JICLT
Journal of International Commercial Law and Technology
Vol. 7, Issue 4(2012)



# Could A Small Town in Romania bring Australia to its Cyber-knees? Not if They Accede to the EU Convention on Cybercrime

**Dr. Angela Adrian**
Senior Lecturer, School of Law & Justice
Southern Cross University
New South Wales, Australia
Angela.adrian@scu.edu.au

**Abstract.** *On 30 April 2010, Attorney-General, Robert McClelland, and Minister for Foreign Affairs, Stephen Smith, announced Australia's intention to accede to the Council of Europe Convention on Cybercrime. (Media Release, 2010) The Convention is the only binding international treaty on cybercrime. It serves as both a guide for nations developing comprehensive national legislation on cybercrime and as a framework for international co-operation between signatory countries. Cybercrime poses a significant challenge for our law enforcement and criminal justice system. The Internet makes it easy for criminals to operate from abroad, especially from those countries where regulations and enforcement arrangements are weak. It is critical that laws designed to combat cybercrime are harmonised, or at least compatible to allow for cooperation internationally. This paper explores what could happen if Hackerville set its sights on Australia.*





## 1. Introduction

The small town of Râmnicu Vâlcea, three hours outside of Bucharest, is known among law enforcement officials around the world as Hackerville. This is somewhat misleading. The town is full of online crooks, but only a small percentage of them are actual hackers. Most specialize in ecommerce scams and malware attacks on businesses. According to authorities, these schemes have brought tens of millions of dollars into the area over the past decade, fuelling the development of new apartment buildings, nightclubs, and shopping centres. Râmnicu Vâlcea is a town whose business is cybercrime, and business is booming. (Bhattacharjee, 2011)

Once upon a time, some Romanian individuals decided to make some money in the world of ecommerce. They developed a product they called Worryware. Worryware was malicious software that pretended to be legitimate computer security software and claimed to detect a variety of threats that did not actually exist. The user of the affected computer was then told that they must purchase the company's anti-virus software in order to repair their computers. Next, the users are hassled with aggressive and disruptive notifications until they supply their credit card number and pay for the worthless "anti-virus" product. The product is, in fact, fake. When their operation had caused more than $74 million in total losses to more than one million computer users the AFP (Australia Federal Police) and the ASIO (Australian Security Intelligence Organization) stepped in to stop them. (story based upon a true FBI investigation).

JICLT
Journal of International Commercial Law and Technology
Vol. 7, Issue 4(2012)

Criminals and terrorists have spotted that the internet is full of possibilities; and needless to say, have exploited it. Criminals make child pornography cheaply and easily on their computers, and then distribute it via internet networks to unknown and unknowable paedophiles. Hackers break into bank computers, transfer funds to their own accounts, and extort the banks. Drug dealers and terrorists use encrypted electronic communications to evade government surveillance. Although there have been improvements to critical infrastructures, computerization has a dark side: insecure information networks make infrastructures vulnerable to the attacks of hackers and "malicious code" such as viruses and worms. These threats are not limited to the direct harms of the crimes themselves. All of the benefits of information networks are at risk if the networks are not safe and secure. If users become unwilling to send their personal and credit card information over the Internet, e-commerce will not flourish. Similarly, citizens will not file their tax returns, bid on government contracts, or use other e-government services if they are afraid to use the networks. (Downing, 2005) Moreover, if a particular country gets a reputation as a haven for Internet crime, consumers and businesses will refrain from interacting with it.

During the 10th anniversary of the Budapest Convention against Cybercrime, Cecilia Malmström (Member of the European Commission responsible for Home Affairs) spoke of the need for Europe to "take stock of the new challenges, as the threat is very much a real one." (Carstensen, 2011) Most of us live in cyberspace and use the international highways of the internet for our daily commutes to business and pleasure. The threats are always nearby. Cecilia Malmström went on to tell us that "the number of cyber attacks in the world is on the rise, and the cost of cybercrime is skyrocketing." International Cybercrime markets are rumoured to be worth anywhere from US $500billion to US $1trillion per annum. (Id.) In Australia, a Computer Crime and Security Survey, run in conjunction with the Australian Federal Police, Queensland Police, Western Australia Police and South Australia Police highlighted the extent of electronic crimes. This survey found that: (1) total losses for organisations surveyed were estimated at $12 million, more than double the losses for 2002; (2) 42 per cent of organisations experienced one or more computer attacks which harmed network data or systems; (3) financial fraud, laptop theft and virus, worm and trojan infections were the largest source of losses. (Levinson & Ceola, 2003) As the Romanians have discovered, this is a lucrative business.

Ironically, Romania implemented the Cybercrime Convention with law nr. 64 on 24 March 2004. The law was published in the Official Monitor nr. 343, on 20 April 2004. The main provisions of the Cybercrime Convention were already incorporated in Title III of the Anti-corruption Law nr. 161/2003, published in the Official Monitor nr. 279 from 21 April 2003. On the other hand, Australia is still in the process of ratifying and implementing the Convention through the Cybercrime Legislation Amendment Bill 2011. This paper looks at how the above scenario would have played out if the players had truly been Romanians and Australians. The paper will conclude suggesting how Australia can join the ranks of the world's cybercrime fighters.



## 2. EU Convention on Cybercrime & Australia: Substantive

The EU Convention on Cybercrime (hereinafter, 'Convention') began as an agreement between member nations of the European Union, although only ten of the twenty seven countries have yet to ratify it. Regardless, it is the only international agreement in the area of cybercrime. Likewise, it is unique in that it is open for signature by non-European member states. The United States, Canada and Japan have all signed the Convention, with the United States also ratifying it.

The Convention is arranged into three key divisions: substantive law, procedural requirements and international cooperation. Certain activities must be criminalised by all signatories. These substanative offenses can be placed into four main categories:

- offences against the confidentiality, integrity and availability of computer data and systems, comprising interference and misuse of devices (Articles 2 – 6);
- computer-related offences such as forgery and computer fraud (Articles 7 – 8);
- content-related offences, in particular the production, dissemination and possession of child pornography (Article 9); and

- offences related to infringement of copyright (Article 10).

Australia is mostly compliant with the Convention's obligations, including the requisite cybercrime offences, the majority of police powers such as interception and access to stored communications and data and most elements of international cooperation. The Cybercrime Legislation Amendment Bill (2011) makes the following amendments to existing powers which ensure full compliance with the Convention's obligations:

- requires carriers and carriage service providers (C/CSPs) to preserve the stored communications and telecommunications data for specific persons when requested by certain domestic agencies or when requested by Australian Federal Police on behalf of certain foreign countries;
- ensures Australian agencies are able to obtain and disclose telecommunications data and stored communications for the purposes of a foreign investigation;
- provides for the extraterritorial operation of certain offences in the Telecommunications (Interception and Access Act 1979;
- amends the computer crime offences in the Criminal Code Act 1995 so that they have adequate scope; and
- creates confidentiality requirements in relation to authorisations to disclose telecommunications data.

The Convention requires signatory nations to sign a number of copyright treaties including The Berne Convention for the Protection of Literary and Artistic Works, 828 UNTS 222 (entered into force 29 January 1970); Paris Act relating to the Berne Convention for the Protection of Literary and Artistic Works, 1161 UNTS 30 (entered into force 15 December 1972); Marrakesh Agreement Establishing the World Trade Organization, 1867 UNTS 3 (entered into force 1 January 1995), annex 1C Agreement on Trade-Related Aspects of Intellectual Property Rights; World Intellectual Property Organization Copyright Treaty, 2186 UNTS 121 (entered into force 6 March 2002). Further, Article 10 of the Convention demands the criminalisation of certain copyright acts. Australia has signed and ratified all of these instruments, and has criminalised many forms of copyright infringement.

In the case of Worryware, the cyber criminals would be clearly breaching the first two areas of the Convention. Specifically the following areas of Chapter II – Measures to be taken at the national level, Section 1 – Substantive criminal law, Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems:

- Article 2 – Illegal Access:By pretending to be legitimate computer security which detected threats, but instead installing said threats through aggressive demands for payment. Not only did this provide illegal access to the victims' computer, but also to their credit card information.
- Article 3 – Illegal Interception: With dishonest intent, the cyber criminals infected the victims' computers and were then able to intercept any transmission from those computers.
- Article 4 – Data Interference: Due to the above offences, the cyber criminals intentionally damaged, deleted, caused deterioration, and altered or suppressed victims' computer data.
- Article 5 – System Interference: Again, due to the above, the cyber criminals have intentionally hindered the functioning of computer systems by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.
- Article 6 – Misuse of Devices: The cyber criminals produced, sold, procured for use and distributed computer programs designed to commit the above offences along with making available computer passwords, access codes, or similar data by which the computer is capable of being accessed with the intent of committing the above offences.
- Article 7 – Computer-related Forgery: This offence was committed when the cyber criminals intentionally and without right, altered, deleted and/or suppressed computer data which resulted in inauthentic data which was to be considered or acted upon as if it were authentic. The intent was to defraud or had a similar dishonest intent.

JICLT
Journal of International Commercial Law and Technology
Vol. 7, Issue 4(2012)

- Article 8 – Computer-related Fraud: The cyber criminals intended to cause the loss of property by others by (a) inputting, altering, deleting, or suppressing computer data, and (b) interfering with the functioning of a computer system with fraudulent and dishonest intention an economic benefit.

The Romanian cyber criminals, in this particular, scenario did not violate the second two areas of the Convention relating to child pornography or intellectual property infringement.

## 3. EU Convention on Cybercrime & Australia: Procedure

The Convention deals with the procedural aspects of cybercrime as well in the following categories:

1. expedited preservation of stored computer data (Articles 16 & 29);
2. expedited preservation and partial disclosure of traffic data (Article 17 & 30);
3. production orders (Article 18);
4. search and seizure of stored computer data (Article 19);
5. real-time collection of traffic data (Article 20); and
6. Interception of content data (Article 21).

The Convention requires procedural changes to law enforcement and drafts ISPs into the law enforcement process. As such, ISPs must implement technical means to aid law enforcement to monitor network traffic. For example, ISPs are required to have facilities that allow for interception of communication. They must have greater search and seizure powers which can be implemented in real-time.

### *3.1 Preservation*

Schedule 1, Telecommunications (Interception and Access) Act 1979, implements the requirements of the Convention. Article 16 requires Parties to establish powers enabling domestic agencies to obtain the preservation of stored computer data (stored communications, including traffic data) for up to 90 days, particularly where there are grounds to believe that the data is particularly vulnerable to loss or modification. The purpose of the 90 day preservation period is to maintain the integrity of that computer data for a period of time as long as necessary to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. Further, Article 16 requires that each party adopt such measures as necessary to oblige the person who is preserving the data to keep confidential the undertaking of such procedures.

Article 29 requires Parties to establish powers enabling a domestic agency to be able to obtain the preservation of stored computer data (including traffic data) at the request of other parties to the Convention. The Convention specifies necessary components of an international preservation request, including that the party seeking preservation must intend to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

Schedule 1 implement these requirements by establishing two classes of domestic preservation notices which allow for domestic agencies to preserve certain stored communications that a carrier holds until the communications can be accessed under a warrant. This prevents the communications from being destroyed before a warrant is obtained. Under this system, certain agencies can give a preservation notice to a carrier requiring the carrier to preserve all stored communications that the carrier holds that relate to the person or telecommunications service specified in the notice. The carrier will breach its obligations under section 313 of the Telecommunications Act 1997 if it does not comply with the notice.

There are three types of preservation notices:

- historic domestic preservation notices (which preserve communications held by the carrier on the day the notice is received that might assist the Organisation in carrying out its function of obtaining intelligence relating to security or a contravention of certain Australian laws for up to 90 days)
- ongoing domestic preservation notices (which preserve communications held by the carrier during a 29 day period after the notice is received that might assist the Organisation in carrying out its function of obtaining intelligence relating to security or a contravention of certain Australian laws for up to 90 days), and
- foreign preservation notices (which cover stored communications held by the carrier on the day the notice is received that might relate to a contravention of certain foreign laws).

### *3.2 Search & Seizure*

The Convention gives law enforcement extensive powers of search and seizure of data and computers in the investigation of cybercrime. These powers do not differ from the current powers of law enforcement to search and seize computers for evidence. The search and seizure provisions are fundamentally analogous to those of data preservation. Measures must be taken to preserve data and evidence quickly due to its volatility of digital evidence. Search and seizure of a computer system or stored device where data may be found involves the right to make a copy of the data, maintain the integrity of the data, and render the data inaccessible to other parties. The Convention aims to encourage, if not guarantee, that domestic law enforcement officers will cooperate with foreign law enforcement officers in requests for the search and seize of a computer for an investigation abroad.

Some commentators are concerned that the Convention will establish an Orwellian system of electronic surveillance because both the Convention and Australian law are silent as to the length of time law enforcement officers may retain a seized computer (system) without bringing charges. (Esposito, 2004; Young, 2004) Such fears are unfounded as the procedural provisions of the Convention only apply to active criminal investigations.

### *3.3 Real-Time Evidence Collection and Interception Capabilities*

Protection of civil liberties (privacy) and human rights are safeguarded under Article 15 of the Convention which directs signatories to prior obligations undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments. Further, real-time evidence collection and interception of communications are subject to the domestic law of each party. So for instance, the Convention does not oblige ISPs to monitor all network traffic and preserve data logs of all of their customers for 90 days in the event that the data might be needed for future investigations. Additionally in Australia, interception of communications must be done under a valid warrant.

Real-time forensics operates in two ways: general evidence collection without a suspect in mind, or specific evidence collection with a particular suspect in mind. Under the general collection of real-time evidence, when a crime is committed, a warrant may be issued allowing law enforcement agents to access ISP data logs (if any) stored at the time of the crime. ISPs routinely monitor their networks using medium packet inspection technologies such as NetFlow. NetFlow is used to check performance and to provide base data for billing and charging records, but does not maintain data logs for long before deleting it, nor does it usually monitor the data with the intention of identifying particular malicious individuals. As such, the value of evidence collected post-crime is dependent on the type of monitoring and detection technologies used by the ISP.

When there is a suspect in mind, a law enforcement officer may apply for a content warrant, which allows the communications of the suspect to be intercepted. Depending on the type of warrant, this could include website contents and email box contents (stored communications warrant), or information about IP traffic to and

from a target IP address/address range or VOIP traffic to and from a phone number. See Part 2-5 Telecommunications Interception Warrant under the *Telecommunications (Interception and Access) Act 1979* (Cth) ('*TIAA*'). Without real-time evidence, there is heavy reliance on the random access memory, or 'RAM', of a computer where information is neither stored centrally nor statically. As such, the probability of finding physical memory after the fact is slight. Real-time data collection allows entire contents of an email box to be captured, whether the information is local or remote. (Reyes, 2007) Where real-time data is stored, law enforcement agents are potentially able to peer at the email box pre-crime, post-crime and during the commission of a crime. The capturing and storing of real-time data requires the assistance of ISPs who are the middlemen or information conduits. (Id.) Law enforcement agents are now able to compel ISPs to intercept communications between parties. (TIAA ss 190 & 191)

### *3.4 Catching Hacker-villains with Convention Tools*

In order to catch the hackers of our story, the AFP and the ASIO will need to ensure that the stored computer data involved in this scam has been preserved in an expedited fashion. (Article 16 & 29) Further, that any disclosure of traffic data is also preserved in an expedited manner. (Article 17 & 30) This data will need to be captured not only in Australia, but wherever else the traffic has flowed. As such, Article 16 has its corresponding Article in 30 under Title 4, Section 2 Specific Provisions, Title 1 – Mutual assistance regarding provisional measures. Under Article 18, production orders will need to be acquired in order to empower the competent authorities to order ISPs to provide subscriber information along with any computer data related to them. Next, search and seizure measures need to be implemented according to Article 19. Again, with regard to international mutual assistance see Articles 31 & 32. As seen above, the Convention allows for real-time collection of computer data as well as the interception of content data. (Articles 20 and 21) Moreover, these provisions are found in regard to mutual assistance. (Articles 33 & 34)

## 4. EU Convention on Cybercrime & Australia: Jurisdiction

No matter how much effort the AFP and ASIO make, if they do not have the cooperation of the state where the cyber villains do business, they will not be able to catch them. So finally, the Convention addresses the issues relating to international cooperation. These may broadly be categorised as:

1. extradition (Article 24);
2. mutual assistance (Articles 25 - 34); and
3. a 24/7 network contact (Article 35).

The Convention signatories must cooperate with investigations with other signatories. The fundamental purpose of the Convention is found in Article 23. The parties shall ensure cooperation 'to the widest extent possible.' Each category shall be examined below.

### *4.1 Extradition*

The Convention uses existing provisions in extradition treaties, rather than superseding them. (Art. 24 (2)) Thus, Articles 2–11 are considered extraditable offences under existing treaties. And as such, are subject to the conditions laid out in the existing extradition treaties. For instance, jurisdiction A deems illegal access to a computer to be punishable by death. Jurisdiction B considers the death penalty to be cruel and unusual punishment. Further, jurisdiction B maintains this position in any extradition treaties to which it accedes. The Convention would not compel jurisdiction B to extradite its citizen to jurisdiction A. Broadhurst (2006) noted that most extradition treaties were agreed before cybercrime became such an issue, which renders them somewhat out of date. However, re-negotiating every bilateral extradition treaty to incorporate cybercrime

elements would be an arduous and onerous task, and highly unlikely one. (Id.) Fortunately, the Convention permits the incorporation of cybercrimes into existing extradition treaties.

Article 24(3) provides signatories the option to make extradition contingent on an existing extradition treaty. If no extradition treaty exists, signatories have no obligation to extradite offenders. This can occur where there are differences in philosophies regarding democracy or human rights. Nonetheless, there are persuasive reasons why nations may want to cooperate with the extradition of offenders of the crimes specified in the Convention. These would include deplorable crimes such as child pornography, large scale fraud, and cyber-terrorism. Cyber-terrorism would include attacks to critical infrastructure; i.e., military defence systems, electrical grids, banking systems and hospital databases. On the other hand, extradition could be considered extreme in the case of small scale copyright infringement. Article 10(3) provides that "A party may reserve the right not to impose criminal liability under paras. (1) and (2) in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to above." Moreover, the Convention accounts for lesser crimes by making extradition contingent on the offence being punishable under the laws of both parties as well as only in situations where there is 'deprivation of liberty for a maximum period of at least one year.' This flexibility lets parties fulfil their obligations to the Convention without compromising their existing domestic safeguards against extradition for unjust or insufficiently serious matters.

### *4.2 Mutual Assistance*

Article 25(1) requires parties to afford one another mutual assistance to the widest possible extent. Article 25(5) allows a party to make this mutual assistance conditional upon the existence of dual criminality. "Dual criminality requires that an accused be extradited only if the alleged criminal conduct is considered criminal under the laws of both the surrendering and requesting nations." (*US v. Saccoccia*, 18 F. 3d 795 (1994)) The dual criminality requirement ensures that a country only extradites a person on the basis of conduct it considers to be criminal. Lack of dual criminality is a mandatory ground of refusal in the current Australian extradition process. Unless dual criminality is satisfied, Australia cannot extradite a person. (Attorney-General Australia, 2006)

Thus, the dual criminality requirement continues to be important. Not for the purpose of isolating nation states and not because criminal law should be associated with one fixed cultural environment; rather, the requirement is significant as it helps to put into practice the rule-of-law concept that each legal system must have for its criminal offenses. The rapprochement of the states and the corresponding approximation of their common efforts to carry out law enforcement trans-nationally demands substantive scrutiny of existing differences among the various systems of criminal law. The dual criminality requirement requires this examination, and in doing so, fosters better harmonization. (Capos, 2009) By making dual criminality a discretionary ground of refusal, Australia would have a more flexible approach to extradition and allow for extradition of a wider range of offences. As a safeguard, the Minister could retain the discretion to refuse extradition on the basis of dual criminality on a case by case basis where there are concerns about the nature of the offence for which the requesting country seeks extradition. (Attorney-General Australia, 2006)

"The primary focus of dual criminality has always been on the conduct charged; the elements of the analogous offenses need not be identical. All the principle of *dual criminality* requires is that the particular acts alleged constitute a crime in both jurisdictions. To satisfy the dual criminality requirement, it is enough that the conduct involved is criminal in both countries." (*Man-Soek Choe v Torres*, 525 F. 3d 733 (2009)) Article 25(3) continues by conditioning dual criminality in similar terms. Dual criminality shall be deemed to be fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

In a cybercrime investigation, time is a critical factor. Digital evidence is changeable. Investigators must collect evidence promptly in order to have sufficient proof to convict. Often they have not figured out the full

extent of crimes committed at the time of a preservation of data request. Dual criminality is then determined once the evidence has been obtained. Thus mutual assistance needs to extend beyond mere preservation of data. As the particularly useful portion of data preservation consists in identifying the points of connectivity. Criminals tend to disguise their IP address through proxy connections. By providing a partial look at data traffic, a snapshot of routing connections could be determined.

### *4.3 Designation of a 24/7 Network Contact*

Article 35 of the Convention creates a network of national points of contact in order to better coordinate criminal investigations and requests for information. The network personnel are required to be properly trained and equipped. They are to operate on a 24-hour, seven-days-a-week basis allowing for immediate assistance. This differs from the traditional channels of cooperation (i.e., Interpol) as it is used to facilitate or directly carry out procedural tasks under the Convention; for example, to preserve data expeditiously or to intercept communications. On the other hand, Interpol is tasked with active criminal investigations involving trans-national crimes. The international cooperation provisions of extradition and mutual assistance are performed by a separate authority, and not by the network. The network contact merely facilitates extradition and mutual assistance requests to the relevant authority pursuant to Article 35(2)(b). Broadhurst (2006) states that '[t]he establishment of this network is one of the most important provided by the Convention.'

## 5. What do Australians have to lose? Privacy.

Australia, a country planning to enact laws governing law enforcement access to electronic evidence, must consider the importance of privacy. Privacy is critical to the functioning of a democratic society and a healthy economy. Into the bargain, competitive markets and economic development also rely on privacy. Businesses cannot compete successfully without the ability to discuss and make decisions in private. Likewise, privacy is critical to the governmental deliberative process. Having every decision made in the public spotlight cripples the ability of government officials to carefully consider problems and develop appropriate solutions through discussion and debate. (Downing, 2005)

Protecting privacy and law enforcement authority are not diametrically opposed. A reduction in one does not necessarily cause a commensurate increase in the other. However, there is no easy way to balance these competing concerns. Australia must make choices about this issue, taking into consideration the scope of their crime and terrorism problems, existing legal structures, and the methods historically used to protect human rights. Moreover, these decisions must also take into account the need to assist other countries in their fight against crime, terrorism, and privacy invasions. (Id.) This internationalisation of information flows has justified claims of extraterritoriality premised on domestic effect. Much online privacy policy today is influenced heavily by extraterritorial European Union regulation. This regulation has, in turn, influenced the EU Cybercrime Convention.

Privacy regulation is characterised by strong differences of opinions between countries. Much information regulation, like copyright, exists in a rough consensus among economically powerful nations. But privacy tends to touch closer to the nation's psyche and culture causing countries to disagree as to what they consider adequate protection of privacy. Europeans, for example, care more about the sanctity of private information than anyone else in the world. (Wu, 2008) They want greater policing of the abuses of the private sector. On the other hand, Americans see privacy as a negative freedom, which is principally a protection from government. They are wary of government restraints on commerce in the name of privacy regulation. Finally, scholars of Chinese culture looking for the meaning of privacy in a Chinese context claim that the Western conception of privacy lacks meaning in the East. (McDougall, 2002) What does this mean for Australians? First, any normative view of privacy must take into account the fact that much privacy policy that affects Australians will be set overseas. Second, those Australians who want more government privacy protection should focus their efforts on convincing significant economic units (i.e., the EU, USA, and China) to enact strong extraterritorial privacy legislation.

In considering how to balance concerns in the procedures for law enforcement, lawmakers should consider the following rule of thumb: the more intrusive into individual privacy a particular authority is, the greater the need for safeguards to ensure that the authority is not abused. (Downing, 2005) Thus, for instance, the legal protections associated with the authority to obtain the content of a communication generally exceed those associated with the authority to obtain non-content traffic data related to that same communication. Similarly, legal systems often provide greater limitations on the authority to intercept a message passing over a computer network than on the authority to access the content of a file that an individual has chosen to store somewhere on a computer network. (see generally, Telecommunications (Interception) Act 1979, 45-46) Lawmakers should decide how intrusive a particular authority is in the context of their society's privacy expectations.

In order to offset some of the concerns raised by privacy advocates in Australia, a Cybercrime Code of Practice for ISPs has been developed. Australian lawmakers have determined that improving the safety and security of the internet depends on early detection of criminal activity. The Code attempts to balance differing concerns between the law enforcement agencies' need to identify, investigate and prosecute offences and the privacy of end users and costs to the industry in complying with the Code. "The objectives of the Code are to: (1) facilitate cooperation between ISPs and law enforcement agencies and establish clear policies and procedures for investigations; (2) provide a transparent mechanism for the handling of law enforcement agencies' investigations for the Internet industry and ensure both ISPs and law enforcement agencies understand the procedures; (3) promote positive relationships between law enforcement agencies and the Internet industry; and (4) ensure that the privacy of users of the Internet will be protected from unlawful intrusion by law enforcement agencies." (Levinson & Ceola, 2003)

Further, "the Code stipulates that customer information collected by ISPs, must be retained for six or 12 months, depending on the type of information. Personal information such as a customer's name, username, email address, phone number, credit card details and address details, must be retained for the greater of six months from the date a customer ceases to be a customer or 12 months after the creation of the record. Operational data, such as dynamic IP allocations records, dates and time of log-ins and the total data transferred, must be retained for six months from the date of creation. ISPs, however, are not required to capture subscribers' phone numbers via caller line identification." (Industry Code for Internet Privacy, 2003)

The Code was delayed in its release due to privacy concerns. However, after consultation with the Privacy Commissioner it was determined that some ISPs might not be bound by the National Privacy Principles which were introduced on 21 December 2001 under the Privacy Act 1988 (Cth) (Privacy Act). As a consequence, the Code requires all ISPs wishing to be a party to the Code to be bound by the Privacy Act, if necessary by voluntarily but formally agreeing to be bound. This means the Privacy Commissioner can exercise his power against ISPs bound by the Code who breach the National Privacy Principles. The Code also reminds ISPs that if they disclose customer information to anyone other than law enforcement agencies, they are at risk of breaching the Telecommunications Act 1997 (Cth) and exposing themselves to the possibility of criminal penalties and up to two years imprisonment. (Levinson & Ceola, 2003)



## 6. Can the Convention beat the Hackers?

Although the Convention has not lived up to the expectations that it raised, it has become a well regarded starting point in combating transnational cybercrime. The procedural tools have been under-utilised to date; but as more nations accede to the Convention, this may change. As was seen earlier in this article, countries like Romania have ratified the Convention and still are hotbeds of cybercrime activity. (Bhattacharjee, 2011) However, Romania has received few international requests under the Convention. (Carstensen, 2011) The substantive provisions in the Convention are similar to Australian law. A few tweaks have been made in the Cybercrime Legislation Amendment Bill 2011 to accommodate any variations. As for procedural provisions, the Convention does not change Australian law. Warrants will still be required. Australian ISPs already have interception and real-time evidence collection capabilities. Preservation of data, production orders and search and seizure of computer systems are already required for the purpose of criminal investigations. The provisions

compel law enforcement and ISPs to fulfil similar duties as they would if a local criminal investigation. This has merely been extended to those law enforcement agents abroad who are party to the Convention.

Further, extradition is only allowed where an extradition treaty between the two parties already exists. Australia would not be forced to extradite offenders to a country where no extradition treaty exists. Dual criminality may also be specified as a condition to extradition. Where a party to the Convention specifies dual criminality as a precondition to mutual assistance, they are able to do so in application to all procedural requirements other than expeditious preservation of data. Accession to the Convention allows Australian law authorities the ability to better investigate criminal offences where the criminal or part of the crime is located in a foreign jurisdiction which is party to the Convention. Although the Convention's mutual assistance provisions are highly diluted in countries like Romania, sufficient resources should be allocated to law enforcement to enable investigation. More requests for mutual assistance need to be made and enforced. Unfortunately, international cybercrime and e-commerce fraud are under-enforced. Priority invariably goes to local crimes with local victims. The Convention does not change this.

With the formation of a European *Computer Emergency Response Team* (CERT) by the end of May 2011 and the call for co-operation between the United States and the EU on Cybercrime, Europol and Interpol may find a lightened load in supporting member states. *ENISA* (European Network and Information Security Agency) has also been coordinating and assisting the local CERT teams within the member nations. Cybercrime needs to be addressed through changes to protocol, education and training of end-users and businesses. A broad commitment to engage the private sector needs to be made in sharing good practices on collaboration with industry, and pursuing specific engagement on key issue areas such as fighting malware, securing industrial control systems (such as water treatment and power generation), and enhancing the resilience and stability of the internet. Governments must be called upon to regulate internet governance structures such as DNS registrars and to impose codes of conduct for ISPs where the industry has not performed satisfactorily in helping to better protect users from cybercrime while maintaining users' privacy. Australia is in a prime position to become a real cybercrime fighting nation. They must roll up their sleeve and ensure that cybercrime detection, prevention, and reduction happen sooner, rather than later.



## Reference

Australia Attorney General (2006) A new extradition system – a review of Australia's extradition law and practice available at http://www.ema.gov.au/extradition2006/extradition.html#australiarequire

Yudhijit Bhattacharjee, (February 2011) Why Does a Remote Town in Romania Have So Many Cyber criminals? Wired 19.02 available at http://www.wired.com/magazine/2011/01/ff_hackerville_romania.html

Roderic Broadhurst (2006) Developments in the Global Law Enforcement of Cyber-Crime, 29(3) Policing: An International Journal of Police Strategies and Management 408, 418

Nadja Capus (2009) Sovereignty and Criminal Law: The Dual Criminality Requirement in International Mutual Legal Assistance in Criminal Matters Max Plank Institute Research Project available at http://www.mpicc.de/ww/en/pub/forschung/forschungsarbeit/strafrecht/rechtshilfe.htm

Jared Carstensen (20 April 2011) European Cybercrime 10 Years On - Why It's Not Working available at http://www.infosecisland.com/blogview/13139-European-Cybercrime-10-Years-On-Why-Its-Not-Working.html

Council of Europe (2001) Convention on Cybercrime Budapest, 23.XI.2001

Richard W. Downing (2005) Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime, 43 Colum. J. Transnat'l L. 705

Gianluca Esposito (2004) 'The Council of Europe Convention on Cyber-Crime: A Revolutionary Instrument?' in Roderic Broadhurst (ed) Proceedings of the 2nd Asia Cyber-Crime Summit (Hong Kong: Centre for Criminology, the University of Hong Kong)

Industry Code of Practice for Internet Privacy (2003) A full copy of the draft Code is available from http://iia.net.au/

International Covenant on Civil and Political Rights, opened for signature 16 December 1966, 999 UNTS 302 (entered into force 23 March 1967)

Joint Media Release, Attorney-General, Hon. Robert McClelland MP & Minister for Foreign Affairs, Hon. Stephen Smith MP (30 April 2010) Australia to Accede to International Cybercrime Convention, available at http://www.ema.gov.au/www/ministers/mcclelland.nsf/Page/MediaReleases_2010_SecondQuarter_30April2010-AustraliatoAccedetoInternationalCybercrimeConvention

Elizabeth Levinson & Natalie Ceola (2003) Cybercrime Code of Practice for ISPs available at www.iia.net.au/cybercrimevt.html

Bonnie McDougall (2002) Love-Letters and Privacy in Modern China (Hong Kong: Random House)

Press Release, Office of Public Affairs, Department of Justice (22 June 2011) Department of Justice Disrupts International Cyber Crime Rings Distributing Scareware available at Department of Justice Disrupts International Cyber Crime Rings at http://www.fbi.gov/news/pressrel/press-releases/department-of-justice-disrupts-international-cybercrime-rings-distributing-scareware

Anthony Reyes, et al (2007) Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors. Syngress Publishing: Waltham, MA

Tim Wu (2008) The International Privacy Regime in "Securing Privacy in the Internet Age" ed. Anupam Chander, Lauren Gelman, and Margaret Jane Radin (Stanford, CA: Stanford University Press)

Jason Young (2004) Surfing While Muslim: Privacy, Freedom of Expression and the Unintended Consequences of Cybercrime Legislation, International Journal of Communications Law and Policy 9

* * * *


Cite as: Adrian, Angela, Could A Small Town in Romania bring Australia to its Cyber-knees? Not if They Accede to the EU Convention on Cybercrime., *Journal of International Commercial Law and Technology*, Vol.7 Issue 3 (October, 2012)