Available online at www.sciencedirect.com

SciVerse ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Legal jurisdiction over malware-related crimes[1]: From theories of jurisdiction to solid practical application

Rizal Rahman [a,b]

[a] *University of Otago, Dunedin 9016, New Zealand*
[b] *National University of Malaysia, Malaysia*

Keywords:
Cybercrime
Malware
Extraterritorial jurisdiction
Convention on cybercrime

ABSTRACT

As far as malware-related crimes are concerned, extra territorial jurisdiction and the law of extradition need one another to work perfectly, but there has never been a standard universal rule governing them. While Universality Principle can be argued to be the most ideal solution to the problem, it is opposed by the supporters of the notion of self-regulation of the internet, not to mention it lacks the required universal support. Thus the determination of the issues has to be based on the analysis of existing measures of practical applications.

1. Applying the theories of jurisdiction on malware-related crimes

The general rule of criminal jurisdiction throughout the world is that the main jurisdictional form for criminal prosecution is spatial in nature, regardless of the nationality of the offender. But as criminals are always on the move, some legislation provides for extraterritorial jurisdiction. For example, the United Kingdom provides for this jurisdiction under s 4, 5, 6, 7 and 8 of the Computer Misuse Act 1990. Considering the borderless nature of cyberspace, there is no doubt at all that this kind of jurisdiction assists, to a certain extent, in apprehending criminals and bringing them to face justice.

As far as the ASEAN region is concerned, cybercrime is recognised as one of the eight transnational crimes (in addition to illicit drug trafficking, money laundering, terrorism, arms smuggling, trafficking in person, sea piracy and international economic crime).[2] The addition of cybercrime into the list was decided in the Official Senior Meeting on Transnational Crime (SOMTC) which was held in Singapore on 10 October 2001.

However, cybercrime is not just a regional problem. While ASEAN, G8 and to a wider extent the Council of Europe have the potential to see eye to eye to the cybercrime problem,[3] different countries have their own distinctive approaches to crimes. Therefore the so-called extraterritorial powers, though stated in clear terms in particular statutes, are not automatic in nature. Koops and Brenner remarked that[4]:

> *At an extreme end of jurisdiction claims, some countries that do have cybercrime jurisdiction provisions, such as Malaysia, have such sweeping provisions that they can theoretically claim jurisdiction for any cybercrime committed... (Emphasis added).*

This means that by theory it is possible, but practically speaking, all countries with extraterritorial jurisdictions are subservient to the procedures listed in designated extradition laws of one another, in the absence of which there may be ad

[1] A category of cybercrime which utilises malware as major means of its operation.
[2] The list of the other transnational crimes was introduced by the ASEAN Interior Ministers' meeting in Manila on 20 December 1997.
[3] See Johan Eriksson and Giampiero Giacomello *International Relations and Security in the Digital Age* (Routledge, New York, 2007) at 163. Eriksson and Giacomello observed that COE and G8 are the most advanced, as far as regional measure is concerned, in fighting cross border cybercrimes. (Eriksson and Giacomello, 2007).
[4] Bert-Jaap Koops and Susan W. Brenner, *Cybercrime and Jurisdiction: A Global Survey* (Cambridge University Press, New York, 2006) at 3. (Koops and Brenner, 2006).

0267-3649/$ – see front matter © 2012 Rizal Rahman. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.clsr.2012.03.004

hoc extradition agreements between countries. And it should always be remembered that there is no standard universal rule for extraterritorial legislation. Countries may lean, at their own accord and choices, towards the Passive Personality Principle, the Active Personality Principle (Nationality Principle) or the Universality Principle.

In determining the locality for whose extraterritorial power applies in any single case, the general practice is to identify and ascertain the place where the offence is initiated or committed or completed; or the place where the effect of the criminal act is felt. But to apply the general rule to perpetrators of malware is not as easy as it seems. Grabosky states that "extradition is likely to be more cumbersome the greater the cultural and ideological distance between the two parties",[5] not to mention that their "enforcement costs are also often prohibitive" due to the time, money and uncertainty required by international investigations and the infrequent existence of "congruence of values and priorities" in different countries.[6]

In addition to the ideological and cultural divide, different legal systems also contribute towards a troublesome extradition process. Brenner, commenting on the "Invita" and "Rome Labs" cases, pointed out: "While informal cooperation proved effective in the Rome Labs investigation, that investigation only required the cooperation of officers from two culturally compatible nations; informal cooperation can be a less reliable mechanism when multiple states with varying legal systems are involved."[7]

The above drawbacks have led criminals to choose "safer" jurisdictions, a "cybercrime haven",[8] to base their operation, where punishment is lighter or extradition arrangements would be troublesome. As put by Chanda[9]:

> *As a biological virus takes over a host cell to proliferate, cybercriminals also seem to be on the lookout for countries that have weak cybercrime laws, poor enforcement, or official corruption.*

As for malware criminals, they are very good in using proxies to hide their identity. With the abundance of free and cracked IP hiders on the net, it is nearly impossible not to detect an innocent computer user, whose IP has been compromised, as the offender. Commenting on the difference in punishment for the same offence in different countries, Yar pointed out that[10]:

> *Cross-national variations can encourage what is referred to as "regulatory arbitrage", with individuals and groups committing offences from those territories where they are assured of facing little or nothing in the way of criminal sanctions.*

This cynicism was also shared by Kon and Church in their case note in *Director of Public Prosecutions v David Lennon*,[11] where they observed that the tendency of UK courts towards a tougher approach to computer[fx1]crime "does not really provide much comfort to legitimate users of the Internet, given the international nature of these attacks and the practical and jurisdictional issues in tracking them back to their sources."[12]

Taking the transnational dimension of cybercrimes into account, the Universality Principle may be regarded as the most comprehensive principle for extraterritorial powers.[13] It allows any country to prosecute any criminal regardless of the locus delicti[14] and/or the nationality of the offender or victim.[15] Commenting on the extraterritorial jurisdiction in the Malaysian Computer Crimes Act 1997, Brenner and Koops pointed out that: "this effectively gives Malaysia's cybercrime statute the widest possible jurisdiction scope, to the effect of establishing universal jurisdiction."[16] According to s 9 of the Computer Crimes Act:

(1) The provisions of this Act shall, in relation to any person, whatever his nationality or citizenship, have effect outside as well as within Malaysia, and where an offence under this Act is committed by any person in any place outside Malaysia, he may be dealt with in respect of such offence as if it was committed at any place within Malaysia.
(2) For the purposes of subsection (1), this Act shall apply if, for the offence in question, the computer, program or data was in Malaysia or capable of being connected to or sent to or used by or with a computer in Malaysia at the material time.

Brenner and Koops argued that the above clause "or capable of being connected to or sent to or used by or with

[5] Peter Grabosky "The Global Cyber-crime Problem: The Socio-Economic Impact" in Roderic G. Broadhurst and Peter N. Grabosky (Ed) *Cyber-Crime: The Challenge in Asia* (Hong Kong University Press, Hong Kong, 2005) 29 at 52. (Grabosky, 2005).

[6] Ibid, at 51.

[7] Susan W. Brenner and Joseph J. Schwerha "Transnational Evidence Gathering and Local Prosecution of International Cybercrime" (2002) 20 J. Marshall J. Computer & Info. L. 347 at 353. (Brenner and Schwerha, 2002). See also Susan W. Brenner and Joseph J. Schwerha IV "Introduction—Cybercrime: A Note on International Issues" (2004) 6(2) Information Systems Frontiers 111 at 112. (Brenner and Schwerha, 2004).

[8] Goodman and Brenner pointed out that a country can be a cybercrime haven by design or by default. See Marc D. Goodman and Susan W. Brenner "The Emerging Consensus on Criminal Conduct in Cyberspace" (2002) 10(2) IJL&IT 139 at 167. (Goodman and Brenner, 2002).

[9] Nayan Chanda *Bound Together: How Traders, Preachers, Adventurers, and Warriors Shaped Globalization* (Yale University Press, new Haven, 2007) at 242. (Chanda, 2007).

[10] Majid Yar *Cybercrime and Society* (Thousand Oaks, London, 2006) at 41. (Yar, 2006).

[11] [2006] EWHC 1201.

[12] Georgina Kon and Peter Church "Case note – *Director of Public Prosecutions v. David Lennon* [2006] EWHC 1201" [2006] 22 *Computer Law & Security Report* 416. (Kon and Church, 2006). See also Lynne Yarbro Williams "Catch Me If You Can: A Taxonomically Structured Approach to Cybercrime" (2008) Forum on Public Policy: A Journal of the Oxford Round Table <www.forumonpublicpolicy.com>. (Williams, 2008).

[13] See "Universal Jurisdiction: UN General Assembly Should Support this Essential International Justice Tool" in *Amnesty International Report* (2010) at 9.

[14] The place where the crimes are committed.

[15] See "Universal Jurisdiction: UN General Assembly Should Support this Essential International Justice Tool" in *Amnesty International Report* (2010) at 9.

[16] Susan W. Brenner and Bert-Jaap Koops "Approaches to Cybercrime Jurisdiction" (2004) 4 J. High Tech. L. 1 at 21. (Brenner and Koops, 2004).