Information & Communications Technology Authority

Public Consultation on

A Policy for Deep Packet Inspection and Similar Technologies

(Ref: CD 2009-4)

Launch Date: 28 July 2009 **Closing Date: 28 August 2009**

Background

1. The Authority recently became aware that a licensee was planning the introduction of Deep Packet Inspection ("DPI") technology on its network. The use of DPI and similar technologies in other jurisdictions such as the European Union, Canada and the United States has raised concerns about privacy and, quite separately, traffic tiering. These concerns have resulted in a number of regulatory investigations and determinations.

2. As the Authority had not had the opportunity to examine the implications for the Cayman Islands of the introduction of the technology which has been controversial in other jurisdictions, it issued a directive to all telephony licensees on 10 July 2009 prohibiting the installation or implementation of DPI or similar technologies until such time as it could conduct a public consultation and make a determination on the matter.

The Technology

3. All traffic being sent over the Internet, whether it is a web page, a data file, or credit card information, is split up into one or more packets of information. Each packet consists of a header followed by data (sometimes called the body or payload).

4. The packet header contains various information including the IP address of both the sending and receiving computer and is used among other things to route it through the network to its destination. The header can be compared to the address on a traditional postal service envelope.

5. The packet data contains the actual information that is being sent from one computer to the other and is the rough equivalent of the letter that would be concealed within a traditional postal service envelope. In the case of a web page, this would include the URL (the plain text address) of the page being requested or transmitted and the contents of that page.

6. Unless special measures are taken to encrypt the data, (e.g. https protocol or a VPN), the packet contents can be read by any operator in the chain of network connections used by the packet.

7. Until recently only packet headers were examined by network equipment. DPI allows Internet Service Providers ("ISPs") to examine the packet data.

Potential Uses of DPI

8. Traditionally, packet headers are inspected by ISPs for a variety of reasons, including optimization of packet routing, detection of network abuse, and statistical analysis. Such inspection, sometimes referred to as "shallow packet inspection" or SPI gives ISPs access to basic information about Internet traffic, but does not disclose the contents of users' email or web surfing to ISPs.

9. In contrast, DPI provides ISPs with access to the content of all unencrypted Internet traffic that ISP customers send or receive. Since most Internet traffic is unencrypted, DPI enables ISPs to intercept virtually all of their customers' Internet activity, including web surfing data, email, and peer-to-peer downloads. Owing to the volume of traffic on most networks, DPI is usually automated and performed by software based on criteria set by the network operator.

10. After inspecting the contents of users' packers, ISPs can use DPI to perform activities based on filter criteria. DPI can be used, for example, to:

    a. build profiles of consumers for marketing purposes;
    b. intercept communications at the request of law enforcement;
    c. restrict access to selected sites or types of information;
    d. enforce copyright laws;
    e. prioritize the transmission of some packets over others; and
    f. identify computer viruses and spam.

    A more detailed list of potential DPI applications is available at www.dpacket.org/articles/deep-packet-inspection-2009-market-forecast.

Cayman Islands Law

11. Sections 73 and 75 of the Information and Communications Technology Authority Law (2006 Revision) ("the Law") may be relevant. They state:

> 73. ICT service or ICT network providers may, subject to the rules and procedures established under section 72(4)-
>
> (a) refuse to provide an ICT service or an ICT network to a subscriber; or
> (b) discontinue or interrupt the provision of such an ICT service or ICT network to a subscriber pursuant to an agreement with that subscriber,

only on grounds which are reasonable and non-discriminatory, and where any such action is taken, the ICT service or ICT network provider shall, within seven days, provide in writing to the subscriber the reasons therefor.

75. (1) Subject to subsection (2), whoever intentionally intercepts, alters, replicates, monitors or interrupts any message (whether in whole or in part) during its transmission over an ICT network or by means of an ICT service by any means is guilty of an offence and liable, for each such message-

(a) on summary conviction, to a fine of ten thousand dollars;
(b) on conviction on indictment, to a fine of twenty thousand dollars and to imprisonment for two years.

(2) A person shall not be guilty of an offence under this section if-

(a) the message is intercepted, monitored or interrupted in obedience to a warrant or order issued by the Governor;
(b) the message is intercepted, replicated, monitored or interrupted for the purpose of preventing a contravention of section 77;
(c) the person by whom the message is sent or to whom the message is sent has expressly or impliedly consented to the interception, monitoring or interruption;
(d) the message is intercepted, monitored or interrupted by the Authority or on the written instructions of the Authority for purposes connected with the execution of its functions under this Law;
(e) the message is intercepted, monitored or interrupted by the ICT network provider or ICT service provider over whose network or service the message is being transmitted for the purposes of-
(i) providing or billing for that ICT network or ICT service;
(ii) preventing the illegal use of the ICT network or ICT service; or
(iii) preserving the technical integrity of an ICT network or ICT service; or
(f) the message is intended to be received by the public.

12. Sections 73 and 75 of the Law were approved by the Legislative Assembly in 2002 as part of the original statute. At that time, practical DPI technology did not exist, and the Authority understands that the possibility that packet data (as opposed to packet headers) could be examined was not considered.

ICT Licences

13. The confidentiality of customer information is also covered in Section 12 of all ICT licences. It states:

12. PRIVACY AND CONFIDENTIALITY

12.1 The Licensee shall maintain the confidentiality of, and refrain from using or disclosing, unless consent has been given to such use or disclosure by the person entitled to the confidentiality of that information:

(a) any confidential, personal and proprietary information obtained in the course of its business from any Subscriber, where such information originates from any such Subscriber;

(b) any information regarding usage of a Licensed ICT Network or a Licensed ICT Service; or

(c) any information received or obtained as a result of or in connection with the operation of a Licensed ICT Network or the provision of a Licensed ICT Service.

12.2 Notwithstanding Condition 12.1, the Licensee is permitted to use such information to operate its Licensed ICT Networks or Licensed ICT Services, bill and collect charges, protect its rights or property or prevent the fraudulent use of the Licensed ICT Networks or the Licensed ICT Services.

12.3 The Licensee shall establish and implement procedures for maintaining the confidentiality of information subject to this Condition 12.

Benefits of DPI for Network Operators

14. By examining packet flows at detailed levels, ISPs can improve network security and guarantee different levels of service to different customer-types. Network security is improved as system administrators can correlate particular packet exchanges with worm- and virus-like behaviour, and implement measures to automatically quarantine infected devices from the rest of the ISP's network.

15. Different levels of service can be guaranteed by associating particular application-types with particular usage-plans or priority levels. For example, a user on a VoIP plan might have their VoIP packets prioritized, whereas a user with a peer-to-peer plan might have their packets given priority on the network. Alternately, all individuals may be given the same plan, and simply have some packets prioritized and others deprioritized. ISPs in some other jurisdictions have argued that such prioritization of network traffic helps to prevent network congestion and thus improves their service to customers.

16. Information gained from DPI can assist ISPs with network design and their plans for network expansion and the delivery of new and enhanced services.

17. Companies marketing DPI have proposed that ISPs can also enhance their revenue streams by providing targeted advertising and by charging content providers fees to ensure that customers have "priority access" to their services.

Further Reading

18. There are numerous web sites and articles on the Internet that present the case in favour of the use of DPI technologies. Examples include:

    a. Numerous articles on www.dpacket.org

b. Submissions to the Canadian Radio-television and Telecommunications Commission by Bell Canada and Rogers Cable Communications at www.crtc.gc.ca/PartVII/eng/2008/8646/c12_200815400.htm#a2a

Areas of Concern

19. In addition to the question of whether or not the use of DPI is legal under the present provisions of the Law, use of the technology raises two issues that have proved to be controversial in other jurisdictions; personal privacy and "Net Neutrality" or traffic shaping.

Personal Privacy

20. DPI gives ISPs complete access to the content of unencrypted messages passing over its network. The information potentially available to it therefore includes:

    a. Which computing devices are sending and receiving the message.

    b. Which web sites and individual web pages are being accessed.

    c. What operating system and browsers are being used.

    d. What type of transfer is taking place (e.g. ftp, bit-torrent, http, VoIP, streaming video, etc).

    e. The originator and addressees of email messages.

    f. The actual content of the data or files being transferred.

21. Some advocacy groups consider that the use of DPI represents an unacceptable invasion of individual privacy, and that the alleged benefits of DPI are either of no benefit to the end-user or that similar results can be achieved using less invasive methods. They believe that, at the very least, use of DPI should be strictly regulated.

Net Neutrality

22. Net Neutrality is a major policy debate in many jurisdictions. A detailed discussion is beyond the scope of this present consultation. In essence, the debate centres around whether or not network operators should be permitted to vary the bandwidth being provided to customers based upon the protocols or applications that the customer is using (e.g. to throttle bandwidth for peer-to-peer and/or according priority to VoIP applications.) Network operators in other jurisdictions argue this action is appropriate in order to avoid network congestion. Those in favour of Net Neutrality argue that customers purchase a "pipe" from the providers and it should not matter what they pass down that pipe. At the very least, they say,

customers should be provided with sufficient information to decide whether or not to purchase services from a supplier that engages in traffic shaping of different protocols or applications. Alternatively, no traffic shaping should be allowed unless customers opt in for that service.

Further Reading

23. Two of the many sites run by opponents of DPI are www.epic.org and www.nodpi.org.

24. Many privacy issues are described on http://dpi.priv.gc.ca/ .

The Consultation

25. To assist the Authority with its consideration of this issue, the Authority directs licensed ISPs to provide responses with supporting rationale to the following questions. In addition, the Authority invites all stakeholders to provide detailed written comments, with supporting rationale, on the issues identified in questions (e), (f), and (g) below.

For Service Providers only

a. Do you currently employ, or do you plan to employ, DPI or similar technologies on your networks?

b. If the answer to (a) is yes, describe in detail the use you make, or plan to make, of these technologies.

c. Do you currently employ traffic management technology or techniques, other than DPI, such as traffic shaping or traffic throttling, that result in the control of a customer's bandwidth?

d. If the answer to (a) or (c) is yes, describe in detail your Internet Traffic Management Policies.

For All Stakeholders (including the General Public)

e. Do you consider that the use of DPI and similar technologies is permissible under the provisions of sections 73 and 75 of the Law? Please supply rationale.

f. Given that DPI and similar technologies did not exist when the Law was originally approved by the Legislative Assembly, is there now a need to review the provisions of sections 73 and 75? If so, please

detail the changes you would recommend and provide your rationale for these changes.

g. What, if any, measures should be put in place to ensure that DPI is used only for legal purposes?

Further Process

26. The ICT Authority requests written submissions from licensees, other stakeholders and the general public by **28th August 2009**.

27. Written submissions should be forwarded to:

By e-mail to:

consultations@icta.ky

or by post:

The Managing Director
Information and Communications Technology Authority
P.O.Box 2502GT
Grand Cayman
Cayman Islands

or by courier:

The Managing Director
Information and Communications Technology Authority
3rd Floor, Alissta Towers
North Sound Way
Grand Cayman
Cayman Islands

or by fax to:

1-345-945-8284

28. Depending upon the responses received to questions (a) to (g) above, the Authority is may to initiate a further round of questions and responses within this Consultation, or to launch new consultations dealing specifically with privacy and Net Neutrality issues.