SUBMISSION NO. 8



26 June 2009

Mr Jeremy Brown,
A/g Committee Secretary,
House of Representatives
Standing Committee on Communications,
Parliament House, Canberra, ACT 2600

By email: coms.rep@aph.gov.au

Dear Mr Brown,

**Inquiry into Cybercrime and its Impact on Australian Consumers**

The Law Society of Western Australia is grateful for an opportunity to comment on the terms of reference for the above inquiry. We note that the given parameters subsume -

a) The nature and prevalence of e-security risks including financial fraud and theft of personal information, including impact of malicious software such as viruses and Trojans;
b) The implications of these risks on the wider economy, including the growing economic and security impacts of botnets;
c) An inquiry into the level of understanding and awareness of e-security risks within the Australian community;
d) The measures currently deployed to mitigate e-security risks faced by Australian consumers:
    I. Education initiatives
    II. Legislative and regulatory initiatives
    III. Cross-portfolio and inter-jurisdictional co-ordination
    IV. International co-operation
e) Future initiatives that will further mitigate the e-security risks to Australian Internet users; and
f) Emerging technologies to combat these risks.

The scope of these terms of reference seem to us to be very suitable. However we have some concerns relating to the apparent underlying assumption that the threats posed by, for example, phishers or users of Trojans or netbots, are homogenous. We would like to suggest that the inquiry will be more useful if there is a clear appreciation that there are at least four different maliciously intentioned groups who may utilise cybercriminal methods against the Australian consumer to attain different ends. Whilst this differentiation may appear academic, we believe that the resulting harms will justify different legal and practical approaches. To illustrate –

- We believe that there is a basic and pressing need to protect persons using the Internet from small time cybercriminals who engage in card skimming, hacking, phishing to allow password and identity theft to facilitate financial fraud or employment based on misappropriated CVs. Such criminals may work alone and may sell stolen identities/credit card information openly over the Net, sometimes bragging about their IT capabilities and achievements. In 2006 one American investigator monitored 13 million messages under 100,000 names posting such sales in chatrooms over 7 months and estimated their value to be around US$93 million[1]. As Australia is said to be one of the top ten countries for cybercrime[2] the commercial effect of similar activities in this region may be assumed to be substantial both for unfortunate victims and for the Federal Government, since perpetrators are undoubtedly failing to declare their full taxable incomes. Moreover there are other types of small-time cybercrime which should not be overlooked – e.g. the infamous 'Nigerian letter' email scam (now morphing into the fake Australian Tax Office Refund scam and the constant Bank account email scams). There is also the use of websites to solicit for fraudulent charities or for misleading or deceptive adverts for goods including tickets for events, which will never be delivered or if delivered will be found to be defective in quality. The perpetrators of such scams are usually quick to disappear once the money has been received.

- Secondly there are the illegal (mostly natural individual) consumers of music, computer programs and videos all of which have been obtained in breach of copyright legislation. It might be argued that these are outside your remit, but equally it is clear that the net effect of such illegal use is to raise the cost – through the need for expensive encryption, steganography/ watermarking and other security devices - for legitimate consumers. With the development of The Pirate Bay[3], a website which now facilitates anonymous downloading of files in breach of copyright, and free access to Bitblinder, an anonymous remailer, the opportunities for illicit copying of films and music produced in Australia has increased, with the corresponding loss of royalties to persons involved in these businesses. There is also the concomitant loss of sales to video and CD shops in the country.

- Thirdly there is the commercial threat posed by more organised national and international cybercriminal groups directly to Australian businesses. This can encompass the use of viruses, Denial of Service attacks, botnets, keylogging, and industrial espionage. The motivation here is usually profit based but it is not inconceivable that unscrupulous operators could resort to hiring hackers etc to damage rivals. It appears there is already the facility of renting-a-botnet[4] to steal information from secretly infected business computers, and the recent Australian Business Assessment Of Computer User Security, based on a national survey of

---

[1] See J. Giles, Your Life Sold For $15, *New Scientist,*23 May 2009 pp 36-39 at p 38.

[2] Ibid, p39

[3] See 'Download Pirates to Launch New Weapon' *Sydney Morning Herald* 17/6/09

[4] Evgeny Morozov, from *Foreign Policy* magazine, interviewed by ABC Background Briefing, 24 May 2009

4,000 businesses, showed that 13% of small businesses, 20% of medium businesses and 30% of large organisations have been affected by security breaches[5] with a resulting cost of between $595 - $649 million. Such costs are passed on to consumers.

- Finally there is the potential threat posed to commerce by malicious governments wishing to cause economic havoc for their own political purposes. This may sound paranoid, but revelations of the Chinese governments benefitting from Ghostnet (their botnet) by acquiring Tibetan secrets suggest the latent opportunities for other governments to misappropriate classified industrial or defence information. GhostRAT, the remote access tool used to infect other people's/ countries computers is apparently freely available for downloading from the Internet[6] and given that some businesses are inadequately protected against spying or infiltration, it should be anticipated that either individuals, organised cybercrime gangs or idealists from less-friendly countries will sooner or later attack Australian industrial secrets, which will also have a deleterious effect on Australian consumers. It is moreover not impossible that either unfriendly governments or organised groups of cybercriminals, noting the chaos caused by the current global financial crisis, might seek to manipulate Australian banking data and stock exchanges for their own ends.

We would further like to make the following suggestions –

- When investigating cybercrime and its impact on Australian consumers, there is a need to consider some pertinent underlying questions e.g. –
    - Can there be property rights of some description in personal information, to overcome the problem of its illegal duplication by hackers who nonetheless fall short of 'stealing' this information in the traditional sense of removing it?
    - What - if any - should be the liability of businesses which hold personal data and yet do not protect this adequately from phishing? Is there a need for a mandated standard/ series of standards depending on the size of a business, the sensitivity of the information it holds, and the possible value to a hacker of this information?
    - What - if any - should be the liability of ISPs who knowingly or negligently allow persons to download songs, videos or computer programs in breach of copyright laws, or who facilitate such illegal downloading by others?
    - What - if any - should be the liability of persons who distribute anonymisers on their websites/ run such anonymisers on their computers? In the absence of a cogent reason for anonymising, should such activity be prima facie evidence of malicious intent?

---

[5] Reported in *Sydney Morning Herald* 16/6/09

[6] International computer security expert, Nart Villeneuve interviewed by ABC Background Briefing, 24 May 2009

- Absent any cogent justification, should possession or use of asymmetric encryption software above a certain power/ bit size be prima facie grounds for a presumption of malign intent if (but only if) the decryption key has not been previously lodged with a Trusted Third Party approved by the government?

- When addressing the questions of the restriction/ elimination of cybercrime in order to benefit consumers, there is an urgent need to address and resolve problems of prosecution of cybercrime, since simply identifying the problems will not lead to their rectification. These problems include-

    - Lack of overarching agreed international standards, regulations and legislation (e.g. flowing from international agreements) as to what constitutes unacceptable commercial behaviour in cyberspace.

    - Problems of jurisdiction and proper law. At the moment it is impractical for many interjurisdictional issues to be litigated due to cost, forum shopping and the incapacity of many individual consumers to enforce a favourable judgement even if they receive this from the courts. The reduction of the law to a purely theoretical guardian of rights is a significant loss to the whole society, not just to the injured consumers.

    - The problem of evanescent evidence. Whilst deleted information can often be restored e.g. via magnetic force microscopy, these techniques usually require experts to utilise them, involving considerable expense and putting them outside the range of most private litigants. Consequently there remain problems in locating and identifying evidence, on computers/ memory sticks etc, which has been deleted and overwritten in an attempt to conceal it.

Thank you for this opportunity to contribute to the discussion concerning your Inquiry. If we may assist in any further way, please do not hesitate to contact us.

Yours sincerely

Mr Dudley Stow
President