PUBLIC CONSULTATION
ON

A POLICY FOR DEEP PACKET INSPECTION AND SIMILAR TECHNOLOGIES

(Ref: CD 2009 – 4)

DIGICEL (CAYMAN) LIMITED RESPONSES TO CONSULTATION

Digicel

The Bigger, Better Network.

August 31, 2009
The ICT Authority (hereinafter called 'the Authority') has issued the ICT Authority Consultative Document CD 2009 – 4 on the Policy for Deep Packet Inspection ('the document') and has asked the operators of telecommunication system within the Cayman Islands several questions on the use and the legality of Deep Packet Inspection (hereinafter referred to as 'DPI'). In particular the Authority has asked the telecommunications providers in the Cayman Islands and other stakeholders the following questions related to the deployment of DPI by Service providers as well as legal questions on sections 73 and 75:

For Service Providers only

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

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

Question (c) Do you currently employ traffic management technology or techniques, other than

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

Question (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.

Question (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.

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

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

Yes, Digicel Cayman uses a limited form of DPI-on the broadband ISP network only.

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

Digicel Cayman only use DPI type technology to protect network integrity (for example to prevent Denial of Service, Zombie, Spambot attacks) and for congestion management purposes.

Question (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?

Digicel doesn't currently use any technology to restrict a customer's bandwidth.

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

Digicel Caymans Traffic Management policy is applied to residential services to allocate bandwidth evenly per customer as part of our fair usage policy. Without such a policy the vast majority of customers would have an inferior broadband experience (specifically Web Browsing, VoIP, Streaming etc) due to bandwidth hungry applications such as Peer2Peer, Denial of Service, Spam etc.

Legal opinion pursuant to ICT Authority Consultative Document CD 2009 – 4

Policy for Deep Packet Inspection

Question (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.

The relevant sections of The Information and Communications Technology Authority Law (2006 Revision) (hereafter referred to as "the Law") have been set out completely in the Document and need not be repeated here.

Section 73 allows the ICT network provider (Digicel (Cayman) Limited which operates a telecommunications service in the Cayman Islands, to refuse to provide ICT services (the service(s)) to a subscriber, or having commenced the provision of the services, allows the provider to discontinue or interrupt the service provided to its subscriber pursuant to the agreement between provider and subscriber.

The section however requires the decision of the provider to be reasonable and non-discriminatory and all decisions shall be communicated in writing to the subscriber or applicant for the service.

A provider may wish to make the acceptance by the subscriber or the applicant for service, of the use of DPI or similar technologies on the network, a precondition to the provision or continuation of service. The question therefore raised by this section is whether or not to do so is reasonable or non-discriminatory.

DPI and its use is a new development in the telecommunications industry. It is a computer networking term referring to devices and any similar technologies that inspect and take action on the contents of the data packet being moved over the provider's network (the payload) rather than just the packet header.

Does DPI as we understand it offend Section 73 of the Law?

In the delivery of voice services, confidential subscriber information is constantly and legitimately captured. On every provider's network the usual CDR information recorded includes the location of the subscriber which is registered on the network automatically. Shallow packet inspection has been a feature of this technology and service as recognized by the Authority and for good reason. It is required in network management for fraud detection and security, traffic management and network analysis. With the increase in cybercrimes and the complexity of third party intrusion on internet traffic and the electronic movement of data, there is an even greater need for stringent monitoring of the service not only to prevent attacks on the subscriber's use of the service but also to safeguard the provider's network. DPI only offers a greater and real time monitoring of the network's traffic usage to meet the ever increasing risk to the service. Whilst DPI allows the provider the potential to drill down past the packet header type of subscriber information and see the contents of the subscriber's communication, the value to the provider and the subscriber in prevention of fraudulent attacks on both, justifies the use of DPI as a precondition to the provision of the service. It is certainly not so offensive a precondition as to make it unavailable to the provider within the limits of Section 73.

Additionally where DPI is to be used for traffic management and bandwidth allocation, it has been endorsed as a reasonable practice by the Canadian Radio television Telecommunications Commission in a decision August 12, 2009, CRTC-484. There the CRTC was asked by Bell Canada if it could:

(i) create two speed options for its Gateway Access Service (GAS) Residence and Business consumers
(ii) institute a usage based billing rate
(iii) impose an excessive usage charge for GAS

and not apply them uniformly across the board to all its customers. The CRTC answered yes to all the above and held that the uneven application to their customers was discriminatory but not unjustly discriminatory. This was consistent with the opinion of the tribunal in Telecoms Decision 2006-77-CRTC where it was considered acceptable that carriers should be able to manage the potential negative outcome of high consuming bandwidth end-users in a manner that does not degrade the quality of service to end users.

These decisions support the use of DPI as a tool to manage traffic and bandwidth allocation in order to improve the efficient delivery of the service to the market within the directive of the Law. None of the three requests of Bell Canada in Decision CRTC-484 could have been accommodated without the explicit and aggressive use of DPI. By approving the requests, CRTC was clearly endorsing the use of DPI in traffic management. In respect of the imposition of the excessive usage charge Bell Canada argued that this allowed the customer to match his level of usage to his willingness to pay for the usage a position accepted by CRTC which went further to say the customer should simply be given time to adjust to the idea and the charge. The decisions recognize the validity of the argument that to make its use a precondition to the delivery of the service is neither unreasonable nor discriminatory.

Does DPI offend section 75 of the Law?

Section 75 prohibits the intentional interception, alteration; replication and monitoring of any messages sent by a subscriber over the service and makes it an offence for the provider to do so. DPI admittedly can be used to do all of the above. However the mere fact that it has the potential for an illegal use does not make the use of DPI without more an illegality. Further there are many layers to which DPI can be applied (from Layer 2 to Layer 7) where DPI may but does not automatically intercept the actual messages sent across the Internet. What the regulator and the public ought to understand is that the particular form of DPI can possess a capability which must be specifically deployed into action and without deliberate activation, does not automatically seek out, intercept or monitor packet data. This can and should only be done where it is clearly with the subscriber's consent or authorized by the Law.

This section offers the provider several real defences to allegations of illegal use of DPI. The crime fighting applications of DPI are properly allowed under sub-section 2 and where the Authority wishes the interception, alteration, replication and monitoring of messages, and DPI technology is used to accomplish this, nothing illegal is committed. Similarly where Digicel's subscribers are required as part of the contract for services, to agree to the use of DPI for traffic management, then Digicel's use of DPI does not offend this section.

Under section 75(2)(e) however any use of DPI to intercept, monitor or interrupt the ICT service 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;

is not an offence under the Law. We respectfully submit that, all our uses to date of DPI and any similar technologies are designed wholly and solely to accomplish the above. In the main, this is substantially the role of DPI in any network. We also submit that the use of DPI for traffic control and bandwidth allocation fall within Section 75(2)(e)(iii). In the alternative we submit that the conventional and persuasive wisdom of the CRTC in Decision CRTC 2009-484, suggests that this purpose is acceptable to achieve the policy objective of the Telecommunications Act where the policy objective much like the Law, is to achieve the efficient provision of an ICT service.

The use of DPI to inspect messages under warrant from the Governor (s75(2)(a)), to intercept, monitor or interrupt messages for preventing contravention of section 77, (s75(2)(b), to inspect messages on the subscriber's consent(s75(2)(c) or on the Authority's direction (75(2)(d) are protected. **In BellCanada/Bell Sympatico use of DPI PIPEDA Complaint In Re 2008 1LRWeb (P&F) 1808,** (**the BellCanada Case)** a complaint was brought against Bell Canada for the use of a new DPI application, the Ellacoya e100. This application was employed by Bell on the basis that it offered network optimization. The complainant argued that this amount of personal intrusion by the Ellacoya e100 was not necessary to affect the stated purpose. However the regulator did not find favour with this objection and directed that Bell could and should change its service agreement and its FAQ's to notify the subscriber that it intends to collect and retain the subscriber's personal information through the use of DPI. It is our view therefore that where the use of DPI does not fall within the approved purpose in section 75(2)(e) of the Law, the provider may nonetheless satisfy the provisions of the Law by declaring its use and purpose through the terms and conditions of the Service Agreement thus bringing the provider within the defence offered by section 75(2)(c).

Digicel must intentionally carry out the acts set out in section 75(1). Where DPI is set as a critical feature of the safe and efficient and normal provision of the ICT services, taking into account advances in technology, it is not correct to say Digicel intentionally intercepts, interrupts or monitors. (This may not be the case where DPI 'alters,' or ' replicates' the message.). This interception and monitoring is conducted as a standard behaviour of the DPI application in its effort to carry out the legitimate functions of Digicel specifically recognized in 75(2)(e). Where the interception, or monitoring is an ordinary incident to the provision of telecommunications services then it is arguably not intentional in the true sense of the word.

We are of the view therefore that the use of DPI does not offend either section 73 or 75 of the Law.

Question (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.

The sections in our view require no further amendment to deal with DPI. The Law provides for an offence if DPI is used illegally. All providers should be able to institute its use within the confines of sections 12, 73 and 75. Digicel can see no problems complying with the Law as it currently exists or envisions any mischief which cannot be so contained. Section 12 makes it clear that any information captured by DPI within section 75(2)(e) must be properly safeguarded in the same way as we safeguard all other confidential data currently captured. Section 12 is consistent with Section 75(2)(e) which specifically allows the provider to use the confidential information which is caught in section 75(2)(e), to operate its networks and to protect its rights, property and to prevent fraud. This is a major function of DPI. Information captured by DPI must be protected through the establishment and implementation of procedures for maintaining its confidentiality. In this regard the Law gives the Authority the power to direct and or guide the provider as it sees fit in the establishment of these said procedures which ultimately recognises and protects the subscriber's privacy. It is important to note that at present all providers under the watchful eye of the regulator, efficiently and effectively protect from unauthorized disclosure a substantial amount of subscriber data for voice as are registered on the CDRs.

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

This requires all the stakeholders to give full and complete details on the capabilities of the DPI applied and the rationale for application. In this regard, the public education by the Authority is a vital part of the monitoring of the use of DPI.

Where the Authority can in consultation with the stakeholders in the industry, set appropriate benchmarks for the layer of inspection in DPI reasonably required to satisfy the operator's legitimate functions as set out in the Law and at the same time to establish and help maintain proper data protection processes for the data captured, then there will be a balance of the subscriber's right to privacy and confidentiality under section 12 of the Law, with the provider's right to manage its traffic, protect the integrity of its systems, and carry out network analysis to improve the efficiency of its service.