House of Representatives Standing Committee on Communications

Answers to Questions on Notice

Inquiry into Cybercrime

Public Hearing 21 October 2009

Australian Communications and Media Authority

Question No: 1

Hansard Ref: COMM 4

Topic: ISP liability

Question:

Is there a liability question for ISPs terminating a service to a client?

Answer:

Under the Internet Industry Spam Code of Practice (IISCP), which is a Code registered by the Australian Communications and Media Authority under the *Telecommunications Act 1997*, each ISP must have an "acceptable use policy" in its contract with each customer. Under clause 7.3 of the IISCP, that acceptable use policy, and so the contract between the ISP and the customer, must contain a clause:

...that allows for immediate account disconnection or suspension when the ISP becomes aware of inbound connections to any service they host that allows email forwarding on behalf of third parties, regardless of whether the open service is provided intentionally, through misconfiguration, or by other means not authorised by that third party including but not limited to through a Trojan horse or virus...

In circumstances where the ISP exercises a contractual right such as this, then the ISP should generally be able to terminate or suspend the service without adverse legal consequences.

In other circumstances, it is not possible to be definitive about the legal consequences of any termination, as those consequences will depend upon all the relevant circumstances of the case, including, in particular, the other terms of the contract between the ISP and its customer.

House of Representatives Standing Committee on Communications

Answers to Questions on Notice

Inquiry into Cybercrime

Public Hearing 21 October 2009

Australian Communications and Media Authority

Question No: 2

Hansard Ref: COMM 7 and 14

Topic: Data sources for AISI

Question:

Where does AISI collect its data from?

Answer:

The AISI collects data from a number of parties who run honeypots, spamtraps, sinkholes and other mechanisms for the purpose of identifying compromised hosts or other malicious activities on the internet.

The ACMA often agrees not to disclose the operations, tools, methods and infrastructure utilised by its partners, and for this reason we cannot publicly disclose all sources. A list of confidential sources will be submitted separately to the Chair of the Standing Committee on Communications.

The publically acknowledged sources are:

* The Shadowserver Foundation
  http://www.shadowserver.org/
* The Australian Honeynet Project
  http://www.honeynet.org.au/
* SORBS (Spam and Open Relay Blocking System)
  http://www.au.sorbs.net/
* The ACMA's own honeypots and spamtraps

House of Representatives Standing Committee on Communications

Answers to Questions on Notice

Inquiry into Cybercrime

Public Hearing 21 October 2009

Australian Communications and Media Authority

Question No: 3

Hansard Ref: not applicable (additional question)

Topic: Consistent reporting of suspected malicious network activity

Question:

The draft ISP E Security Code of Practice leaves the reporting of network attacks to the discretion to ISPs:

a. what is the rationale for continuing to allow ISPs such wide discretion on whether or not to report criminal and other illegal activity to AusCert and law enforcement?

b. if ACMA's powers were to be strengthened in relation to ISPs, especially those that fail to take action in response to compromised machines, what 'enforcement' model and type of powers would be appropriate?

Answer:

a. The E-Security Code of Practice is being prepared by the Internet Industry Association. As such, the ACMA is only tangentially involved as an observer, despite the focus on the AISI reports present in the code. As the E-Security Code of Practice will be a voluntary industry code, it will not be registered with the ACMA and its provisions will not be not enforceable. Criminal enforcement is not a responsibility of the ACMA.

   AISI reports do not generally reveal criminal activity by Australian ISP subscribers; they indicate that these Australians are the victims of unknown third parties. When the ACMA suspects criminal activity from Australia it directly contacts the applicable state police or, depending on the type of offence, the Australian Federal Police.

b. The ACMA generally practises a graduated approach to regulation including appropriately escalating enforcement. The current code is planned to take the form of an industry best practice document and is not a registered code.

   Given a need to increase regulation in this area the ACMA would have the following options:

   1. A registered industry code – for example, the Internet Industry Spam Code of Practice is a code registered with ACMA that shares come commonalities with the E-Security Code of Practice. Pursuant to section 121 of the *Telecommunications Act 1997*, the ACMA can order sections of industry to comply with an industry code.

House of Representatives Standing Committee on Communications

Answers to Questions on Notice

Inquiry into Cybercrime

Public Hearing 21 October 2009

Australian Communications and Media Authority

2. An industry standard – pursuant to Part 6, Division 5 of the *Telecommunications Act 1997*, should the ACMA feel that an industry code has not been developed, is not appropriate or the code has failed, the ACMA can mandate an industry standard apply. All sections of the industry must comply with industry standards and civil penalty provisions exist for breaches of the standard.

3. Primary legislation – should it be deemed that an industry standard is not sufficient to enforce industry compliance in the matter, primary legislation may be considered. This would potentially allow for the provision of criminal penalties for non-reporting of compromises.

   The ACMA anticipates that the industry will comply with the current code considering the level of interest that has been shown by ISPs. The ACMA also feels that an increased level of regulation would draw resources away from combating the incidence of compromises on ISP networks.

House of Representatives Standing Committee on Communications

Answers to Questions on Notice

Inquiry into Cybercrime

Public Hearing 21 October 2009

Australian Communications and Media Authority

Question No: 4

Hansard Ref: not applicable (additional question)

Topic: Infected website

Question:

ACMA gave evidence that the problem of infected websites is now the number one issue that must be addressed to adequately respond to cyber crime:

a. what strategies does Australia need to consider for addressing the problem of infected websites?

b. what legal powers, and technical and personnel resources are needed to implement a nationally scaled strategic response to infected websites?

Answer:

a. A range of options for addressing the problem of infected websites could be considered, including a web compromise reporting and detection system. Such a system could operate under a similar framework to that of the AISI, that is, the ACMA could obtain data on compromised web pages from various sources (including developing an internal capability), collate this data, and provide daily aggregated reports to ISPs identifying infected web pages residing on their networks. In addition to ISPs, domain owners and hosting companies could also be included.

b. A registered industry code outlining industry procedures for dealing with infected websites and notifications of infected websites could apply. As the ACMA has the power to enforce the provisions of registered codes, this could be pertinent in cases where there was a need to direct a service provider to remove malicious content. A registered code would also serve the purpose of indemnifying ISPs who act on reports of infected websites.

House of Representatives Standing Committee on Communications

Answers to Questions on Notice

Inquiry into Cybercrime

Public Hearing 21 October 2009

Australian Communications and Media Authority

Question No: 5

Hansard Ref: not applicable (additional question)

Topic: Malicious unauthorised internet publication of images and statements

Question:

Most ISP user agreements include terms that make using the service for an unlawful activity a breach of contract. However, the unauthorised publication of malicious and defamatory images and statements appears to have increased:

a. does ACMA have any powers to order the take down of specific material or an entire website hosted in Australia or overseas that publishes unauthorised malicious images or statements, intended to ridicule, defame or otherwise harm a victim?

b. if not, what are the pros and cons of expanding ACMA's power to enable it to respond to an individual complaint where the ISP fails to act on substantiated breach of the users agreement?

Answer:

a. The ACMA's powers in relation to online content do not expressly cover unauthorised malicious images or statements, intended to ridicule, defame or otherwise harm a victim. Under Schedule 7 to the *Broadcasting Services Act 1992* (BSA), the ACMA has the power to direct an Australian hosting service provider to take-down content that is prohibited content (or in certain cases take action to ensure that the content is not prohibited content). Prohibited content is defined in clause 20 of Schedule 7 to the BSA, with reference to the National Classification Scheme categories set out in the *Classification (Publications, Films and Computer Games) Act 1995* (Classification Act), and includes:

- content that is classified RC or X
- content that is classified R18+ and not subject to a restricted access system
- content that is classified MA15+, not subject to a restricted access system, and provided on payment of a fee.

The National Classification Scheme is a portfolio responsibility of the Minister for Home Affairs. The ACMA asks the Classification Board to classify content that has been the subject of a complaint when the ACMA is uncertain of the appropriate classification. In the case of content that is hosted in Australia, the ACMA must ask the Classification Board to classify content that is likely to be prohibited.

The requirements for restricted access systems are set out in Restricted Access System Declaration 2007 (http://www.acma.gov.au/webwr/_assets/main/lib310563/ras_declaration_2007.pdf).

The types of content which comprise each classification are set out in the Schedule to the Classification Act, and the Classification Board's Guidelines for Classification of Films and Computer Games. The types of content which are likely to be prohibited content include:

- depictions or descriptions of child sexual abuse
- depictions of sexual activity
- depictions of sexual violence
- detailed depictions of violence
- detailed instruction in crime or violence
- material which advocates the doing of a terrorist act.

The Classification Board's guidelines state classifications are to be determined with regard to the impact of the material in question. Factors such as whether material is unauthorised, defamatory, intended to cause harm to a person or ridicules a person may have some bearing on its impact and classification, but are not likely to be primary determinants of its classification.

The ACMA does not have power under the BSA to direct removal of prohibited content that is hosted outside Australia. Instead such content is added to a list of URLs that is provided to filter software vendors. This arrangement is set out in a code of practice for ISPs that is registered under the BSA.

b. Such a proposal would be complex to implement in terms of identifying and locating services that are subjects of complaints, and establishing the facts of the unlawful activity, which can be expected to be open to dispute and may be a matter for a court. Such a proposal would significantly expand the scope of material covered by the current Online Content Scheme and, as such, would be a matter of government policy.

House of Representatives Standing Committee on Communications

Answers to Questions on Notice

Inquiry into Cybercrime

Public Hearing 21 October 2009

Australian Communications and Media Authority

Question No: 6

Hansard Ref: not applicable (additional question)

Topic: Memoranda of Understanding

Question:

During the hearing on 21 October, ACMA advised that Australia has entered into a number of MOUs with different countries to assist with information sharing, especially in relation to spam.

a. Could ACMA please provide a typical example of such an MOU for the Committee's information?

b. How is the privacy of Australian's protected under the MOUs?

Answer:

a. An example of a typical MOU the ACMA has in place with a government body from another country is the Memorandum of Understanding between the ACMA and the New Zealand Department of Internal Affairs (DIA). The intent of this MOU is to assist in the fight against spam by establishing channels of communication that allow both the ACMA and the DIA to move quickly in response to the challenges and demands of the ever-changing spam environment.

   A copy of the ACMA - DIA MOU is provided at **Attachment A**.

b. The ACMA's MOUs are non-binding agreements that set out to facilitate information sharing with overseas regulators.

   MOUs are entered into voluntarily and do not create any enforceable rights or obligations on any signatory to the MOU. The terms of an MOU do not override any legislation in place in a signatory's country/jurisdiction.

   The ACMA generally complies with MOUs to which it is a party to the extent that it can, and, in deciding whether it can do so, the ACMA is cognisant of Australia's legislative framework, including the *Privacy Act 1998*. The ACMA will decline to accede to a request for information from another signatory where provision of such information would contravene any law to which the ACMA is subject, or would be inconsistent with government policy.

   Similarly, the other signatories to MOUs with the ACMA are not required to do anything that would contravene a law of their jurisdiction or otherwise be inconvenient.

Memorandum of Understanding

Between

The Australian Communications And Media Authority (ACMA)

And

The New Zealand Department of Internal Affairs (DIA)

1. BACKGROUND

1.1 The Australian Communications and Media Authority (ACMA) is a statutory agency established under section 6 of the *Australian Communications and Media Authority Act 2005* of the Commonwealth of Australia. ACMA regulates broadcasting and datacasting services, radiocommunications, telecommunications and Internet content in Australia

1.2 ACMA is responsible for the regulation and enforcement of, among other things, the sending of commercial electronic messages under the *Spam Act 2003* and telemarketing within the meaning of, and in accordance with the *Do Not Call Register Act 2006*.

1.3 The New Zealand Department of Internal Affairs (DIA), through the Anti-Spam Compliance Unit of its Regulation and Compliance Branch, is responsible for the enforcement of the *Unsolicited Electronic Messages Act 2007*, in accordance with section 20 of that Act.

2. DEFINITIONS

2.1 In this Memorandum, ACMA and DIA shall agree to the definition of the terms used in the operative clauses as follows, unless otherwise indicated:

(a) **adverse information** means any information which is not publicly available and which relates to a person (other than an Agency as defined in this Memorandum) and which has the potential, if publicly disclosed, of affecting in a negative way the reputation, standing, interests or rights (legal, beneficial, legitimate or other) of that person;

(b) **Agency** means either the ACMA or DIA as the context allows and Agencies shall be construed accordingly;

(c) **confidential information** means information provided in circumstances where an agency is subject to a duty of confidence, whether arising by the application of statute, common law or equity;

(d) **Memorandum** means this Memorandum of Understanding;

(e) **Minister** means the Minister responsible for administering the enactment by which the agency is established;

(f) **person** includes an individual, a natural person, a body corporate, an unincorporated association, a partnership, a statutory authority or instrumentality of a government;

(g) **requested agency** means the agency to which a request has been made under this Memorandum; and

(h) **requesting agency** means the agency making a request under this Memorandum.

3. PURPOSE AND SCOPE

3.1 The Agencies recognise that co-operation between them is desirable to assist in the discharge of their respective functions in Australia and New Zealand.

3.2 The purpose of this Memorandum is to promote and facilitate the cooperation, assistance and exchange of information, including confidential information, relevant to the regulatory functions of each Agency, while recognising the legal, policy and administrative limits on the powers of each agency to exchange such information.

3.3 This Memorandum aims to establish channels of communication between the Agencies and to increase mutual understanding of the operations and functions of the Agencies, so that the Agencies are in a better position to meet the challenges and demands of the regulatory environment

Part I: Framework for consultations regarding matters of mutual interest

4. STATEMENT OF INTENT

4.1 This Memorandum is a voluntary statement of intent of the Agencies to provide full mutual assistance to, and cooperation with the other Agency and accordingly does not create any enforceable rights or binding legal obligations upon the Agencies.

4.2 This Memorandum does not prohibit either Agency from taking other measures which conform to domestic or international law, to achieve the same purpose.

4.3 This Memorandum does not affect the right or ability of either Agency to obtain information from any persons to ensure compliance with, or to enforce the laws or regulations of the country of either Agency. In particular, this Memorandum does not affect any right of either Agency to communicate with, or obtain information or documents from, any person, on a voluntary basis or otherwise, in the country of the other Agency.

4.4 This Memorandum does not affect the ability of the Agencies to exchange non-confidential information.

Part II: Provision of information, documents and assistance

5. EXCHANGE OF INFORMATION

5.1 The Agencies will use their best endeavours to comply with the terms of this Memorandum.

5.2 The Agencies agree that, subject to their respective laws and regulations, information available to one Agency, will be shared as requested, provided

that compliance with the request will not adversely affect the operations of the requested Agency.

5.3 When exchanging confidential information, the Agencies acknowledge the confidentiality and secrecy requirements of the laws and regulations under which each Agency operates. The requesting Agency will comply with any such conditions placed on the exchange of information and will not release or disclose to a third party(other than its legal advisers), without the express consent of the requested Agency or as specified in the Request.

5.4 The requested Agency may deny a request under this Memorandum on the grounds that:

(a) the request is not made in accordance with the provisions of this Memorandum;

(b) giving effect to the request would:

i) be contrary to the national or public interest or the law of the country of the requested Agency; or

ii) be beyond the statutory powers of the requested Agency;

iii) relate to the administration of a law, regulation or requirement that does not exist, and has no parallel within the jurisdiction of the requested Agency;

iv) put the requested Agency in breach or at risk of being in breach, of a legal or equitable duty owed to any person (particularly relating to confidentiality, privacy and procedural fairness);

v) expose the requested Agency to the threat of legal proceedings, however unjustified those proceedings may be;

vi) be contrary to, or incompatible with, the requested Agency's aims or any of its policies or internal guidelines, whether or not such aims, policies or internal guidelines are set out in writing; or

vii) in the requested Agency's opinion, place too great a strain on its resources or substantially or unreasonably divert its resources.

5.5 Where the requested Agency denies or opposes a request for assistance, it will provide reasons why it is not providing assistance within 14 days of receiving the request. The Agencies will consult on other possible means of dealing with the request.

6. UNSOLICITED INFORMATION

6.1 The Agencies may, without any prior request for assistance, provide to each other information they hold which they may consider useful to the other Agency in the performance of its functions and for the purposes that may be specified in the provision of the information. In such cases, the terms and

conditions of this Memorandum will apply if the providing Agency specifies that the information is given under this Memorandum.

6.2 The Agencies will endeavour to hold meetings (in-person or by other arrangement), at least on an annual basis, to discuss related topics and share information

7. REQUESTS FOR ASSISTANCE ON COMPLIANCE AND ENFORCEMENT MATTERS

7.1 Requests for assistance in relation to compliance and enforcement matters must be made in writing and addressed to the appropriate contact specified in the principal points of contact set out in Annexure A.

7.2 When making a request for assistance, the Agencies will endeavour to provide sufficient information including (as practicable) the following:

(a) a description of the assistance, documents or information sought by the requesting Agency;

(b) the purpose(s) for which the assistance, information or documents are sought;

(c) a brief description of the facts giving rise to the request (including details of the rule or law to which the subject matter of the request relates);

(d) whether the information is sought as part of an investigation into suspected breaches of the law or for compliance purposes;

(e) the link between the specified rule or law and the regulatory functions of the requesting Agency;

(f) where the request relates to an alleged breach, the possible sanctions, penalties or consequences that may result from proceedings arising from the investigation;

(g) a suggested time period for reply and if appropriate, the urgency of the request; and

(h) to whom, if anyone, onward disclosure of information is likely to be necessary and the reason for such disclosure;

7.3 If the matter is urgent, such requests may be submitted in summary form or in such other manner, as is agreed between the parties, provided that any such request is confirmed in writing in the manner set out in clause 7.2 within 5 business days.

8. PROCEDURE FOR REQUESTS FOR INFORMATION OR DOCUMENTS

8.1 An Agency may request information or documents or assistance, not relevant to a compliance or enforcement matter from the other Agency

8.2 All requests for documents or information will be made in writing, or orally, and unless agreed otherwise, be confirmed in writing within a reasonable period and include the information set out in 8.3.

8.3 The requesting Agency will ensure that a request for documents or information shall include the following details:

(a) a description of the subject matter of the request;

(b) the purpose for which the information is required;

(c) a description of the information or documents;

(d) a suggested time period for reply and if appropriate, the urgency of the request; and

(e) any requirements for confidentiality in respect of the request.

9. PROCEDURE FOR PROVISION OF INFORMATION OR DOCUMENTS

9.1 The requested Agency will consider each request on a case-by-case basis to determine whether the request will be complied with under the terms of this Memorandum.

9.2 The requested Agency will use its best endeavours to advise the requesting Agency, within seven days of receipt of the request, as to its decision on the request and a time frame for responding to the request, provided that:

(a) where the requested Agency requires the consent of a person, or is required to advise a person of the request before complying with such a request, the requested Agency will advise the requesting Agency of this fact before contacting that person; or

(b) where the request cannot be complied with completely, the requested Agency may at its discretion consider whether there may be other assistance that may be given, or whether another person or body within its jurisdiction may be able to assist the requesting Agency.

9.3 The requested Agency may provide information or documents to the requesting Agency subject to the following conditions:

(a) with written restrictions or limitations as to the use, access or storage of the requested information or documents;

(b) any confidentiality requirements relating to the information or documents provided, which may include releasing the information subject to an undertaking of confidentiality being provided;

(c) if the requested Agency is likely to incur significant costs and expenses in obtaining the information, it will provide the requesting Agency with an estimate of costs and expenses and seek agreement as to a contribution to the costs and expenses before providing that information; and

(d) such other conditions as the requested Agency considers appropriate.

10. PERMISSIBLE USE OF THE INFORMATION

10.1 The requesting Agency shall use the documents or information provided pursuant to this Memorandum solely for the purposes stated in the request

10.2 Where the request was made under clause 7, the information or documents furnished shall be used solely for purposes stated in the request with a view to ensuring compliance with or enforcement of the laws and regulations specified in the request and for any criminal, civil or administrative proceeding dealing with the purported contravention of the provisions specified in the request.

10.3 If the requesting Agency wishes to use the information provided for any purpose other than those stated in the request:

(a) the requesting Agency must ask the requested Agency for its consent to use the information or documents for another purpose; and

(b) the requested Agency must, within 14 days of receipt of such request, indicate in writing, or orally (followed by written confirmation), whether or not it consents to such use.

10.4 The requested Agency may agree to the use of such information subject to such conditions as specified in writing.

11. CONFIDENTIALITY OF REQUESTS

11.1 The requesting Agency shall take every precaution to keep confidential all requests for information made under this Memorandum, the content of such requests and any other matters arising from consultation about the requests

11.2 In all cases, the requesting Agency shall endeavour to keep confidential any information or documents received pursuant to this Memorandum if requested to do so by the requested Agency, unless a law, including a court order, of the country of the requesting Agency requires disclosure of the documents.

11.3 Unless specified in conditions imposed by the requested Agency nothing in this clause will prevent the flow of information to relevant Government Ministers (and their agents) under any reporting requirements that affect the relevant agency.

11.4 Where compelled by law or a court order to disclose the information received, the requesting Agency should, wherever possible, give prior written notification to the requested Agency before such a disclosure can be made The Agencies will consult as to the response and any appropriate action

Part III: Miscellaneous provisions

12. CONTACT POINTS

12.1 All communications between the Agencies should be between:

(a) the principal points of contact as defined in Annexure A, which may be amended by written notice from either Agency, without the need for re-signature of this Memorandum; or

(b) an officer of an Agency authorised to perform the usual duties of a principal point of contact during an absence from duty; or

(c) any officer of an Agency authorised by a principal point of contact to communicate on their behalf for the purposes of this Memorandum.

13. FACILITATING CONTACT WITH OTHER BODIES

13.1 Each Agency may, in its discretion, refer the other Agency to another body in its jurisdiction where that body is likely to have information or be able to assist the other Agency in respect of a request for information or documents, provided always that body reserves the right to decide whether or not to provide the requested assistance.

14. TERM OF MEMORANDUM

14.1 This Memorandum will have a term of three (3) years, unless terminated in accordance with Clause 17

15. REVIEW OF MEMORANDUM

15.1 The Agencies will keep the operation of this Memorandum under periodic review and will consult with a view to improving its operation or making amendments to give effect to this Memorandum.

15.2 Any term of this Memorandum may be amended or waived by the Agencies' mutual consent in writing.

16 EFFECTIVE DATE OF THIS MEMORANDUM

16.1 This Memorandum will be effective from the date of its signature by the Agencies.

17. TERMINATION OF MEMORANDUM

17.1 Either Agency may terminate this Memorandum before the expiry of the term of three (3) years by giving thirty (30) days written notice to the other Agency. Where an Agency gives such notice, this Memorandum will continue to have effect with respect to all requests for assistance made before the date of the receipt of the notification.

Signed for and on behalf of ACMA

Chris Chapman
Chair

Signed on this 7th day of April 2009

Signed for and on behalf of DIA

Brendan Boyle
Chief Executive

Signed on this 2nd day of April 2009

Annexure A

CONTACT POINTS REFERRED TO IN CLAUSE 7.1 OF THE MEMORANDUM

ACMA

Julia Cornwell McKean
Manager
Anti-Spam Team
Australian Communications and Media Authority

Grant Symons
Executive Manager
Converging Services branch
Australian Communications and Media Authority

DIA

Joe Stewart
Manager
Anti-Spam Compliance Unit
New Zealand Department of Internal Affairs