



Cyberspace Law and Policy Centre
A Centre for the Public Interest in Networked Transactions

Inquiry into Cybercrime

Submission to the Standing Committee on Communications on the inquiry into
cybercrime and its impact on Australian consumers

Alana Maurushat

Lecturer and PhD Candidate, UNSW Faculty of Law

Deputy Director

Cyberspace Law & Policy Centre, UNSW Faculty of Law

September 15, 2009

1.0 Introduction

Thank you for the invitation to make a submission on the inquiry into cyber crime and its impact on Australian consumers.

This submission is made by researchers at the Cyberspace Law & Policy Centre (CPLC) <<http://www.cyberlawcentre.org/>>, University of New South Wales Faculty of Law. CPLC is a public interest centre focused on representing the user's perspective in public policy. Alana Maurushat, the Centre's Deputy Director, is finishing a PhD in the area of Internet Security and Cybercrime. A portion of this submission is taken from her graduate research, "**The Malware Matrix: Combating the Commercial Malware Industry Through Security Policy**". The Centre is indebted to student research interns Shannon Kalish for her work on the submission, and to Pauline Rapaport and David Vaile for their comments.

This is a supplemental submission at the invited request of Jane Hearn dealing with two additional points: 1) "whether Australia would benefit from being part of the Council of Europe Convention on Cybercrime" and 2) identification of gaps in the law which made prosecution difficult.

1.0 Council of Europe Convention on Cybercrime

Due to time restrictions, I have outlined a number of points relevant to the benefits and detriments of signing and ratifying the Cybercrime Convention. They are below:

1.1 All Signatories to the Convention Must Criminalise Certain Activities

- Australian law enforcement agencies are already very cooperative both domestically and internationally in aiding cybercrime investigations.

- Australia's decision to sign the Cybercrime Convention, therefore, has no bearing on motivating our law enforcement agencies to cooperate with overseas law enforcement.
- The Cybercrime Convention creates four main categories of offences:
 - 1) offences against the confidentiality, integrity and availability of computer data and systems, comprising interference and misuse of devices,
 - 2) computer-related offences such as forgery and computer fraud,
 - 3) content-related offences, in particular the production, dissemination and possession of child pornography, and
 - 4) offences related to infringement of copyright.
- *Australia already criminalises the above four categories of conduct. From a substantive perspective, Australia is compliant with the Convention.*
 - Eg. Australian authorities have aggressively pursued offences related to **child pornography** in both coordinated national efforts, and through international stings with their involvement with Interpol. Australia criminalises access, distribution, and possession of child pornography along the same lines as the Cybercrime Convention.
 - Eg. The Convention mandates signatory nations to also sign a number of **copyright** treaties including *The Berne Convention for the Protection of Literary and Artistic Works*, the *Paris Act, Trade-Related Aspects of Intellectual Property Rights (TRIPS)*, and the *World International Property Organisation (WIPO) Copyright Treaties*. The Convention mandates the criminalisation of certain copyright acts. Australia has signed and ratified all of these instruments, and has criminalised many forms of copyright infringement.
 - Eg. All jurisdictions within Australia have incorporated legislation dealing with **unauthorised data** misuse and abuse
 - Eg. Likewise, **forgery and fraud** remain offenses
- The Convention mandates that nations signatory to the Convention create specific laws punishing specific cybercrimes. The approach by many nations including the United States and Australia has been to use the existing substantive criminal laws for traditional offline crimes, for online crimes. Squeezing condemnable online conduct into existing criminal provisions often leads to unsuccessful prosecution. This is explored in **2.0 Loopholes in the Australian System**.

1.2 ISPs Must Implement Technical Means to Aid Law Enforcement to Monitor Network Traffic

- The Convention shifts the role of ISPs from dis-intermediary to intermediary in law enforcement.

- The Convention requires ISPs to have facilities that allow for interception of communication in real-time.
- Domestic law enforcement agencies are given search and seizure abilities.
- The infrastructure and technical capacity for most Australian ISPs to perform the above relevant functions is already there. Criticism of the Australian infrastructure on the above points was more relevant in the late 1990s and early 2000s, at the time of drafting the Convention. Most ISPs in western nations, after the terrorist attacks of 9/11, have these capabilities.
- It is important to note that the Convention does not mandate the controversial technology of Deep Packet Inspection by ISPs (now being considered in the United Kingdom). Should Australia decide to head in this direction there would likely need to be a separate inquiry due to the pervasiveness of this technology.
- The Convention requires ISPs to *expeditiously* preserve data logs for ninety days. This remains a controversial point but most notably in its operation with the obligation to provide mutual assistance . This is further considered Section c) below.
- The nature of many cybercrimes, unlike other traditional off-line crimes, requires that evidence collection and preservation be done expeditiously. **The ability to expeditiously preserve a data log is critical in many forms of cybercrime.** For other forms of cybercrime - most notably in the areas of SPAM, Phishing, and many forms of Banking Fraud - the types of obfuscation techniques used (dynamic DNS, fast-flux botnet, double fast-flux botnet, and encrypted proxies) make preservation of evidence extremely difficult. These types of crimes, most often associated with organized crime activity, must be dealt with by means of disruption, technology and a market-based approach as prosecution for these types of crimes is often extremely difficult.
- Adequate log retention may be in practice extremely onerous and of little value in many circumstances, so there should be an obligation to review the application of log retention.
- The Convention, however, does not deal with what is to be done with the stored data after the ninety day period elapses. Should Australia sign the Convention, clear language as to data retention and destruction should accompany any provision on point.
- The Convention also does not deal with the security measures / standards necessary to prevent data breach. Such storage of a large quantity of data also provides a rich ground for information theft.
- There is much criticism of the Convention as being repugnant to privacy protection, the ability for anonymous speech and free speech. These are distinct causes for concern, especially given that Australia does not have a Bill of Rights, Human Rights Act, or a high level of Constitutional protection of civil liberties such as in the United States and Canada. Any Convention provisions adopted, for example, in Canada which may be repugnant to civil liberties may be challenged under the Canadian *Charter of Human Rights and Freedoms*. The same safeguards are not present in Australia, therefore, Australia needs to be particularly cautious in its adoption of procedures which unduly impact on civil liberties.

1.3 Signing States Must Cooperate with Investigations with Other Member States

- **Mutual Assistance** in cross-border investigations is mandated by the Convention. However, unlike most other treaties, the condition of “**dual criminality**” is not present in the Convention. This means that compliance with expedited mutual assistance requests is mandatory even when something that is illegal abroad, would be perfectly legal within Australia’s borders.
- **The Conventions allows signatory States to stipulate dual criminality.** This would allow Australia a comfort zone of knowing that they would not be required to hand over data logs in the case of legal activity in Australia. For example, criminalised content such as political dissent in some foreign countries is often criminalised under multiple provisions including the use of a telecommunications mechanism to transmit illegal materials. The data misuse provisions in some countries could allow for the possibility of a wide ambit of content. “Dual criminality’ is critical, and failure to require it is a flaw in the convention warranting not signing it, unless such a stipulation is entrenched.
- ***Mutual Assistance provisions, however, are significantly diluted as countries with significant cybercrime industries are not party to the Convention.*** Russia, for example, is not party to the Convention.
- Even if nations such as Russia were to sign the Convention, there is scepticism that sufficient resources would be allocated to law enforcement to enable investigation. **The fact is that in ALL nations, cybercrime and e-commerce is under-enforced. Priority inevitably goes to crimes where the victims are locals.** The Convention cannot change this fact. And as a number of other submissions highlight, more resources along with their effective use must be given to law enforcement agencies in Australia.

2.0 Loopholes in the Existing Australian Legal Framework

The relationship between adware, spyware, spam, phishing, search engines, botnets, money mules, and organized crime in general is an *inherently complicated structure*. The connection between many of these supposed legitimate activities such as adware, and malicious applications, is not well documented. Regulatory and policy analysis has typically focused on one or two elements such as spam and phishing, or, in another common example, botnets and DDoS attacks. The artificial categorisation of attacks without comprehension and acknowledgement of how the pieces fit together has led to ineffective and wrongly targeted approaches to policy.

The Centre is currently working on a case study of the Netherlands adware company Dollar Revenue, tracing its roots back to organised crime and botnets, and comparing the legal

framework of the Netherlands with that of Australia. Cybercrime provisions and the governing structure of cybercrime responsibility in the Netherlands have led to successful prosecutions and fines in the area. **There are a number of loopholes in the Australian system which would make such an investigation difficult if not impossible. The following passage offers a detailed example of a Dutch adware company (DollarRevenue) illustrating challenges for law enforcement within the system.**

2.1 Highlighted Points

- **Installation of unwanted software without the user's INFORMED consent is not expressly illegal in Australia**
- **The Australian legal framework is convoluted and outcomes uncertain.**
- **There is no multiplication of small-impact victimisations distributed across numerous jurisdictions.**

These points are considered in detail with a concrete example below.

2.2 Adware / Spyware Example of DollarRevenue

DollarRevenue (DR) Company is a joint venture of three Dutch enterprises (E.C.S. International B.V., WorldToStart B.V. and Media Highway International B.V.) These three enterprises along with their managing directors, whose identities remain undisclosed due to pending criminal investigation, were issued fines totalling one million Euros by the Dutch Telecom Regulator, OPTA, for installing unsolicited software onto over 22 million computers worldwide. According to OPTA's press release of the decision, two companies were fined €300,000 EUR each while the third company was fined €200,000 EUR. The joint venture in question essentially involves three individuals: a director, a programmer and an investor – some of whom are under current criminal investigation for ties to organised crime¹. One director was fined an additional €300,000 EUR while another was fined €200,000 EUR. €300,000 EUR is the maximum that OPTA may impose for failure to adequately inform users of the purpose and function of the installed software as well as for failure to provide a method of reverse installation under the *Dutch Telecommunications Act 2004*.

In its decision, OPTA cites the following reasons for issuing the fine:

These illegally-installed programs unleashed a flood of popup windows containing advertisements for all kinds of products and services. Unsolicited search toolbars were also installed, nested in the toolbars of Windows XP and Microsoft Internet Explorer, where they displayed 'alternative search results'.

¹ Many notorious Russian botnet herders with ties to organised crime were paid to distribute DollarRevenue (DR) software. The money trail leads to a number of organised crime units operating in Eastern Europe. One individual of DR Company in particular is being investigated for more formal ties with such organised groups. This information was imparted under Chatham House Rules at a closed session cybercrime workshop with law enforcement agents.

As the software did not include uninstall functions, it could only be removed with expert assistance.²

Similar activities of the DR company have been reported on stopbadware.org, sunbelt-software and spamlaw.com. The OPTA report, however, fails to mention that DollarRevenue is also involved with malicious spam, iframe injections, and Trojan downloads, which initialise information-capturing software (such as passwords and browser histories). Stopbadware.org claims that the Trojan horse drsmartloader.exe was detectable after installing DR software. This Trojan then allowed the additional installation of adware components including SurfSideKick, Webhancer, NewDotNet and Command Service.³ Spamlaw.com reports that additional adware and Trojan files are downloaded, including a DollarRevenue Trojan, along with, for example, Adware-DCToolbar, Adware-Zeno, and Uploader-R.⁴ Some of the Trojan horse applications made available through other bundled adware programs with DR Software (such as iframedollars) collected usernames and passwords for Internet banking and e-commerce websites. Sunbelt Malware Research Labs provides a screen capture list and video of over 2000 additional adware/spyware programs downloaded in a single DR Software application.⁵ Of these programs, several hundred are executable Trojan style programs.

A conditional penalty was also imposed prohibiting the directors of DR Company from further distribution of unwanted software. The OPTA issued fine was appealed by DR Company. On June 18, 2008, the OPTA Commission dismissed DR Company's objections.⁶ DR Company lodged an appeal against the Commission's decision to the Rotterdam District Court on July 29, 2008.

DR Company claims to be a legitimate advertising company, which displays advertising on third-party computers. The company claims to install its software with proper consent and notice. Captured below is the publicly displayed business model of DR Company as of November 9, 2006, using the Internet Wayback Machine .

² OPTA, "Fact Sheet: Decision to Impose Fine on DollarRevenue" (December, 2007) available at <http://www.cytrap.eu/files/ReguStand/2007/pdf/2007-12-18-DollarRevenue-largestSpywareFineEurope-NL-OPTA.pdf>

³ See <http://www.stopbadware.org/rports/reportdisplay?reportname=dollarrenvue>

⁴ More adware and Trojan files are included on the website. See the Spamlaws website at <http://www.spamlaws.com/Dollarrevenue-adware.html>

⁵ Sunbelt list and video transmission of over 2000 unsolicited software available at <http://www.sunbelt-software.com/ihs/alex/deskwizzclickfraud542006.pdf>.

⁶ OPTA "Decision on objection concerning fines for distributing unsolicited software (DollarRevenue)" available at <http://www.opta.nl/asp/en/publications/document.asp?id=2724>

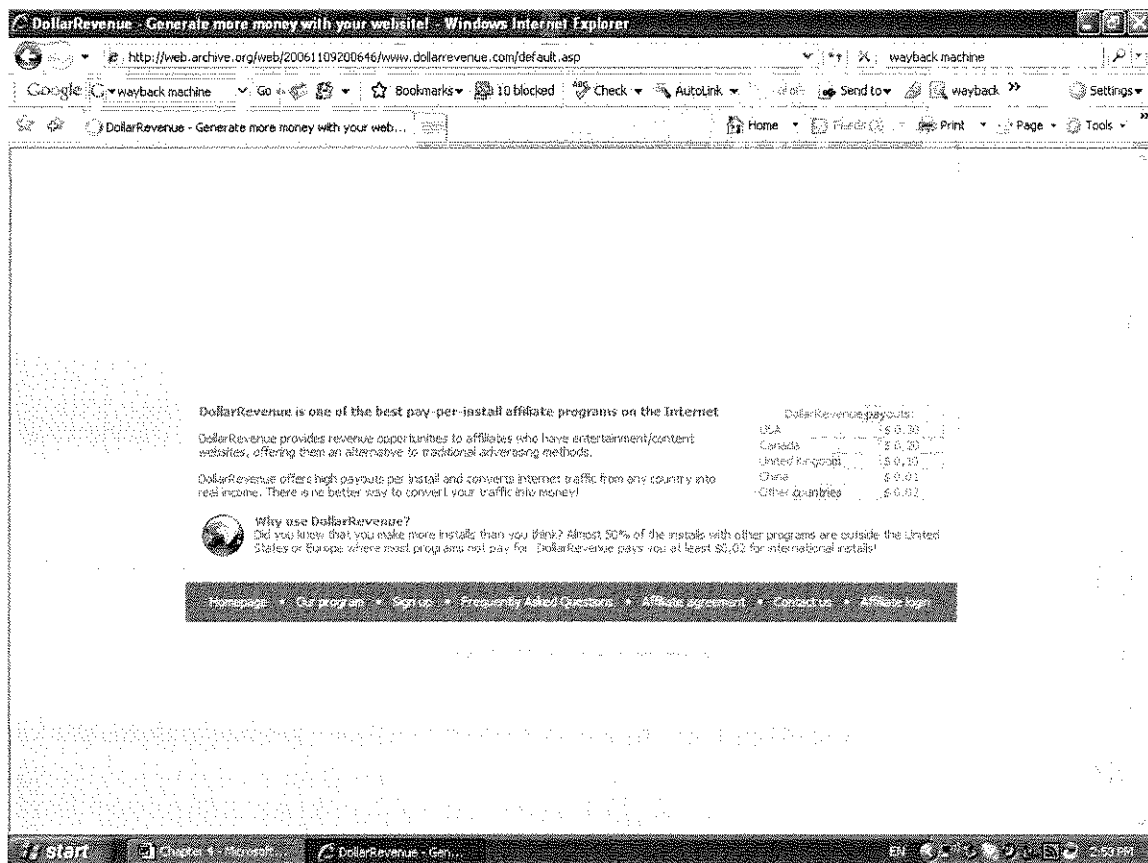


Figure 1.0 Wayback Machine screen shot of www.dollarrevenue.com 'Home Page' as at Nov. 9, 2006

The company uses an affiliate business model where third parties sign-up to DR Company and agree to deploy DR Software through ActiveX and software bundling. Active payouts in North America average \$.25 cents per installation as seen above. Affiliates use a multitude of means to trigger DR Software downloads including SPAM, botnets, luring chatroom sessions, and so forth. DR Company is structured like many spyware companies from a legal perspective – **there is an attempt to transfer liability to third-party affiliates through an online contract.**

Prosecution and legal recourse in a situation such as DollarRevenue could potentially take a number of avenues. As seen in this case study, DollarRevenue was fined by the Dutch telecommunications authority OPTA and DR is being investigated for criminal activity. Two botnet herders that distributed DR software were found guilty of accessing a computer without authorisation in Florida and New Zealand.

Installing software without a user's informed consent is a violation of the Dutch *Telecommunications Act*.⁷ **The *Telecommunications Act* prohibits both unsolicited electronic communications (spam) and the storing of information or gaining access to information in the equipment of end users without permission and proper information (malicious software). The SPAM Act in Australia does not deal with unwanted software installation.** OPTA, the Dutch overseeing body charged with overseeing the

⁷ *Telecommunicatiewet*. The English translation of the Dutch Act was provided by the Ministry of Economic Affairs to the European Union SMART group for their country profile study of Spam and Spyware. See *Spam and Spyware Study SMART 2008/0013 Country profile (Netherlands)*.

Telecommunications Act, has been given wide powers to actively investigate, fine, and issue penalties, and compliance notices. OPTA works with the Dutch police (KLP) to bring criminal charges where it is warranted.

By way of contrast, Australia does not prohibit spyware or many forms of malware. An adware company that paid affiliates to install software without informed user consent would not likely attract legal scrutiny. In 2005, the Senate put forth the *Spyware Bill*, however, the legislation was not passed. The *Spyware Bill* would have prohibited the installation of software without proper and informed consent by the user. The Department of Broadband, Communications and the Digital Economy (DCITA) was given the task of reviewing the legislative framework on spyware and concluded that existing Australian laws were sufficient to protect Australians from spyware and malware. Specifically, the DCITA concluded that the *Criminal Code 1995 (Cth)*, *Trade Practices Act 1974 (Cth)*, *the Australian Securities and Investments Commissions Act 2001 (Cth)*, *Corporations Act 2001 (Cth)*, *Privacy Act 1988 (Cth)*, *Criminal Law Consolidation Act 1935(SA)*, *Telecommunications Act 1997 (Cth)* and the *Telecommunications (Interception) Act 1979 (Cth)* adequately dealt with spyware and malware. DCITA is of the view that spyware may be dealt with through technical means. The report states that:⁸

[s]pyware can be dealt with through technical measures similar to those used to respond to other e-security threats such as spam, phishing and worms. There are a number of freely available and commercial tools that detect, remove and prevent spyware. These are accessible on the Internet or obtaining through retail outlets. Anti-spyware programs should be maintained and updated regularly.

As many of the submissions have noted, anti-spyware and anti-virus software is not up to the task. Malware distributors utilise invasive methods derived at avoiding detection.

The Australian system is convoluted. Any SPAM aspects in a DollarRevenue type investigation would be the prerogative of ACMA, while any type of potentially misleading conduct would fall under ACCC's jurisdiction. It is unclear exactly how the *Trades Practice Act* would apply to an adware/spyware situation where user consent was obtained. S.52 for Deceptive and Misleading Acts does not attract fines whereas it is doubtful if a s.75 Unfair Conduct challenge could be made which could attract fines. In any event, the use of the TPA to address adware and spyware companies would be an uncertain event vulnerable to a multitude of interpretations.

From the legal perspective, charges and fines have not been made against *a single corporation or organisation* for spyware or malware distribution in Australia. Contrast this finding to jurisdictions that have mandated an authority such as OPTA or the United States Federal Trade Commission, where over 100 fines and charges have been made against spyware and malware distribution companies such as DollarRevenue in the United States, Canada and Europe.

⁸ DCITA, "Outcome of Review of the Legislative Framework on Spyware" 2004 available at http://www.dbcde.gov.au/communications_for_consumers/security/spyware/outcome

There would be no obstacles in Australia to pressing charges against a botnet herder. Like the United States and New Zealand, Australia prohibits accessing, modifying, or impairing data or a computer system without consent.⁹

2.3 There is no multiplication of small-impact victimisations distributed across numerous jurisdictions.

Investigation and prosecution of many cybercrimes, in particular fraud, is often done on a balance of expenditure and impact. Most Australian states specify a minimum loss threshold, below which an investigation cannot be launched (Eg. \$35 000). Many organised cybercrime groups operate 'under the radar' of investigation by utilizing various techniques. For example, one could commit credit card fraud of \$5 million dollars without attracting investigative attention providing that the amounts stolen per jurisdiction operated below whatever budget threshold existed in the jurisdiction. Steal \$10 from 100 people in NSW, another \$10 from 100 people in Victoria, another \$10 from 100 people in France, and so forth. **There needs to be an express Memorandum of Understanding or legal provision which allows aggregation of amounts thereby triggering criminal investigation. This needs to be done inter-State in Australia as well as between nations.**

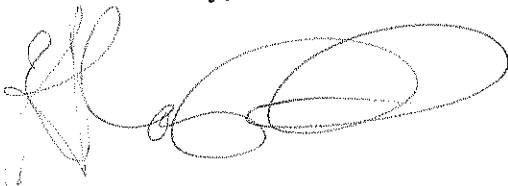
2.4 Emerging Crimes?

There are a number of online activities which the Australian public find distasteful which would not likely attract criminal attention. These are listed without any specific detail, only by way of consideration by the Inquiry Committee:

- Offense to arrange to meet a minor to engage in sexual activity.
- Cyber-bullying resulting in harm.
- Identity Theft
- Unwanted installation of software without a user's informed consent

Thank you for the invitation to make this supplemental submission.

Yours Sincerely,



Alana Maurushat

Lecturer and PhD Candidate, Faculty of Law, UNSW
Deputy Director, Cyberspace Law and Policy Centre, UNSW
a.maurushat@unsw.edu.au +61 2 9385 8027

⁹ See s.476(2) *Criminal Code 1995 (Cth)*.

