain Australian territories (such as Christmas Island and the Cocos (Keeling) Islands) for the purposes of limiting the ability of offshore entry persons to make valid visa applications.

(b) **Migration Amendment (Excision from Migration Zone) (Consequential Provisions) Act 2001 (Cth)**

This Act empowers members of the Australian Defence Forces to detain certain persons in excised offshore places.

(c) **Migration Legislation Amendment Act 2001 (No. 5) (Cth)**

This Act amends the Migration Act 1958 in order to authorise an airline operator, shipping operator, travel agent or proscribed organisation to disclose information about any matter relating to travel by persons to or from a migration zone to an officer, even if the information is personal information as defined in the Privacy Act, for the purposes of facilitating the administration and enforcement of the Migration Act or Regulations.

(d) **Migration Legislation Amendment Bill 2002 (Cth)**

This Act makes changes to clarify the status of non-citizen children born in Australia. It also authorises the taking of security for compliance with conditions to be imposed on a visa yet to be granted. Further, it amends the law relating to special purpose and bridging visas.

(e) **Migration Legislation Amendment (Procedural Fairness) Bill 2002 (Cth)**

This Bill provides that the codes of procedure in the Migration Amendment Bill are an exhaustive statement of the natural justice hearing rule.

(f) **Migration Legislation Amendment (Transitional Movement) Bill (Cth)**

This Bill creates a new category of "transitory person." A "transitory person" is an offshore entry person taken to another country, but not assessed to be a refugee. A transitory person can be brought to Australia if he/she needs medical attention, and for some other reasons, but cannot make a visa application while in Australia.

Some Policy Considerations

Privacy Issues

11 Privacy Principles at section 14 of the *Privacy Act 1988* (Cth) regulate personal information collected, held and used by Commonwealth government agencies.

The new legislative scheme regulating the private sector is based on 10 National Privacy Principles (NPPs) which dictate how private organisations should handle personal information. An interference with privacy will occur if the relevant act or practice breaches an approved privacy code that binds the organisation or an NPP, if no privacy code applies.

Privacy of individuals is also protected in other ways. The *Telecommunications Act 1997* (Cth) prohibits carriers and carriage service providers from disclosing or using any information or document which relates to the affairs or personal particulars of another person. This prohibition is subject to a number of exceptions, mainly relating to law enforcement. The *Telecommunications (Interception) Act 1979* (Cth) provide protections against interception of communications passing over a telecommunications system without the knowledge of the person making the communication. Again, this prohibition is subject to a number of exceptions relating to law enforcement.

These protections extend to the external territories of Australia, such as Christmas Island and the Cocos (Keeling) Islands. However, the excision of these territories in the legislation amending the Migration Act casts doubt over the extent of protection offered. Of the amendments above, only the *Migration Legislation Amendment Act (No 5) 2001* makes specific reference to the *Privacy Act*. The amendment authorises disclosure of personal information so that there is no breach of the NPPs or the *Privacy Act*.

Civil Liberties Issues

The NSW Council for Civil Liberties made a submission to the Legal and Constitutional Legislation Committee on the *Migration Legislation Amendment (Procedural Fairness) Bill 2002* (**"Procedural Fairness Amendment"**) and the Migration Legislation Amendment Bill (No 1) 2002.

In relation to the Procedural Fairness Amendment, the NSW Council for Civil Liberties submitted that the "codes of procedure" specified in the Migration Act specified a substantially lesser standard of fairness than the common law principles of natural justice. Specifically, the "codes of procedure" provide that the decision maker is not required to invited submissions on a matter regarded as potentially adverse to an applicant's case. This is contrary to the common law requirement of natural justice, which requires an applicant to have an opportunity to answer such matters. The Council submitted that the Bill would "perpetuate an undesirable standard of public administration and protect it from legitimate scrutiny and criticism."

In relation to the *Migration Legislation Amendment Bill (No 1)*, the Council submitted that no justification was provided for the blanket abrogation of natural justice principles for individuals holding "special purpose visas". The Council submitted that as a matter of principle executive decisions should not be made without allowing the person affected an opportunity to answer adverse material, and that in any case a decision maker could satisfy the requirements of natural justice in the case of a person who is unable to be contacted by having made reasonable efforts to contact the person.

Intelligence and Enforcement Powers

(a) ***Measures to Combat Serious and Organised Crime Act 2001 (Cth)***

This Act amends the Crime Act 1914 so that law enforcement officers and authorised persons are exempt from criminal and civil liability for offences committed in the process of an operation for the purposes of obtaining evidence that may lead to the prosecution of a person for a serious offence (eg theft, drugs, fraud, sex offences and threats to national security punishable by imprisonment for 3 years or more).

Certain controls apply, including that a law enforcement office can only gain immunity for liability for committing an offence pursuant to an operation which has been authorised by a certificate issued by an authorised office of

the Australian Federal Police and National Crime Authority ("authorised controlled operation").

Officers authorised under Part IAC of the Crimes Act to acquire evidence or, or use, an assumed identity, are also immune from civil or criminal liability for offences which may be committed in the course of the authorised activities. Offences have also been created to deter the improper disclosure and use of assumed identities.

(b) ***Intelligence Services Act 2001 (Cth)***

The Act defines the functions and services of ASIS (Australian Secret Intelligence Service) and DSD (Defence Signals Directorate). Under the Act, the functions of ASIS include:

- to obtain intelligence about capabilities, intentions and activities or people or organisations outside Australia;
- to communicate intelligence;
- to conduct counter-intelligence activities;
- to liaise with intelligence services of other countries; and
- other activities as the Minister directs.

The functions of DSD include:

- to obtain intelligence about capabilities, activities or intentions of people or organisations outside Australia in the form of electromagnetic, electric, magnetic or acoustic energy;
- to communicate intelligence;
- to provide material advice and assistance to Commonwealth and State authorities on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means;
- communications technologies and cryptography.

Certain controls apply in respect of intelligence activities. These include an extensive Ministerial authorisation regime associated with the proper conduct of the agencies' functions

The Act also provides limited immunities from civil and criminal proceedings in respect of unintended consequences of Australian legislation. Immunities do not extend beyond those necessary to enable agencies to carry out their functions, and do not permit any act in relation to things which need to be authorised by a warrant under the Australian Security Intelligence Organisation Act, the Interception Act of the Telecommunications Act. There is also a statutory obligation on agencies to respect rights to privacy. The Minister is required to make written rules to ensure activities are carried

out with due regard to those rights and the Attorney- General must be consulted.

(c) ***Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Bill 2002 (Cth) ("ASIO Amendment Bill")***

This Bill is currently before Parliament. It gives ASIO the ability to seek warrants to question people in relation to terrorist offence and then detail them for up to 48 hours following questioning. This period of detention can then be extended for an indefinite period. A person can also be required to provide information and records and ASIO can remove and retain records and things relating to a terrorist offence under the Bill.

A "prescribed authority" can issue a warrant, but only after the Attorney-General has consented and if he/she is satisfied that there are reasonable grounds for believing that issuing the warrant will substantially assist in the collection of intelligence that is important in relation to a terrorism offence and that relying on other methods would be ineffective. The prescribed authority must also be satisfied that there are reasonable grounds for believing that the warrant will substantially assist the collection of intelligence that is important in relation to a terrorist offence. If the warrant does not state who the person detained may contact, the person may not contact anyone while in detention, apart from the Inspector-General of Intelligence and Security or the Ombudsman. There are other safeguards on the power, including that the prescribed authority must be present during questioning.

Some Policy Considerations

Privacy Issues

All three pieces of legislation impact upon the privacy-related protections in the *Privacy Act* and the *Telecommunications Act*.

The immunities from civil and criminal liability granted to officers of the agencies for breaches committed in the course of authorised activities provide a significant escape from privacy obligations in the course of investigations. Although the *Intelligence Services Act* 2001 provides that immunities from criminal and civil liability granted to officers of the agencies are not intended to permit any act in relation to premises, persons, computers, things or telecommunications services in Australia that would otherwise only be authorised under warrant or in accordance with section 283 of the *Telecommunications Act*, it is unclear what this means and the extent to which it limits the activities of the agencies.

The ASIO Amendment Bill raises significant privacy concerns with its additional powers to ASIO officers, especially the power to strip search detained persons and the power to remove and retain things and records.

Civil Liberties Issues

The extension of powers of law enforcement agencies, combined with their immunity from civil and criminal liability for acts/offences committed in the course of authorised activities create concerns for civil libertarians. The power given under the ASIO Amendment Bill to detain persons suspected of terrorist activities for unlimited time periods, without the ability to contact even a lawyer, represents a dramatic shift in attitudes towards civil liberties. Michael Rozenes, the former Commonwealth Director of Public Prosecutions, is quoted in the Sydney Morning Herald (May 1 2002) as stating: "Such is this a novel proposition that you can take a person [when] he or she is not the subject of charge or suspicion, have their liberty removed from them, put them into indefinite custody and not have them have the ability of being advised by lawyers of whether they should speak or not speak. There ought to be judicial supervision of the process which we do not have, there ought to be legal advice available to the detainee which we do not have, and there ought to be a privilege against self-incrimination."

National Security and Anti-Terrorism

The first piece of legislation to be brought before Parliament in response to the events of 11 September 2001 was the Criminal Code Amendment (Anti-Hoax and other Measures) Bill. This Act is not yet in force. The second piece of legislation was the Criminal Code Amendment (Espionage and Related Offences) Bill 2002. That Bill has not yet been passed. The next 5 Bills were introduced as a package of anti-terrorist bills. These Bills are:

- Security Legislation Amendment (Terrorism) Bill 2002 [No.2]
- Suppression of Financing of Terrorism Bill 2002
- Criminal Code Amendment (Suppression of Terrorist Bombings) Bill 2002
- Border Security Legislation Amendment Bill 2002
- Telecommunications Interception Legislation Amendment Bill 2002.

All 7 of these Bills are dealt with below.

(a) ***Criminal Code Amendment (Ant-Hoax and other Measures) Act 2002 (Cth)***

This Act makes it an offence to case an article to be carried by postal service with the intention of introducing the false belief that the article is harmful or that an explosive device has been left in any place. It also makes it an offence to use the post to make a threat to kill, cause serious harm, menace, harass or cause offence. The Act also increases the penalties for the misuse of postal and other services.

(b) ***Criminal Code Amendment (Espionage and Related Offences) Bill 2002 (Cth)***

The main effect of the Bill is to establish new offences dealing with the protection of national security and defence. The Bill makes it an offence to communicate information concerning national security or defence if the likely result is that the information is disclosed to another country or foreign

organisation. The Bill also covers the communication of information concerning another country that is either held or controlled by the Australian government.

The Bill refers to conduct that may prejudice Australia's *security* and defence rather than *safety* and defence therefore including a range of material or information not included in current legislation.

The range of activities that may constitute espionage has been expanded and the maximum penalties for a person convicted of espionage is increased from 7 years to 25 years imprisonment.

"Information" is defined to mean "information of any kind, whether true or false and whether in a material form or not and includes an opinion and a report of a conversation.

Some Policy Considerations

The definition of "information" provided in the Bill has been criticised by many organisations as being extremely wide. The New South Wales Council for Civil Liberties submission on the Bill observed that it no longer limits acts of espionage to classified information but extends it to a wider variety of government held or controlled information. The Council argues that the proposed legislation could thus be used against activists or whistle blowers.
The Council notes that the change in terms to "*security* and defence" from "*safety* and defence" means that the operations and methods of intelligence and security agencies are caught by the Bill and that disclosure of illegal activities engaged in by these kinds of organisations may constitute "espionage" within the meaning of the Bill. The Council cites the possibility that a human rights organisation could be charged and convicted of an offence for publicising security operations of repressive regimes in other countries. The Council recommends a tighter definition of information and the introduction of a "public interest defence" for the actions of whistle blowers.

Interesting arguments were advanced at the time of the 2001 Bill. These included:
Limits on public discussion
John Fairfax Holdings Limited, and its publications also wrote to the Attorney General making the following points:
Sections 82.3 and 82.4(3) are overly broad. They make no distinction between national security information and information that has nothing whatever to do with national security. Fairfax argues that the Bill would have the effect of preventing public discussion by including official information, not just that related to national security. The Bill hampers public discussion by criminalising receipt – that is today legal – of information about the workings of Government.
The Bill (Section 82(3)) treats any unauthorised disclosure of information by public servants as if

it involved a leak of official secrets. Under existing law, a recipient, such as a journalist, could only be prosecuted where an official secret is involved, and they had knowledge of that fact. The Bill also removes the need for the Commonwealth to prove that a recipient either knew, or had reasonable grounds to believe, its release involved a breach of the official secrets provision of the Crimes Act, Section 97(6). There is no need to prove intent; mere possession of official information will be enough. Therefore, if it is a crime to disclose any information, or to receive any information, the Bill, by limiting the coverage of the workings of government, directly hampers or prevents public discussion of the issues of the day – and therefore goes to the heart of the operation of a free press in a democracy.

Impinges on Lange principle of implied freedom of communications

Fairfax believes that the Bill as presently drafted, unlawfully impinges upon the implied freedom of communication concerning government and political matters enshrined in the Australian Constitution and recognised by the High Court in *Lange v ABC*. Fairfax argues that an important safeguard in previous legislation, one where there was an onus on the Crown to prove beyond reasonable doubt that the recipient of an official secret was either aware that the information had that status or aware of information which would reasonably lead to that conclusion, has been removed. The Bill imposes an offence of strict liability, lack of knowledge is no defence to a prosecution of the recipient under the new, generic, Section 82(3).

(c) ***Security Legislation Amendment (Terrorism) Bill [No 2] (Cth)***

This Bill creates two new offences: "treason" and "terrorist act." The offence of treason includes such matters as causing the death of the Sovereign, levying war against the Commonwealth, assisting an enemy at war with the Commonwealth, assisting a country or organisation engaged in armed hostilities against the Australian Defence Force or forming an intention to do any of the above and manifesting that intention by an overt act.

A terrorist act is an action done or threat made with the intention of advancing a political, religious or ideological cause and does not include lawful advocacy, protest or dissent. A terrorist act must also fall within certain categories including serious harm to a person or serious damage to property.

The Bill also contemplates cyber-terrorism, as another specific requirement for a terrorist act is if it "seriously interferes with, seriously disrupts or destroys, an electronic system including, but not limited to:
(i) an information system; or
(ii) a telecommunications system;...

The Bill creates further offences for a person who possesses a thing connected with preparation for a terrorist act, or who collects or makes a document

connected with a terrorist act. These offences are absolute liability offences and the penalty is life imprisonment.

Under the Bill, the Attorney-General may proscribe an organisation if the Attorney-General. It is an offence:

- to direct the activities of a proscribed organisation;
- directly or indirectly to receive funds from or give funds to a proscribed organisation;
- to be a member of a proscribed organisation;
- to provide training for or train with a proscribed organisation; or
- to assist a proscribed organisation.

Some Policy Considerations

Civil Liberties

Liberty Victoria, in its submission to the Senate Committee, submitted that the definition of terrorism is too broad, vague and unwieldy. Liberty Victoria pointed out that the terms "terrorist" and "terrorism" are not value-neutral, and are in fact now inextricably linked with people from Arabic or Middle Eastern backgrounds and people of the Muslim faith. The Federal Government's linking of terrorists and refugees during the election has left the term with heavy undertones of racial and religious stereotypes. Liberty Victoria expressed concern that despite the fact that "lawful advocacy, protest or dissent or industrial action" are not included in the definition, the imprecise nature of the definition combined with political and ideological positions that change with the government of the day, political activity such as public demonstrations or unplanned industrial activity may be caught within the provisions.

Privacy

The Federal Privacy Commissioner, in his submission to the Senate Committee, expressed concern over the definition of terrorism, noting that it may encompass a wide range of offences. If the definition of terrorism include offences that might otherwise be regarded as minor, then it is possible that the privacy rights of individuals will be unduly infringed during an investigation.

Constitutional Issues

Professor George Williams, Director of the Gilbert and Tobin Centre of Public Law wrote a letter to the Senate Legal and Constitutional Legislation Committee on 3 April 2002 examining the constitutional aspects of the proposed bill. Professor Williams submits that there are serious questions over whether the defence, external affairs and nationhood powers could support the Terrorism Bill in a time of relative peace. Certain provisions in the Terrorism Bill may exceed what the High Court would consider to be appropriate and adapted, and the Terrorism Bill has the capacity to burden freedom of political communication.

A number of submissions to the Senate Committee pointed out the similarity between this Bill and the *Communist Party Dissolution Act*. Professor Williams submits that the Bill may not suffer from the same constitutional defect as the *Communist Part Dissolution Act* as review of a

decision may be sufficient available. However, the Bill may still be invalid because the limited scope of review means that the law fails to pass the more general proportionality test. Professor Williams expresses concern over the similarity of the 2 pieces of legislation in the broad powers they purport to give to the executive to ban an organisation.

Professor Williams also points out a number of public policy issues, such as absence of fairness in the proscription regime and the lack of meaningful review mechanisms. The central concern is with the nature and breadth of the Attorney-General's proscription power. Professor Williams states: "If such a power is to exist it should only be exercisable by a more fair and open process, and should be limited to organizations that are actively involved in carrying out or supporting terrorist acts."

(d) ***Suppression of Financing of Terrorism Bill 2002 (Cth)***

This Bill creates an offence directed at those who provide or collect funds used to facilitate or engage in a terrorism act. The Bill requires cash dealers to report suspect transactions and enable the Director of Australian Transaction Reports, the AFP (Australian Federal Police) and the Director-General of Security to report information to foreign intelligence and law enforcement agencies. The Bill also introduces higher penalties for providing/dealing assets of persons engaged in terrorism activities.

Some Policy Considerations

Privacy

The Federal Privacy Commissioner, in his submission to the Senate Committee, submitted that the concept of "reasonable grounds" as cited in this Bill, has the potential to be interpreted broadly. In the future, this broad interpretation could lead agencies and organisations to disclose personal information that was never intended to be disclosed this way. The Commissioner submits it would be preferable that the legislation make explicit the exact sorts of personal information that may be disclosed and under what circumstances this can be done. In the case of disclosing personal information overseas, the Commissioner recommends that the legislation should provide for agencies to ensure that foreign governments and their law enforcement agencies are bound by equivalent standards for handling personal information as would be the case in Australia.

(e) ***Criminal Code Amendment (Suppression of Terrorism Bombings) Bill 2002 (Cth)***

This Bill seeks to amend the Criminal Code by creating offences relating to terrorist activities using explosive or lethal devices. Under the Bill a person commits an offence if:

(a) the person intentionally delivers, places, discharges or detonates a device; and

(b) the device is an explosive or other lethal device and the person is reckless as to that fact; and

(c) the device is delivered, placed, discharge, or detonated, to, in, into or against:

(i) a place of public use; or

(ii) a government facility; or

(iii) a public transportation system; or

(iv) an infrastructure facility; and

(d) the person intends to cause death or serious harm.

A person also commits offence if the person does (a) to (c) above and the person intends to cause extensive destruction to the place, facility or system and the person is reckless as to whether that intended destruction results or is likely to result in major economic loss.

Some Policy Considerations

Inconsistency with head legislation

This Bill was introduced to give effect to the International Convention for Terrorist Bombings. Proposed sections 72.3(1) and (2) create offences that require intention to be proven and strict liability applies to paragraphs 1(c) and 2(c). This is the opposite situation under the head Bill, which does not require intention for a terrorist offence to be proven. This inconsistency between 2 bills in the same package, designed to deal with the same problem is of considerable concern. Philip Boulton, convenor of Criminal Defence Lawyers NSW, pointed out during his submission to the Senate Committee's public forum on 1 May 2002, that it appears that this Bill provides a more satisfactory model, from a civil liberties point of view, for dealing with terrorist bombings than the head Bill.

(f) ***Border Security Legislation Amendment Bill 2002 (Cth)***

This Bill introduces a number of measures which increase the power of Customs and Customs officials. The Bill requires an employer of a "restricted area employee" or an issuer of a security identification card to a person to provide to an authorised officer the "required identity, information", being the name, address, date and place of birth of that person, as well as any other information set out in the regulations.

The Bill also requires an operator of a ship or aircraft to report to Customs on the passengers and crew who will be on board the ship or aircraft when it

arrives at the port or airport. A Note to the section states that this must be complied with even if the information is personal information as defined in the Privacy Act. Customs must then pass this information on to the Department of Immigration and Multicultural and Indigenous Affairs. For certain kinds of aircraft or ship (which will be specified in the regulations) the operator must also make a report to the Department. An operator of an international passenger airline must also allow authorised officers to have access to the operator's passenger information. A Note to the section states that this obligation must be complied with even if the information is personal information as defined in the Privacy Act.

The Bill also seeks to increase the powers of Customs and Customs officials in several ways, including allowing Customs officers to patrol airports, increasing the restricted areas and allowing officers to remove people from those areas.

Privacy

The Federal Privacy Commissioner, in his submission to the Senate Committee, submitted that it is necessary to consider whether this Bill is appropriate to the social context in which it will function, both in the present and in the future. Various provisions in the Bill seek to make lawful acts and practices that might otherwise be inconsistent with the provisions of the Privacy Act. Accordingly, future review of the legislation would be imperative. The Commissioner also expresses concern at the lack of an obligation on the employer or agency to inform an individual that their personal information is being collected an disclosed. The Commissioner notes a number of provisions in the Bill that include loosely defined terms, unilateral decision-making powers and elements of subjectivity which are difficult to reconcile with the principles of accountability and transparency. The Commissioner also points out that there is significant potential for agencies to act beyond the policy intent of the provisions, and that there are unlikely to be many complaints associated with the handling of personal information under the proposed legislation, given the largely covert nature of its operation. As a result, the Office of the Privacy Commissioner will carry clear obligations in ensuring the transparent and accountable discharge of the powers, which raises problems at a time when the Office is already diverting resources to meet the workload resulting from the Private Sector Amendments to the Privacy Act.

(g) ***Telecommunications Interception Legislation Amendment Bill 2002 (Cth)***

This Bill seeks to clarify the operation of the Telecommunications (Interception) Act in relation to telecommunications services involving a delay between transmission and access by the recipient ie email, voicemail and short messaging services (SMS).

The amendments deem a delayed access message which has become a "stored communication" to be no longer "passing over a telecommunications

system" and therefore, not able to be accessed pursuant to a warrant under the Interception Act. Access to stored communications would have to be authorised under warrants issued under a Commonwealth, State or Territory Crimes Act or Criminal Code.

"Stored communication" is defined to mean a communication that:
(a) has been submitted using a delayed access message service; and
(b) is stored on equipment; and
(c) can be accessed using that equipment, or that equipment in combination with other equipment, but without using a line, unless the use of the line is merely for the purposes of, or an incidental result of:
(i) turning on the equipment; or
(ii) obtaining power required to operate the equipment; or
(iii) any other action prescribed by the regulations.
An example given in the Bill of a stored communication is an email which has been downloaded from a service provider onto a computer and can be accessed using that computer without any further use of a line. An example of what will not be considered a stored communication is a voicemail message which can only be accessed by dialling a number.

The Bill includes child pornography, arson and terrorism as serious offences in relation to which a warrant may be sought. Acts of terrorism are included as a Class 1 offence. The effect of this amendment is to permit agencies to apply for a warrant authorising the interception of communications where information that may be obtained would be likely to assist in the investigation of an offence constituted by conduct involving an act of terrorism.
Under the Telecommunications (Interception) Act 1979 (**Interception Act**) a warrant may be sought in respect of a class 1 offence from an eligible Judge or a nominated AAT member if the Judge or AAT member is satisfied that, among other factors, the information that would be likely to be obtained by intercepting the communication would be likely to assist in connection with the investigation of a class 1 offence, having regard to:

- the extent to which methods which do not involve intercepting communications have been used by or are available to the agency;
- how much of the information would be likely to be obtained by such methods; and
- how much the use of such methods would be likely to prejudice the investigation.

Other purposes of the Bill are to include certain anti-corruption authorities as eligible authorities for the purposes of the Act, extend the purposes for which lawfully obtained information may be communicated and used in cases

relating to acts or omissions of police officers and the investigation of serious improper conduct by the Anti-Corruption Commission of Western Australia, and to make minor corrections and clarifications to the Interception Act.

Some Policy Considerations

Confusion over "stored communications"

Electronic Frontiers Australia Inc. comments on this Bill on its website.[1] EFA submits that the wording of the Bill is ambiguous in relation to "stored communications" and fails to properly clarify the situation concerning e-mail stored temporarily on an ISP's mail server. Oz NetLaw (the Internet Law Practice of the Communications Law Centre) makes the same point in its submission to the Senate Inquiry.

As stated above, the Bill suggests that an email downloaded from a service provider onto a computer is an example of a stored communication and a voicemail message which can only be accessed by dialling a number is an example of a communication which is not stored. However, it is arguable that an unread email sitting on an ISP's server ,may be considered to be a "stored communication" and therefore not covered by the Interception Act.

It is not clear what kind of access can be obtained to "stored communications" if this legislation were to be enacted. Although the Attorney-General suggests in this second reading speech that search warrants would apply, the Australian Privacy Charter Council points out in its submission to the Senate Committee that such communications might be only protected to the extent provided by Part 13 of the Telecommunications Act, which is itself ambiguous about the treatment of emails and other delayed access messages. The Council notes that certificates under s.282(3), (4) and (5) cannot be used in relation to the "contents of substance or communications" but it is never certain whether this prevents their use for some stored messages, or whether it would be lawful for telecom businesses to give access to stored messages under s282(1) or (2). The Council also submits that in some overseas jurisdictions, such as Germany, emails are protected by strong interception safeguards until they have been downloaded and read by the recipient. The Council is of the view that until the recipient has been able to make a decision about storage, the message must be considered to be protected content.

Privacy Issues

The Federal Privacy Commissioner's submission to the Senate Committee stated that "For most of the 20th Century it has been a fundamental tenet of Western democracy that direct, personal conversations should not be intercepted, except under tightly controlled and extremely limited circumstances. The privacy provisions that this Bill defends, in a general sense, are therefore welcome. It is not clear, however, whether the proposed amendments will provide the clarity that is necessary to ensure that adequate privacy protection is extended to all levels of telecommunications interception." The Privacy Commissioner is concerned by the Bill's ambiguity in relation to emails stored on an ISP's server. The Commissioner is also concerned by the way that protections have been removed from stored communications. The Commissioner submits

[1] www.efa.org.au/Issues/Privacy/tia_bill2002.html, updated 7 April 2002

that evolving technologies have lead to a substantial increase in the use of stored communications, such as email and SMS messaging. Reading someone's stored communication is just as intrusive as intercepting a voice communication and should be subject to an equal level of privacy protection, and certainly a greater level of protection than would be afforded under the *Telecommunications Act 1997*. The Commissioner also suggests that the intrusive nature of the provisions means they should be subject to a sunset clause.

Definition of Terrorism

Oz NetLaw, in its written submission to the Senate Committee and its oral submission at the public forum held by the Senate Committee on May 1 2002 expressed its dissatisfaction with the failure of the Bill to define "terrorism" or "act of terrorism". If we assume that the definition will be carried over from the head bill, this is problematic for 2 reasons: First, it makes the Interception Bill unnecessarily dependant on the passing of the head bill and creates an unnecessary need to import one statutory concept into another statute; Second, the Bill makes an act of terrorism a Class 1 offence, along with murder, kidnapping and narcotics offences. This is of particular concern because of the low threshold required for the issue of warrants in relation to Class 1 Offences. The failure of the Bill to define "terrorism" or "act of terrorism" raises questions about how widely the Bill may be applied and the Bill, as currently drafted, fails to provide adequate assurances regarding civil liberties and privacy of individuals and organisations.

PART 2

Cybercrime Legislation in Australia

Last year, the Federal Government passed the *Cybercrime Act 2001* (**Cybercrime Act**) which amended the *Criminal Code 1995* by inserting new computer offences. The aim of the *Cybercrime Act* was to update the criminal law to reflect the types of crime being committed in cyberspace, and to assist in the prosecution of such crimes. This Act was to commence operation in April 2002.

The provisions of the *Cybercrime Act* are consistent with the terms of the Council of Europe Convention on Cybercrime, which was adopted by the Committee of Ministers in November 2001. A summary of the Convention is set out at Appendix F of this paper.

Similar provisions have been enacted or are intended to be enacted in the State and Territory jurisdictions of Australia.

Under the *Crimes Act 1914* (Cth) the following computer offences exist:

- Causing a communication in the course of carriage to be received by a person or a carriage service other than the person or service to whom it is directed[2];
- Using a carriage service supplied by a carrier or carriage service provider to menace or harass another person in a way that a reasonable person would regard as offensive[3];
- Manipulating or tampering with any facility belonging to r operated by a carrier or carriage service provider or operating or using a device so as to hinder the normal operation of a carriage service[4];
- Intentionally transmitting a signal to a satellite operated by a carrier or carriage service provider[5];
- Manipulating or tampering with a facility belonging to a carrier or carriage service provider[6];
- Connecting equipment to or using equipment connected to a telecommunications network in the commission of an offence if the equipment is unlabelled in breach of a labelling instrument or is not authorised by a connection permit or the connection rules, or if labelled, is labelled as not complying with the applicable standards[7];
- Otherwise than for use by a carrier or carriage service provider in connection with the operation or maintenance of a network, manufacturing, advertising, displaying, offering for sale, selling, using or possessing equipment that will allow switching of

[2] s.85ZD Crimes Act 1914 (Cth)
[3] s.85ZE Crimes Act 1914 (Cth)
[4] s.85ZG Crimes Act 1914 (Cth)
[5] s.85ZH Crimes Act 1914 (Cth)
[6] s.85ZJ Crimes Act 1914 (Cth)
[7] s.85ZK Crimes Act 1914 (Cth)

telecommunications services if the equipment is unlabelled in breach of a labelling instrument or is not authorised by a connection permit or the connection rules, or, if labelled, is labelled as not complying with the applicable standards[8];

- Otherwise than possession by a person in the course of the person's duties of lawfully intercepting communications, manufacturing, advertising, offering for sale, selling, using or possessing an apparatus or device capable of unlawfully intercepting a communication[9].

The *Cybercrime Act* 2001 (Cth) introduces 7 new computer offences. These offences have extraterritorial jurisdiction recognising that computer crime often occurs outside the country. The geographical origins of the conduct constituting the offence is not important because if Australia is affected then prosecution can take place here.

The *Cybercrime Act* 2001 is concerned with offences caused by:

- means of a telecommunications service, or
- means of a Commonwealth computer and /or data contained therein, or
- data held on behalf of the Commonwealth in a computer.

The Act provides for concurrent operation of Commonwealth, State & Territory laws to avoid gaps in jurisdiction and allow computer crimes to be prosecuted where it is most convenient. For example, the State & Territory computer offences would cover computer crime activities by employees using an internal computer network

The term "computer" has been left undefined so that the computer offences embrace technological change. This complies with the discussions raised in the *Model Criminal Code Report* on computer offences.

Summary of the new offences:

It is an offence to knowingly without authorisation:

1. Access[10] or modify data held in a computer or impair electronic communications to or from, a computer[11].

[8] s.85ZKA Crimes Act 1914 (Cth)
[9] s.85ZKB
[10] s.476.1 (1) *Access to data held in a computer* means:

(a) the display of the data by the computer or any other output of the data from the computer; or

(b) the copying or moving of the data to any other place in the computer or to a data storage device; or

(c) in the case of a program—the execution of the program.

[11] s.477.1

The person must intend to commit, or facilitate the commission of, a serious offence against a law of the Commonwealth, a State or a Territory (whether by that person or another person) by the access, modification or impairment.

2. Cause modification of data held in a computer to cause impairment.[12]

   To commit this offence, a person must know that the modification is unauthorised and is reckless as to whether the modification impairs or will impair access to that or any data held in any other computer or the reliability, security or operation, of any such data.

   This offence is intended to catch hackers and persons who circulate disks containing computer viruses.

3. Cause impairment of electronic communications to or from a computer.[13]

   This offence is designed to target 'denial of service attacks'. This occurs, where, for example, a website is swamped with a large volume of unwanted messages which overload and impair the functioning of the computer system.

   This offence applies only to acts and not omissions.

4. Access or modify restricted data held in a computer.[14]

   Restricted data is defined as any data in a computer to which access is restricted by an access control system.

   The provisions is intended to cover situations where, for example, an employee breaks a password on his or her employer's computer system to access the internet or access protected information.
   :

5. Cause any impairment of the reliability, security or operation of data held on a computer disk, credit card, or other device used to store data by electronic means.[15]

   The disk, credit card or other device must be owned or leased by a commonwealth entity.

6. Possess or control data with the intention that the data be used to commit or facilitate the commission of any of the foregoing offences.[16]

[12] s.477.2
[13] s.477.3
[14] s.478.1
[15] s.478.2
[16] s.478.3

7. Produce, supply or obtain data with the intent to commit or facilitate the commission of any of the foregoing offences.[17]

[17] s.478.4

Appendix A

Australia

LIST OF AUSTRALIAN LEGISLATION

Current federal legislation relating to terrorism - list established by Australian Parliament House - Law - Internet Resources. As at 01-05-02.
http://www.aph.gov.au/library/intguide/law/crimlaw.htm#Terrorism

* **Air Navigation Act 1991**
  Part 3 Aviation security
  Implements: Convention on International Civil Aviation; International Air Services Transit Agreement
* **Air Navigation Regulations 1947**
  Part 7 Aviation security
* **Australian Federal Police Act 1979**
* **Australian Protective Service Act 1987**
* **Australian Radiation Protection and Nuclear Safety Act 1988**
* **Australian Security Intelligence Organisation Act 1979**
* **Banking (Foreign Exchange) Regulations 1946**
  Regulations 8(1)(a), 38-39
* **Charter of the United Nations (Anti-Terrorism Measures) Regulations 2001 (Statutory Rules no 297/2001)**
  Explanatory Statement [plain English guide]
* **Charter of the United Nations (Sanctions - Afghanistan) Regulations 2001 (Statutory Rules no 181/2001**)
  Explanatory Statement [plain English guide]
* **Charter of the United Nations (Sanctions - Afghanistan) Amendment Regulations 2001 (Statutory Rules no 298/2001)**
  Explanatory Statement [plain English guide]
* **Chemical Weapons (Prohibition) Act 1994**
  Implements: Convention on the Prohibition of the Development, Production, Stockpiling and use of Chemical Weapons and on their Destruction
* **Crimes Act 1914**
* **Crimes (Aviation) Act 1991**
  Implements: Convention on Offences and certain other Acts Committed on Board Aircraft (the Tokyo Convention of 1963); Convention for the Suppression of Unlawful Seizure of

Aircraft (the Hague Convention of 1970); and the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (the Montreal Convention of 1971

* **Crimes (Biological Weapons) Act 1976**

  Implements: Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction

* **Crimes (Foreign Incursions and Recruitment) 1978**

* **Crimes (Hostages) Act 1989**

  Implements: International Convention Against The Taking Of Hostages

* **Crimes (Internationally Protected Persons) Act 1976**

  Implements: Convention on the prevention and punishment of crimes against internationally protected persons, including diplomatic agents

* **Crimes (Ships and Fixed Platforms) Bill 1992**

  Implements: Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation and the Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf.

* **Criminal Code Act 1995**

  Sections 70, 89-89A, Parts II, IIA, VII

* **Customs Act 1901**

  Section 50

* **Customs (Prohibited Imports) Regulations 1956**

  Regulation 4A Importation of objectionable goods

* **Defence Act 1903**

  Part III Division 1 Calling out and directing utilisation of Defence Force

* **Defence (Special Undertakings) Act 1952**

* **Intelligence Services Act 2001**

  Explanatory memorandum

* **Migration Act 1958**

  Section 501 Refusal or cancellation of visa on character grounds

* **Migration Regulations 1994**

  Schedule 2 (786.224) Provisions with respect to the grant of Subclasses of visas

* **National Crime Authority Act 1984**

* **National Road Transport Commission Act 1991**

  Section 41B National security and special circumstances exemptions — Australian Defence Force

* **Nuclear Non-Proliferation (Safeguards) Act 1987**

  Implements: Nuclear Non-Proliferation Treaty

* **Petroleum (Submerged Lands) Act 1984**

  Section 140B Emergency periods

* **Proceeds of Crimes Act 1987**

* **Public Order (Protection of Persons and Property) Act 1971**

* **Telecommunications Act 1997**

Part 16 Defence requirements and disaster plans

* **Telecommunications (Interception) Act 1979**

* **Weapons of Mass Destruction (Prevention of Proliferation) Act 1995**

Further implements: Biological Weapons Convention, the Nuclear Non-Proliferation Treaty and the Chemical Weapons Convention

STATE AND TERRITORY LEGISLATION

Northern Territory

* **Criminal Code Act 1983**

Schedule I, Part III, Division 2 Terrorism (sections 50-55). Note: terrorism is defined in section 50 and made an offence in section 54

Queensland

* **Police Powers and Responsibilities Act 2000**

Sections 132-137 Emergency use of surveillance devices

Tasmania

* **Classification (Publications, Films and Computer Games) Enforcement Act 1995**

Sections 3, 10

Victoria

* **Petroleum (Submerged Lands) Act 1982**

Sections 151B. Emergency periods

Appendix B

United Kingdom

Information on this legislation can be found at www.cyber-rights.og/documents/anti-terrorism.htm.

TERRORISM ACT 2000

Summary: Failure to disclose information about terrorism. The Act reintroduces the offence of a general failure to disclose information about terrorism. It was previously contained within in the *Prevention of Terrorism Act (PTA*) in relation to Northern Ireland. The new provision extends the provision to domestic and international terrorism.

ANTI-TERRORISM, CRIME & SECURITY ACT 2001

The full text of this Act can be found at www.homeoffice.gov.uk/oicd/antiterrorism. The summary below is largely taken from the Cyber-Rights website (above).

Summary: The Act amends the Terrorism Act 2000. The Act authorises the jailing of foreigners without a hearing if they are identified as potential terrorists. The Act also gives government new powers to monitor a person's telephone, e-mail and internet use. Under the Act police can arrest and hold a person for up to 7 days if they believe an offence is about to be committed. The person may be denied access to a lawyer during this time. Police can also search properties without a warrant.

One of the more controversial sections of the Act is that it shifts the onus of proof. Persons in possession of items, which may be linked to terrorist purposes must prove that the items are for some other purpose.

Purpose of the Act

The Act's purposes are set out in the Explanatory Notes as follows:

- Cut off terrorist funding
- Ensure that government departments and agencies can collect and share information required for countering the terrorist threat
- Streamline relevant immigration procedures
- Ensure the security of the nuclear and aviation industries

- Improve the security of dangerous substances that may be targeted or used by terrorists
- Extend police powers available to relevant forces
- Ensure that we can meet our European obligations in the area of police and judicial co-operation and our international obligations to counter bribery and corruption
- Update parts of the UK's anti-terrorist powers

A central purpose is to enhance anti-terrorist and security capability. It does this via a number of measures including measures relating to data retention and data gateways.

Part 3 and Schedule 4 to the Anti-terrorism, Crime and Security Act 2001 contain provisions to remove current barriers which prevent customs and revenue officers from providing information to law enforcement agencies in their fight against terrorism and other crime. They also harmonise many existing gateways for the disclosure of information for criminal investigations and proceedings.

The Act creates a new gateway giving HM Customs and Excise and the Inland Revenue a general power to disclose information held by them for law enforcement purposes and to the intelligence services in defence of national security. This ensures that known criminals are brought to justice. For example, the provisions of the Act would allow for information on a suspected terrorist financier's bank account to be passed to the police.

The Act also clarifies and harmonises a number of existing gateways for disclosure of information from public authorities to agencies involved in criminal investigations and proceedings. The gateways will ensure that public authorities can disclose certain types of otherwise confidential information where this is necessary for the purposes of fighting terrorism and other crimes.

Part 11 contains provisions facilitating the retention by communications providers of data about their customers' communications for national security purposes. It sets up a structure within which the Secretary of State can issue a code of practice relating to the retention of communications data by communications service providers, such as telephone and internet companies. Retained data can then be accessed by the security, intelligence and law enforcement agencies under the terms of a code of practice, which is being drawn up in consultation with industry and the Information Commissioner.

Section 104 provides that if the voluntary scheme proves ineffective the Secretary of State may by affirmative order be authorised to impose mandatory retention directions on communications service providers. Section 105 provides that the power to invoke the mandatory scheme in section 104 will itself lapse unless renewed by affirmative order.

Communications data is information about the use made of communications by a service provider's customers, e.g. subscriber details, itemised billing. It does not include the content of such communications, i.e. what was said over the phone or written in an email.

Investigators use this data to trace criminals' activities and establish links between conspirators. Currently communications service providers are obliged to erase this data when they no longer need it for commercial purposes. This has a severe impact on criminal investigations.

The Telecommunications (Data Protection and Privacy) Regulations 1999 regulate the retention of such data by communication service providers providing that such data can only be retained for certain specific purposes. Otherwise it must be erased or made anonymous. Communications data can be a useful tool for law enforcement agencies and if held by a communications service provider is accessible by a public authority under Chapter II of Part I of the Regulation of Investigatory Powers Act 2000. However, whilst the Regulations permit the retention of communications data on national security and crime prevention grounds, they do not give any general guidance as to when these might apply. Accordingly, before these provisions were introduced communications service providers did not have a clear lawful basis for retaining communications data beyond the period for which it was required for their own business purposes.

The Regulation of Investigatory Powers Act 2000 (RIPA) sets out clear limits on the purposes for which the security, intelligence and law enforcement agencies may request access to data relating to specific communications (e.g. relating to a particular customer or telephone line). Mass trawls or "fishing expeditions" are NOT permitted. The Anti-Terrorism Act allows for a voluntary code of practice, defined in statute, to ensure that service providers have a clear remit for retaining data, which complement the powers given to public authorities in RIPA.

It also contains a reserve power to review these arrangements and issue directions under secondary legislation if necessary. The need to maintain a reserve power must be reviewed every two years and may be renewed by affirmative order. Once the power has been exercised, there is no need for further review.

REGULATION OF INVESTIGATORY POWERS ACT 2000

Summary: The Act sets out limits on the purposes for which the security, intelligence and law enforcement agencies may request access to data relating to specific communications. These provisions complement the Terrorism Act 2000 by clarifying the lawful basis for the retention of data by communications service providers.

Purpose of the Act

The purpose of the Act is to ensure that relevant investigatory powers are used in accordance with human rights. The powers covered include:

- interception of communications;
- the acquisition of communications data;
- intrusive surveillance; and
- covert surveillance in the course of specific operations.

The Act is designed to ensure that the law covers:

1. the purposes for which they may be used;
2. which authorities can use the powers;
3. who should authorise each use of the power;
4. the use that can be made of the material gained;
5. independent judicial oversight;
6. a means of redress for the individual.

Section 1 of the Act makes it an offence "for a person intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communication in the course of its transmission…" It applies to public postal and telecommunications systems and to private telecommunications systems which are linked to a public network.

Comment and Policy Considerations

Quicklinks, Issue no. 217 – 16 December (BBC)

"The House of Lords finally agreed to the Anti-terrorism, Crime and Security Act after concessions from Home Secretary David Blunkett. In a major policy U-turn, Mr Blunkett agreed to drop proposals making incitement to religious hatred a criminal offence. The new act allows foreign terror suspects to be detained without trial where they cannot be deported – those arrested will have right to appeal although not to a full court of law. That power will, however, have to renewed by Parliament after 15 months. Other measures mean police can access more data, such as tax returns, but disclosure must be proportionate to tackling terrorism. Other concessions included: Limiting the introduction of anti-terrorist measures agreed at a European level, allowing seven "wise people" to review the measure after two years, limiting police access to electronic data such as e-mail and the internet on suspicion of terrorist activity."

Patrick Wintour, chief political correspondent, The Guardian

Friday December 7, 2001

Lord Strathclyde, the Tory leader in the house, said: "The amended bill still gave exceptional new powers to fight terrorism, which everyone wants.

"The amendments deny the state the right, which many feared, to commandeer private and personal information on the merest suspicion of a criminal offence quite unrelated to terrorism..."

The defeats threw out a government plan to give police and other public bodies powers to demand a wide range of public bodies, including schools and hospitals, to disclose any information relevant to possible criminal investigation or proceedings.

New powers to require internet service providers and businesses to retain data for use in potential criminal investigations by the police were thrown out. Peers instead restricted the right to seek disclosure to cases involving threat to national security or terrorism.

Baroness Buscombe, the Tory peer, called the bill draconian and insisted it "must not be used as a convenient vehicle and excuse for legitimising fishing expeditions".

Later peers voted to insert the right to judicial review of a home secretary's decision to order indefinite detention of a suspected foreign terrorist.

Later, the home secretary said in a statement: "Terrorists are not just involved in terrorism; they are also involved in many other types of crime to fund and facilitate their activities."

He added: "We should also bear in mind that links with terrorism may only be established once a criminal investigation is well under way."

The Home Office's statement on Human Rights

"The provisions of the Act are compatible with the European Convention on Human Rights, but the Government finds it necessary to derogate from Article 5(1) of the Convention in respect of the detention powers in the Act.

The events of September 11th pose a direct challenge to the UK to ensure we are as fully prepared as possible to meet the threat of terrorism. The Anti-Terrorism, Crime and Security Act 2001 is the result of an extensive review of our existing legislation that we have the necessary powers to ensure the safety of UK citizens at home and abroad. The review of terrorism legislation which proceeded the introduction of The Terrorism Act 2000 meant that we already

had in place many of the powers needed to protect UK citizens. This Act expands on those powers already established to take account of the changed threat and to equip the UK better to face the menace of global terrorism.

It strikes a balance between respecting our fundamental civil liberties and ensuring that they are not exploited by those who would destroy them. It brings specific targeted and proportionate measures into place so that the enforcement, intelligence and other services can tackle the new terrorist threat."

Appendix C

United States of America

There is a considerable amount of legislation since September 11. The Thomas Database of the Library of Congress lists 17 pages of bills, acts, and resolutions under the title, "LEGISLATION RELATED TO THE ATTACK OF SEPTEMBER 11, 2001" (http://thomas.loc.gov/home/terrorleg.htm)

Probably the two main pieces of legislation relevant to this subject are the **USA PATRIOT Act** (enacted on 26 October 2001) and the **Cyber Security Enhancement Act of 2001** (not in force), outlined below.

Notes on the legislative developments are available from several sources.

- The Centre for Democracy and Technology includes analysis of how the PATRIOT Act changed US Law. http://www.cdt.org/security/010911response.shtml

- Electronic Frontier Foundation provides: "EFF Analysis Of The Provisions Of The USA PATRIOT Act That Relate To Online Activities (Oct 31, 2001)" http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html

- Current US federal law in the form of the consolidated US Code can be accessed at http://www4.law.cornell.edu/uscode/

There is debate and discussion on a range of other proposals (such as use of ID cards), though not necessarily reflected in legislative initiatives. Among the range of other Acts are:

TERRORISM RISK PROTECTION ACT

"H.R. 3210 creates a temporary industry risk spreading program to ensure the continued availability of commercial property and casualty insurance and reinsurance for terrorism-related risks to limit immediate market disruptions, encourage economic stabilization, and facilitate a transition to a viable market for private terrorism risk insurance." http://www.gop.gov/committeecentral/docs/bills/107/1/bill.asp?bill=hr3210

FINANCIAL ANTI-TERRORISM ACT OF 2001

"H.R. 3004, the Financial Anti-Terrorism Act of 2001, provides the United States with new tools to combat the financing of terrorism and other financial crimes. The measure contains provisions to strengthen law enforcement authorities, as well as to enhance public-private cooperation between government and industry in disrupting terrorist funding."
http://www.gop.gov/committeecentral/docs/bills/107/1/bill.asp?bill=hr3004

USA PATRIOT ACT

Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism Act (USA PATRIOT Act).

The Act limits judicial approval and review of government electronic surveillance measures. It also expands government surveillance powers and lowers the standard of evidence, which must be met for obtaining a person's personal records. Some provisions of the Act are subject to a "sunset clause" and will expire in 2006.

Non-US citizens could be tried in military tribunals rather than civil courts. Widening of powers in relation to intelligence gathering, immigration violations and criminal procedure. Increased powers to intercept communications related to an expanded list of terrorism acts. More information can be obtained from Internet service providers, and expands the range of records that can be sought by a court order. Justice Department has issued an executive regulation allowing monitoring of traditionally confidential conversations between lawyers and detainees in Federal custody.

Comment and policy considerations

The Center For Democracy & Technology, Washington DC
http://www.cdt.org/publications/pp_7.11.shtml

"President Bush on October 26 signed into law an anti-terrorism package that dismantles many privacy protections for communications and personal data. Many of the provisions are not limited to terrorism investigations, but apply to all criminal or intelligence investigations.

The Bill:

* Allows government agents to collect undefined new information about Web browsing and e-mail without meaningful judicial review;

* Allows Internet Service Providers, universities, network administrators to authorize surveillance of "computer trespassers" without a judicial order;

* Overrides existing state and federal privacy laws, allowing FBI to compel disclosure of any kind of records, including sensitive medical, educational and library borrowing records, upon the mere claim that they are connected with an intelligence investigation;

* Allows law enforcement agencies to search homes and offices without notifying the owner for days or weeks after, not only in terrorism cases, but in all cases - the so-called "sneak and peek" authority;

* Allows FBI to share with the CIA information collected in the name of a grand jury, thereby giving the CIA the domestic subpoena powers it was never supposed to have;

* Allows FBI to conduct wiretaps and secret searches in criminal cases using the lower standards previously used only for the purpose of collecting foreign intelligence."

Centre for Democracy and Technology
Washington DC

Summary and Analysis of Key Sections of USA PATRIOT ACT of 2001
E-Commerce & Privacy Group: Ron Plesser, Jim Halpert, Milo Cividanes
Date: October 31, 2001
http://www.cdt.org/security/011031summary.shtml

"Service providers have expanded obligations under this Act. For example, the definitions of trap and trace device have been significantly expanded to allow for access to certain information (excluding content) concerning Internet activity. Another example is the obligation to respond to a nationwide service of process that in some instances may not identify your company on the face of the service document. The Act does permit you to seek clarifications.

The Patriot Act contains three favorable features for communications companies. First, it provides specifically that nothing in the Act creates any new requirements for technical assistance, such as design mandates. Therefore, the right, if any, of the government to require use of design mandates such as "Carnivore" technology or other technical assistance by service providers is not affected or augmented by the Patriot Act.

Second, in several important areas, the Act expands service provider protections (including immunities and good faith defenses) for complying with new or existing surveillance authority, as

is the case in FISA wiretaps and disclosures of records. The Act also creates expanded ability for the government to conduct wiretaps, at the request of service providers, of hackers and other "trespassers" on service provider networks.

Third, the Patriot Act amends and limits the Cable Act to make it clear that companies offering cable-based Internet or telephone service will be subject to the requirements of the Cable Act to notify subscribers of government surveillance requests only where detailed cable viewing information is being sought. In all other instances, cable operators offering these services can respond to a government surveillance request under ECPA, which does not require service providers to notify subscribers of requests."

Extract from the same article of comments concerning provisions relevant to Internet companies, Internet service providers, and telecommunications carriers:

Section 216: Modification of authorities relating to use of pen registers and trap and trace devices.

Bottom Line: Probably the most significant surveillance expansion in the Act. Clarifies that pen register/trap and trace authority applies to Internet traffic, permits nationwide service of process, and requires reports on use of "Carnivore"-type technology. Does not sunset.

This provision makes three changes to existing law. First, by adding the terms "routing" and "addressing" to the phrase "dialing and signaling information," this amendment is intended to clarify that the pen register and trap and trace authority under ECPA applies to Internet traffic, provided that the information retrieved by these devices "shall not include the contents of any communication." Although the term "content" has a statutory definition, see 18 U.S.C. § 2510(8) (the term content "includes any information concerning the substance, purport, or meaning of [the] communication"), it is vague and has not been tested in the context of Internet communications. It will be important to monitor law enforcement requests to determine what Internet-related information law enforcement seeks to obtain under the new law beyond the "to" and "from" header information in e-mail communications that it already receives under existing pen register and trap trace law.

Second, this provision also grants federal courts the authority to issue pen register and trap and trace orders that are valid anywhere in the United States, not just within their own jurisdiction. The advent of nationwide service will likely result in providers being asked with some frequency to render assistance even though they are not specifically named in the order and the assistance being requested is not specifically defined in the order.

We worked on two modifications to this provision that permit service providers to demonstrate that in they are in fact complying with this new authority, and are eligible for a statutory good-faith defense or immunity from suit. First, Section 216 provides that a service provider has the right to receive a written certification from law enforcement confirming that the order applies to the provider being served with it. Moreover, Section 216 amends 18 U.S.C. § 3124(d) to clarify that compliance with a pen register/trap and trace "order," rather than the express "terms of such order" makes a service provider eligible for statutory immunity. Nevertheless, nationwide service could make it very difficult for local or regional service providers to oppose, modify, or contest court orders because it will require service providers to travel to numerous courts, in multiple jurisdictions, to address concerns over the breadth of court orders.

Third, Section 216 directs law enforcement to file an ex parte and in camera report with the court whenever it uses a "Carnivore" device (defined as "installing and using its own pen register or trap and trace device on a packet-switched network" of a provider). The report would identify, inter alia, "the configuration of the device at the time of its installation" and "any information which has been collected by the device." The existence of these reports may help in future public policy debates on the propriety of the government compelling ISPs to install "Carnivore" devices and the extent of the use of such devices.

The provision is a permanent change to federal law and is exempted from the sunset provision of Section 224.

Section 217: Interception of computer trespasser communications.

Bottom Line: Protects the government from liability for warrantless interceptions of hackers and similar "trespassers" at the request of a service provider; service providers' protection is less clear.

This section provides new protection from liability for government officials if they conduct warrantless wiretaps of computer "trespassers" (persons who are not known to owner or operator of the computer to have a contractual relationship with that owner or operator and who gain unauthorized access to the system). The drafters presume that, under the "switchboard" provision of existing law (18 U.S.C. § 2511(2)(a)(i)), owners or operators of computers have the authority to intercept the communications of trespassers. Section 217 is designed to protect law enforcement officials when the owner or operator delegates that authority to law enforcement. (Under the “switchboard” exception, a service provider can intercept or disclose a user’s communications when “necessary . . . to the protection of the right or property of the provider.”)

Although the House Judiciary Committee bill contained language that would have explicitly protected the service provider from liability for authorizing or providing facilities or technical

assistance for this surveillance, the final legislation does not contain this language. To the extent that a court determines that the "switchboard" exception does not authorize owners or operators of computers to intercept the communications of trespassers, this omission could present a problem because there is case law indicating that ECPA's good faith defenses are not a basis for avoiding liability where actions are taken on the basis of an erroneous belief that a statutory provision authorizes the action. Nevertheless, Section 217 does not compel service providers to permit law enforcement to engage in the warrantless surveillance of trespassers, but rather leaves that decision entirely to the discretion of the service provider.

Section 814: Deterrence and prevention of cyber-terrorism. (Computer Fraud and Abuse Act Amendments: Narrowing Civil Liability)

Bottom Line: Expands government's authority to prosecute hacking and denial of service attacks, codifies In re DoubleClick decision for private litigation under the Computer Fraud and Abuse Act, clarifies the meaning of damage/loss under the CFAA, and precludes private lawsuits for negligent design or manufacture of hardware or software.

At the Administration's request, Section 814 increases criminal penalties for Computer Fraud and Abuse Act (CFAA) violations, adds computers located outside the U.S. to the definition of "protected computers" covered by the statute, adds a definition for the important, but previously undefined, statutory term "loss," and clarifies that criminal prosecutions for hacking or unauthorized transmissions may be brought under 18 U.S.C. § 1030(a)(5) if a "related course of conduct" causes $5,000 in loss. At the same time, Section 814 contains several improvements upon current law for civil defendants, who have increasingly become a target of plaintiff class actions brought using the private right of action contained in the CFAA.

First, § 814(a) provides that the CFAA $5,000 damage threshold is satisfied through loss caused by a related course of conduct "for purposes of an investigation, prosecution, or other proceeding brought by the United States only." The negative implication of this language appears to be that a single act, not a related course of conduct, producing $5,000 in harm is necessary for anyone other than the government to bring a private lawsuit under the CFAA. If this interpretation prevails in the courts, then this provision will codify a recent decision in In re DoubleClick Privacy Litigation, 154 F. Supp.2d 497 (S.D.N.Y. 2001), that a civil action under § 1030(g) generally may be brought only if a "single act" produces $5,000 of loss within the meaning of the statute.

Second, § 814(d) generally preserves the current $5,000 threshold for private lawsuits under § 1030(g) of the CFAA for "loss" to a computer system, except for cases involving damage to a system used by the government for the administration of justice, national defense, or national security. It also clarifies that the $5,000 threshold required for a private lawsuit under § 1030(g) applies both to actions for "damage" and "loss," thereby eliminating a statutory ambiguity that plaintiffs' class action lawyers had attempted to use to avoid the $5,000 threshold.

Third, § 814(d) contains a provision from the original Senate bill stating that "[n]o action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware." Although this language could be somewhat clearer, this provision likely will be very helpful in obtaining dismissal of CFAA claims such as the ones challenging alleged defects in software or hardware that have been brought by several large class actions.

CYBER SECURITY ENHANCEMENT ACT OF 2001

Summary of the legislation from Library of Congress - Thomas Database
http://thomas.loc.gov/cgi-bin/bdquerytr/z?d107:HR03482:@@@L&summ2=m&

"Cyber Security Enhancement Act of 2001 - Directs the United States Sentencing Commission to amend federal sentencing guidelines and otherwise address crimes involving fraud in connection with computers and access to protected information, protected computers or restricted data in interstate or foreign commerce or involving a computer used by or for the Federal Government. Includes among exceptions to otherwise criminal conduct emergency disclosures to a governmental entity by an electronic communication service and specified disclosures made in good faith. Increases penalties for violations where the offender knowingly causes or attempts to cause death or serious bodily injury.

Directs the Attorney General, acting through the Federal Bureau of Investigation, to establish and maintain a National Infrastructure Protection Center to serve as a national focal point for threat assessment, warning, investigation, and response to attacks on the Nation's critical infrastructure, both physical and cyber.

Establishes within the Department of Justice an Office of Science and Technology to work on law enforcement technology issues, addressing safety, effectiveness and improved access by Federal, State, and local law enforcement agencies. Includes investigative and forensic technologies, corrections technologies, and technologies that support the judicial process.

Abolishes the Office of Science and Technology of the National Institute of Justice, transferring functions, activities, and funds to the newly formed Office.

Requires the Director of the Office to operate and support National Law Enforcement and Corrections Technology Centers."

Comment and Policy Considerations

Caron Carlson, *eweek* February 27, 2002
"Bill Gives Gov't Greater Access to E-Mail"
http://www.eweek.com/article/0,3658,s=712&a=23326,00.asp

Do you want the Department of Motor Vehicles to be able to read the private e-mail that runs over your network?

If a bill approved by the crime panel of the House Judiciary Committee becomes law, any government entity--not just law enforcement agencies--will be able to receive e-mail and other electronic communications without a court order, so long as a service provider believes an emergency requires its disclosure without delay. The measure is part of a larger initiative aimed at reducing computer-related crime.

"A mouse can be just as dangerous as a bullet or a bomb," said Rep. Lamar Smith, R-Texas, chairman of the crime subcommittee and sponsor of the Cyber Security Enhancement Act of 2001. "We cannot afford to let technology be our weakness."

The measure would broaden a provision in the hastily enacted USA PATRIOT Act, which was signed into law just four months ago. The provision, whose primary purpose was to eliminate disincentives to sharing crime-related information with law enforcement, covers situations when a service provider reasonably believes that an emergency requires immediate disclosure.

The pending bill would further lower the bar to turning over private communications by authorizing a service provider to share data with the government if the provider, in good faith, believes an emergency requires disclosure without delay. The initiative concerns privacy advocates, who argue that the existing legislation already infringes on Fourth Amendment rights and is devoid of checks and balances that discourage illegal disclosures.

"The communications [that can be disclosed] are not limited to communications related to a crime; there is no report to a judge, no report to Congress, and there is no notice to the individual whose e-mail is disclosed," said James Dempsey, deputy director of the Center for Democracy and Technology in Washington. "This bill says not only that the information can go to law enforcement, but it can go to any government authority, including the proverbial dog catcher," Dempsey said

The bill would also increase penalties for computer crimes, establish a new FBI National Infrastructure Protection Center, and establish an Office of Science and Technology at the

Department of Justice, charged with developing personalized guns, bullet-resistant and explosion-resistant glass, monitoring systems that provide precise location information, and DNA identification technologies.

The IT industry widely supports the legislation because it reduces network operators' liability when sharing information with the government. "The threat of cyber attacks is real, and its fallout is a significant economic drag on the U.S. economy, precisely at a time when we can least afford it," Robert Cresanti, vice president of policy at the Business Software Alliance, said in a prepared statement, applauding the subcommittee's passage of the bill.

STATE LAWS

An overview of State Legislation Addressing Terrorism is available from the National Conference of State Legislatures.
http://www.ncsl.org/programs/press/2001/freedom/terrorism01.htm

Appendix D

Canada

The major act covering post-September 11 initiatives is the **Anti-terrorism Act**. This was supplemented by the **Public Safety Act**.

The Department of Justice summaries the anti-terrorism package as achieving three ends:

- Identify, prosecute, convict and punish terrorist groups
- Provides new legislative tools to law enforcement and national security agencies
- Stronger laws against hate crimes and propaganda.

Information is available in "Highlights of Anti-Terrorism Act", Department of Justice, (http://canada.justice.gc.ca/en/news/nr/2001/doc_27787.html)

ANTI-TERRORISM ACT 2001

The Act received royal assent on 18 December 2001.

Information on the Act is available from the site of the Parliament of Canada. The following summary is taken from the legislative outline provided on that site.
http://www.parl.gc.ca/37/1/parlbus/chambus/house/bills/government/C-36/C-36_3/C-36_cover-E.html

"This enactment amends the *Criminal Code*, the *Official Secrets Act*, the *Canada Evidence Act*, the *Proceeds of Crime (Money Laundering) Act* and a number of other Acts, and enacts the *Charities Registration (Security Information) Act*, in order to combat terrorism.

Part 1 amends the *Criminal Code* to implement international conventions related to terrorism, to create offences related to terrorism, including the financing of terrorism and the participation, facilitation and carrying out of terrorist activities, and to provide a means by which property belonging to terrorist groups, or property linked to terrorist activities, can be seized, restrained and forfeited. It also provides for the deletion of hate propaganda from public web sites and creates an offence relating to damage to property associated with religious worship.

Part 2 amends the *Official Secrets Act*, which becomes the *Security of Information Act*. It addresses national security concerns, including threats of espionage by foreign powers and terrorist groups, economic espionage and coercive activities against émigré communities in Canada. It creates new offences to counter intelligence-gathering activities by foreign powers

and terrorist groups, as well as other offences, including the unauthorized communication of special operational information.

Part 3 amends the *Canada Evidence Act* to address the judicial balancing of interests when the disclosure of information in legal proceedings would encroach on a specified public interest or be injurious to international relations or national defence or security. The amendments impose obligations on parties to notify the Attorney General of Canada if they anticipate the disclosure of sensitive information or information the disclosure of which could be injurious to international relations or national defence or security, and they give the Attorney General the powers to assume carriage of a prosecution and to prohibit the disclosure of information in connection with a proceeding for the purpose of protecting international relations or national defence or security.

Part 4 amends the *Proceeds of Crime (Money Laundering) Act*, which becomes the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. The amendments will assist law enforcement and investigative agencies in the detection and deterrence of the financing of terrorist activities, facilitate the investigation and prosecution of terrorist activity financing offences, and improve Canada's ability to cooperate internationally in the fight against terrorism.

Part 5 amends the *Access to Information Act*, *Canadian Human Rights Act*, *Canadian Security Intelligence Service Act*, *Corrections and Conditional Release Act*, *Federal Court Act*, *Firearms Act*, *National Defence Act*, *Personal Information Protection and Electronic Documents Act*, *Privacy Act*, *Seized Property Management Act* and *United Nations Act*. The amendments to the *National Defence Act* clarify the powers of the Communications Security Establishment to combat terrorism.

Part 6 enacts the *Charities Registration (Security Information) Act*, and amends the *Income Tax Act*, in order to prevent those who support terrorist or related activities from enjoying the tax privileges granted to registered charities.

Comment and Policy Implications

Criticism of Bill C-36 is available from the following sources:

- The Canadian Centre for Policy Alternatives
  http://www.policyalternatives.ca/publications/c-36.html
- Amnesty International
  http://www.amnesty.ca/sept11/C36.htm
- Canadian Association of University Teachers
  http://www.caut.ca/english/bulletin/2001_nov/president.asp

PUBLIC SAFETY ACT

The following introduction taken from the information on Bill C-42 'The Public Safety Act' provided by the Parliament of Canada explains the relationship of the Public Safety Act to the Anti-terrorism Act.
http://www.parl.gc.ca/common/Bills_ls.asp?lang=E&Parl=37&Ses=1&ls=C42&source=Bills_Individual

"Bill C-42, the proposed *Public Safety Act*, received First Reading in the House of Commons on 22 November 2001. The Bill is one of three in the government's legislative response to the events of September 11 in the United States. Bill C-36, the *Anti-terrorism Act*, received Royal Assent on 18 December 2001. On 28 November 2001, the House of Commons unanimously consented on a motion to delete from Bill C-42 section 4.83 in clause 5 amending the *Aeronautics Act*. The same day, that section was introduced as Bill C-44 in order to provide for speedier passage than consideration as part of Bill C-42 would have allowed for. It received Royal Assent on 18 December 2001.

Bill C-42 amends 19 existing Acts, and enacts a new statute to implement the Biological and Toxin Weapons Convention, which entered into force on 26 March 1975."

The Act will amend the following Acts:

- Aeronautics Act
- Department of Health Act
- Food and Drugs Act
- Hazardous Products Act
- Navigable Waters Act
- Pest Control Products Act
- Quarantine Act
- Radiation Emitting Devices Act
- Canada Shipping Act; Canada Shipping Act, 2001.

Computer Systems and Networks are dealt with under PART 10, which amends the National Defence Act. The following summary of these provisions is taken from the Parliament website document http://www.parl.gc.ca/common/Bills_ls.asp?lang=E&Parl=37&Ses=1&ls=C42&source=Bills_Individual

"Clause 87 creates a new Part V.1 of the Act, dealing with the interceptions of communications involving the Department of National Defence (DND) or Canadian Forces computer systems. This new provision ensures that DND and the Canadian Forces have the authority to protect their computer systems networks and the information they contain from attack or manipulation."

"New section 273.7 allows the Minister of National Defence to authorize in writing public servants in the department or persons acting on behalf of the department or the Forces who operate, maintain or protect computers and networks to intercept private communications. The interception can only be carried out in order to identify, isolate or prevent the unauthorized use of, interference with, or damage to departmental and military computers and networks. The Minister may also authorize in writing the Chief of the Defence Staff to direct military personnel to carry out such interceptions. In either case, the Minister must be satisfied that certain conditions are met. These are that:

- the interception is necessary to identify, isolate or prevent an unauthorized use of, interference with, or damage to the systems or networks or data, and that measures are in place to ensure that only information that is essential for these purposes will be used or retained;
- the information cannot be reasonably obtained by other means; and
- that measures are in place to protect Canadians' privacy in the use or retention of the information.

Authorizations or renewals are for periods not exceeding one year. Part VI of the *Criminal Code*, which otherwise prohibits the interception of private communications occurring within Canada, does not apply. In addition, government officials are not civilly liable for improper disclosure or use of intercepted information under section 18 of the *Crown Liability and Proceedings Act*.

Some amendments to the *National Defence Act* were also made in Bill C-36, the *Anti-terrorism Act*. Thus, under clause 122 of Bill C-42, new section 273.7 will be renumbered 273.8 and new section 273.9 will be added to the Act. The new section indicates the duties of the Commissioner of the Communications Security Establishment (CSE) with regards to the interception of communications originating from, directed to, or transiting through departmental or military computer systems and networks. The Commissioner of the CSE has jurisdiction to: review the activities of the department and the Forces to ensure compliance with the law; undertake an investigation in response to a complaint; and inform the Minister of National Defence and, if appropriate, the Attorney General if any activity of the department or the Forces does not appear to be in compliance with the law."

Appendix E

European Union

TELECOMMUNICATIONS PRIVACY DIRECTIVE

In light of the events of September 11th, the European Commission altered original proposals to update its 1997 Directive on telecommunications privacy in favour of more comprehensive amendments. Despite opposition from the Commission's own Data Protection Commissioners, the Commission agreed to propose a raft of measures – recommended by security and law enforcement agencies – to allow for the retention and interception of prescribed data.

The amendments are due to be considered by the Council of the European Union on 15 May 2002 with Members of the European Parliament likely to be subject to significant pressure from their home nation governments to support the measures. In specific terms, the proposed amendments to Article 15.1, known as the 'common position', will restrict the scope of existing Article rights and obligations when such restriction constitutes a necessary measure "for the protection of public security, defence and State security (including the economic well-being of the State when the activities relate to State security matters) and for the enforcement of criminal law …"[18].

EU PROPOSAL FOR A COUNCIL FRAMEWORK DECISION ON COMBATING TERRORISM

Available at http://europa.eu.int.
This proposal has been adopted by the European Parliament, and awaits final signature. A Framework Decision is binding on member States, but only in the result to be achieved. The form and methods are left to the States.

Definition of terrorism

- Defined as offences intentionally committed against one or more countries, their institutions or people, with the aim of intimidating them, or seriously altering or destroying the political, economic, or social structures of a country. (Article 3)
- This article also sets out a list of offences which will be dealt with as terrorist offences if they fall within the above definition.

[18] Amendment 1, recital 11, *Draft Recommendation for Second Reading*, 15396/2/2001 – C-50035/2002 (12 March 2002)

- There are concerns about this broad definition of terrorist offences, which could have the potential to criminalise public and social acts of protest as terrorism.[19]
- Article 3 also defines terrorist groups as a structured organisation that acts in concert to commit the offences specified earlier.

Extradition and prosecution

- Article 11 requires that those States who do not extradite its nationals under its laws must establish jurisdiction over those who commit terrorist acts in other member States. If appropriate, it must prosecute such nationals for terrorist offences committed elsewhere.
- However, this article will be superseded once a related proposal comes into effect. This proposal will overcome extradition procedures and establish a European Arrest Warrant, which can be executed throughout all member States.[20]

Exchange of information

- Article 13 requires member States to establish points of contact for exchange of information for the purposes of this Framework Decision.
- It also requires the sharing of any information on possible terrorist offences affecting another member State.
- This aspect could also be supplanted by another proposal which seeks to extend the Schengen Information System (SIS).[21] The SIS is an existing system for sharing of law enforcement information among the States.
- This would extend the SIS to include a database of persons to be prevented from travelling to certain events during certain periods, and a restricted access database of terrorists.

Money laundering

- This framework decision does not deal with money laundering specifically, but this aspect has been updated in light of the terrorist events with an amendment to the EU's directive on money- laundering.[22]
- The scope of the obligations on member States has been extended. It now extends money-laundering efforts to proceeds of all serious crime, while previously it only covered drug offences.

[19] A group of lawyers have a drafted an appeal against this proposal. See http://www.statewatch.org/news/2001/nov/07appeal.htm.
[20] See the EU Council Framework Decision on the European arrest warrant and the surrender procedures between the Member States. This has also been adopted by the European Parliament.
[21] As reported at http://www.statewatch.org/news/2002/apr/01sis.htm.
[22] See EU announcement at http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=IP/01/1441|0|RAPID&lg=EN

- Obligations are also extended to non-financial activities and professions which could be vulnerable to misuse by money launderers, such as real estate agents and dealers in high-value goods.

Appendix F

Council of Europe

COUNCIL OF EUROPE CONVENTION ON CYBERCRIME

Summary: In November 1996 the European Committee on Crime Problems (CDPC) decided in to set up a committee of experts to deal with cyber-crime. The revised and finalised draft Convention and its Explanatory Memorandum were submitted for approval to the CDPC at its 50th plenary session in June 2001, following which the text of the draft Convention was submitted to the Committee of Ministers for adoption and opening for signature.

The Cybercrime Convention was signed by the following member states of the Council of Europe in Budapest 23 November 2001:

> Albania, Armenia, Belgium, Bulgaria, Croatia, Cyprus, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Malta, Moldova, Netherlands, Norway, Poland, Portugal, Romania, Spain, Sweden, Switzerland, The former Yugoslav Republic of Macedonia, Ukraine and Turkey.

Non- member states that have also signed are Canada, United States, Japan and South Africa. However, as five countries have not yet ratified the Convention, it has not yet entered into force.

The Cyber-crime Convention covers three areas:

(i) harmonisation of national criminal laws relating to both computer crime and offences committed by use of computers and telecommunications systems.
(ii) new procedures and rules providing for domestic investigatory powers necessary to assist the investigation and prosecution of computer crime;
(iii) new rules to set up a regime for international cooperation in the detection and prosecution of cyber-crime.

Harmonisation of national criminal laws

Articles 2 to 11 list the basic requirements that a state must adopt when legislating criminal offences.

Computer Specific offences

Article 2: Illegal Access

Each party must adopt legislative measures to establish the criminal offence of intentionally accessing a computer system without right.

Article 3: Illegal interception

Each party must adopt legislative measures to establish the criminal offence of intentionally intercepting non-public transmissions without right.

Article 4: Data interference

Each party must adopt legislative measures to establish the criminal offence of intentionally damaging and interfering with computer programs and data without right.

Article 5: System functioning

Each party must adopt legislative measures to establish the criminal offence of intentionally hindering the functioning of computer systems without right.

Article 6: Misuse of devices

Each party must adopt legislative measures to establish the criminal offence of intentionally misusing 'hacker' tools or programs to be used in the committing of offences in Article 2-5 without right.

Computer related offences

Article 7: Computer-related forgery

Each party must adopt legislative measures to establish the criminal offence of intentionally altering computer data to result in inauthentic data with the intent to be considered authentic.

Article 8: Computer-related fraud

Each party must adopt legislative measures to establish the criminal offence of intentionally altering computer data or interfering with computer systems with the fraudulent intent to procure an economic benefit.

Content-related offences

Article 9: Offences related to Child pornography

Each party must adopt legislative measures to establish the criminal offence of intentionally producing, making available, distributing, procuring or possessing child pornography through a computer system.

Article 10: Offences related to infringement of copyright and related rights.
Each party must adopt legislative measures to establish the criminal offence which meet the obligations of the Bern Convention for the Protections of Literary and Artistic works, the agreement of Trade-related Aspects of Intellectual Property Rights, the WIPO Copyright Treaty, the Rome convention and the WIPO Performances and Phonograms Treaty.

Ancillary liability and sanctions

Article 11: Attempt and aiding or abetting
Applies to Articles 2 to 10.

Article 12: Corporate Liability
A legal person (corporation) is liable for the criminal acts (Articles 2-11) of employees in a leading role (or someone under their failed supervision) and which are undertaken for the benefit of that legal person.

The above articles are only low-level general principles so that each state retains flexibility in terms of what acts and elements will be included in the offences.

Articles 2 to 9 require that in each case the criminal offence must be committed "intentionally" – which is left open to national interpretation – and "without right" – which would leave lawful government acts unaffected.

Procedural Rules for the Detection, Investigation of Cyber-crime

Section 2 sets out the procedural measures which a party must implement for the criminal investigation of cyber-crime.

Article 16: Expedited preservation of stored computer data
Each party must preserve specified computer data vulnerable to loss or modification.

Article 17: Expedited preservation and partial disclosure of traffic data associated with data communications for up to 90 days
Each party must preserve and partially disclose traffic data to identify service providers.

Article 18: Production order
Each party must ensure introduced measures allow for the production of stored computer data.

Article 19: Search and Seizure of stored computer data

Each party must ensure introduced measures allow for the search and seizure of stored computer data.

Article 20: Real-time collection of traffic data

Each party must ensure introduced measures can compel a service provider to collect traffic data in real time.

Article 21: Interception of content

Each party must ensure introduced measures can compel a service provider to collect content in real time.

International Co-operation

Chapter 3 sets out the principles for international co-operation to the widest extent possible for the investigation in criminal matters described in Articles 2-11.

Article 24: Extradition

Articles 2-11 are extraditable offences.

Article 25: General Principles relating to mutual assistance

Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations and as necessary to carry out the obligations of Articles 27 –35. These include provisions which ensure mutual assistance in the absence of any mutual assistance treaties (27 and 28) as well as those regarding specific provisions for mutual assistance including: the ability for a party to request another to expeditiously preserve computer data (29) and traffic data (30) as well as collect traffic data (33) and content (34) in real time and access the preserved computer data (31) expeditiously; ensuring trans-border access to stored computer data which is publicly available (32), and; the designation of a point of contact available on a 24 hour, seven day a week basis to ensure immediate assistance.

Article 26 Spontaneous Information

A party may forward to another party information obtained in its own investigations when it considers the disclosure might assist the receiving party.

* * *

The fourth part of the Convention contains, with some exceptions, provisions based on the 'Model final clauses for conventions and agreements concluded within the Council of Europe' which were approved by the Committee of Ministers at the 315th meeting of the Deputies in February 1980.

Commentary

Brian Krebs, "Council Of Europe Adopts Global Cyber-Crime Treaty", http://www.newsbytes.com/news/01/172012.html

"The multi-country treaty has steadily come under fire from several consumer and civil liberties groups concerned that the convention could lead to the emergence of an international electronic surveillance network, or a kind of "global Big Brother…
In addition, First Amendment groups worry about the implications of a supplemental protocol that will soon be added to the agreement that makes any Internet publication of racist or xenophobic material a criminal offense."

Jane Rawlings, "The Council of Europe Draft Convention on Cyber-crime: A European perspective on a global problem", *Computers and Law*, Sept. 2001

"The privacy and human rights measures that should protect the citizens of a party against the overzealous or wrongful exercise of investigative powers have been left to safeguards in a Party's national law (Article 15). … These may be more or less effective, depending on:
(i) whether or not the Party concerned has acceded to instruments such as the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms or the 1966 United Nations International Covenant on Civil and Political Rights and;
(ii) the extent to which these have been implemented into that Party's national law."

"The Cyber-Crime Convention contains no requirement that a party should put in place measures to compensate service providers … who may be the targets of the exercise of the … powers."

This paper was prepared by Oz NetLaw: the Internet Law Practice of the Communications Law Centre. The Communications Law Centre is based at UNSW and Victoria University.
Oz NetLaw is sponsored by Clayton Utz and Gilbert and Tobin.
Contributors included Isabella Alexander, Derek Wilding, Victoria Marles, Lillian Kline, Anthony Hoo, Drew Macrae, Judy Kim, Farhan Quettawala, Robert McMahon.