# SECOND RESPONSE TO ICTA's CONSULTATION

# ON

# 'A POLICY FOR DEEP PACKET INSPECTION AND SIMILAR TECHNOLOGIES'

## (Ref: CD 2009-4)

**July 28, 2009**

By e-mail to: consultations@icta.ky

September 28, 2009

Landline | Internet | Mobile | Entertainment

## INTRODUCTION

Cable and Wireless (Cayman Islands) Limited, trading as LIME ("**LIME**") is pleased to provide the following submissions in response to the Authority's 28 July 2009 "Public Consultation on A Policy for Deep packet Inspection and Similar Technologies" ("**CD 2009-4**"), as amended by the Authority's 13 August 2009 letter. In accordance with the Authority's instructions, LIME responded to questions a to d at paragraph 25 of CD 2009-4 on August 28, 2009. In that response, LIME indicated that it does not currently employ Deep Packet Inspection ("**DPI**") technologies on its network but that it had formulated plans to implement DPI to facilitate:

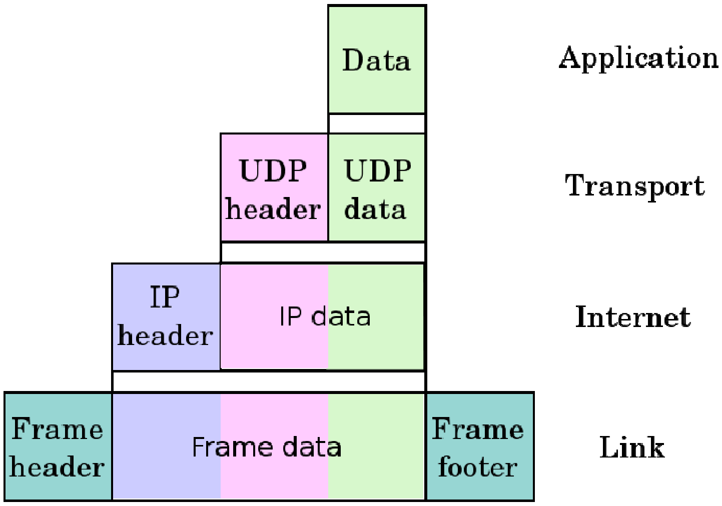
- Enforcement of agreement with customers for the delivery of download speeds and usage.
- Better understanding of the IP traffic profile of the Internet backbone.
- More effective routing of traffic on LIME's Internet network.
- Assistance in the development of customized services and billing.
- Protecting the network and the service quality offered from exposure to security threats.

In this submission, LIME will describe DPI, address the context for the deliberations on DPI, and then answer the Authority's questions e through f at paragraph 25 of CD 2009-4.

## WHAT IS DPI?

DPI is the foremost technology for identifying and authenticating protocols and applications conveyed by IP across the network of an Internet Service Provider ("**ISP**"). DPI provides real time analysis of IP network usage and consequently allows ISPs to optimize network performance in real time.[1]

As the Authority is aware, an Internet Protocol packet consists of a series of stacked layers, where the "data" of one layer is the "header" and "data" of the next layer. The following diagram[2] represents this.



Each header is in turn broken down into a number of fields. "Traditional" routing of packets inspects the "Source Address" and "Destination Address" fields in the "IP Header" portion of the packet in order to decide where to next route the packet.

DPI allows for inspection of other parts of the packet, including other fields in the IP Header, other headers, or, in its most intrusive form, the customer's "Data" itself.[3] It is this most intrusive form of "inspection" that has caused the most public policy concerns. The focus of many of the comments from the non-Licensee interested parties in this proceeding

[1] Pg. 1, https://www.dpacket.org/articles/deep-packet-inspection-2009-market-forecast
Pgs. 1, 2, https://www.dpacket.org/articles/digging-deeper-deep-packet-inspection-dpi

[2] Available at http://upload.wikimedia.org/wikipedia/commons/3/3b/UDP_encapsulation.svg, and licensed under the Creative Commons Attribution ShareAlike 3.0 licence.

[3] A useful description of the different levels of inspection is available on the website of the Office of the Privacy Commissioner of Canada, at http://dpi.priv.gc.ca/index.php/essays/deep-packet-inspection-its-nature-and-implications/.

bear this out. LIME notes, however, that some customers encrypt their messages. This protects the privacy of their "content" in the "Data" portion of the packet.

However, as the Authority has recognized in CD 2009-4, DPI technology also has many benefits and these benefits, defined in Table 1 below, should not be discarded simply because a technology might be misused.

**Table 1**[4]

| Application | Details |
|---|---|
| Security | DPI is used increasingly to underpin security applications and to fight spam, phishing, distributed denial of service (DDoS) attacks, botnets, viruses, and other threats. |
| Lawful Intercept | The Communications Assistance for Law Enforcement Act (CALEA) and its equivalents in countries other than the U.S. require operators to ensure that security services can use equipment for surveillance. DPI is needed to do this in a VoIP environment. |
| Traffic Monitoring | As DPI's origin, traffic monitoring was, and still is, used to help operators understand what is happening in their networks and to see which applications are using bandwidth. |
| Traffic Management | Operators' next move was to use DPI to throttle, block, or shape traffic at a macro or application level, to control the impact of bandwidth-hungry applications such as P2P. |
| Peering Control | An extension of traffic management, giving carriers better control over the traffic that they are sending out over peering points, and hence better control over costs. Carriers in emerging markets are seeking to manage down the peering costs, which, by virtue of traffic flow balances, have always favored operators in the U.S. and Europe. In addition, the generation of outbound traffic by users not on an operator's network (e.g., via P2P protocols grabbing content) has become a significant issue. |
| QoS Assurance | By enabling packet-level tagging and prioritization based on an understanding of what a packet is, where it has come from, and where it is going, DPI is now used to assure the QoS for different applications on an application, service, or customer basis. |
| Provision of Tiered Services | The next logical step if you can manage QoS at a granular level is to monetize that ability, which operators are doing by offering tiered services. |
| Customized Pricing & Billing | Provision of customer-, service-, and application-based pricing packages. For instance, offering customers the ability to subscribe to premium-priced gaming services, where their personal gaming traffic is prioritized through the network. |
| Event-Based Billing & Traceability | Understanding what packets pertain to which data streams is important for knowing how much data has been used and what should be billed. For instance, if customers buy and download a large video (such as a film) from |

[4] https://www.dpacket.org/articles/deep-packet-inspection-2009-market-forecast

| | |
|---|---|
| | a service provider's online shop, they might reasonably expect that traffic to be excluded from their fair usage allowance. |
| Content Enrichment | Adds data to packet headers to determine how data streams are treated – or in some cases, what sort of stream might be sent. Operators might use this to vary the format of content according to the capabilities of the receiving device (e.g., mobile phone vs. PC). |
| Advertising | Vendors acknowledge that there is a lot of regulatory and public scrutiny of this area, and that the development of services must move forward in the proper manner. The publicly acceptable face of this is asking customers to take reduced-rate services in return for receiving advertising tailored to their application and content usage. |
| Ad Tracking | This application monitors the effectiveness of online ads and measures to what extent marketing campaigns are influencing online behavior. |
| Parental & Network-Based Control | Many parental-control solutions are now linked to DPI, enabling much finer granularity of content filtering. A network-based extension would block certain undesirable URLs or Websites altogether (e.g., if they provide access to illegal content), irrespective of whether parental control applications have been used. |
| Digital Rights Management (DRM) | In some countries, legal frameworks may create an environment that will effectively compel DPI deployment to enable DRM enforcement. This would enable filtering of content to analyze whether it has been copied. |
| Customer Customizable Managed Services | DPI capabilities are being extended beyond the operator. For instance, new solutions enable wholesalers to give their Internet service provider (ISP) customers the ability to offer customized DPI-based solutions to their own end customers. They also enable service providers to give their enterprise customers DPI-based portals to manage their own IP-VPN traffic, based on a deeper insight of what is happening. |

## FURTHER SUPPORT FOR DPI TECHNOLOGY

As operators across the world deploy 3G networks, it has become apparent that DPI is a key requirement for managing consumer needs and a plethora of applications. This is primarily based on three business drivers, "improved efficiency, delivering a better product and increasing revenue[5]. The case for DPI in 3G networks shows that DPI is required to ensure that the limited radio frequencies are managed in such a way that capital expenditure and operational costs can be reduced.

Secondly DPI is a key requirement to ensure that mobile operators are able to provide an acceptable customer experience. Increasing network capacity will not solve the problem where for example P2P and video demand a constant bandwidth as opposed to the typical

[5] 3G and LTE Need DPI – http:/www.xchangemag.com, Karle Wale

‘bursty’ nature of IP usage. DPI is required to provide real-time intelligence and it allows the service provider to then take rules-based decisions to best manage its traffic. This is a major issue for 3G operators and if the functionality of DPI is significantly constrained by the regulator, it is likely to result in poor customer experience and increased churn.

From the perspective of a service provider, DPI is essential to support current business needs and when considering the limited frequencies in the mobile spectrum, it becomes even more critical to an operators ability to deploy a network that offers customers a sustainable and high-performance service on a scalable infrastructure.

## CONTEXT FOR DELIBERATIONS ON DPI

### The Authority’s Directive

In its directive, dated July 10, 2009, the Authority gave the following basis for prohibiting the installation of DPI and similar technologies until a determination is made following this proceeding:

- DPI and similar technologies are highly controversial and are currently the subject of regulatory investigation in the EU and Canada.

- Use of DPI and similar technologies arguably breaches the provisions of section 7 of the ICTA Law.

Neither of these two reasons demonstrates there is an issue that needs to be addressed in the Cayman Islands. While the fact that the technology has been controversial overseas and the fact that there is a need to interpret the Law are valid reasons for conducting a public consultation, they are not valid reasons for issuing a directive to licensees.

In addition, it became apparent from their 28 August 2009 submissions that Digicel Cayman Limited and WestTel Limited have already implemented DPI in their networks. The directive, however, did not apply to those two companies, as it applied only prospectively.

Further, while there is no evidence on the public record regarding how long these companies had implemented DPI, LIME was not aware of any person raising any issues or suggesting that licensees were in any way behaving improperly prior to the Authority's directive. LIME believes that, had the directive been based upon a thorough examination of all of the facts and issues, instead of improper considerations such as controversy in other countries, it is likely that a different and more considered directive would have been issued.

## DPI in Canada and US

In both the United States of America ("**US**") and Canada there were events that precipitated the examination of DPI and the attendant issues. In both cases the issue was not about DPI, the technology but about reasonable/ unreasonable network practices.

In the case of Bell Canada, the summary and conclusion of the matter is:

> On 3 April 2008, the Canadian Association of Internet Providers (CAIP) filed an application with the Commission requesting certain orders directing Bell Canada to cease and desist from throttling Internet traffic generated by peer-to-peer (P2P) file-sharing applications on its wholesale ADSL access service known as Gateway Access Service (GAS). In Telecom Decision 2008-108, in response to the application from CAIP, the Commission determined that, based on the record of that proceeding, Bell Canada's application of its traffic-shaping measures to GAS were not in violation of the Act, and it therefore denied CAIP's application[6].

In the case of Comcast in the US, a formal complaint was made to the Federal Communications Commission ("**FCC**") by Free Press and Public Knowledge against Comcast Corporation, alleging that Comcast was secretly degrading peer-to-peer applications, and seeking a declaratory ruling from the FCC that Comcast's actions were in

[6] Paragraph 6, Telecom Public Notice CRTC 2008-19, Notice of Consultation and Hearing, Review of Internet Traffic Management Practices of Internet Service Providers. http://www.crtc.gc.ca/eng/archive/2008/pt2008-19.htm

violation of the FCC Internet Policy and did not conform to 'reasonable network management'.

In the 'Comcast Order' the FCC said that[7] :

> We consider whether Comcast, a provider of broadband Internet access over cable lines, may selectively target and interfere with connections of peer-to-peer (P2P) applications under the facts of this case. Although Comcast asserts that its conduct is necessary to ease network congestion, we conclude that the company's discriminatory and arbitrary practice unduly squelches the dynamic benefits of an open and accessible Internet and does not constitute reasonable network management. Moreover, Comcast's failure to disclose the company's practice to its customers has compounded the harm.

While the FCC did find that Comcast Internet network management practices were unreasonable, it is to be noted that the decision was made on:

- the specific facts of the Comcast case and was not a general ruling on Internet / network traffic management.

- the fact that Comcast was found to have used a method known as injecting "reset [8]packets" into P2P communications to interrupt them. This practice was found not merely to delay P2P file transfers, but to terminate them completely. The FCC concluded that Comcast's practice was not minimally invasive because it was not limited to periods of congestion nor to geographic areas actually experiencing congestion.

[7] Pgs. 24, TELUS Comments on Telecom Public Notice CRTC 2008-19, Review of Internet Traffic Management Practices of Internet Service Providers. http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1029656.pdf

[8] Pgs. 24, TELUS Comments on Telecom Public Notice CRTC 2008-19, Review of Internet Traffic Management Practices of Internet Service Providers. http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1029656.pdf

In both the Bell Canada and Comcast proceedings, it was recognized that ISPs need to manage their network and the issues revolved around the compliance with legislation and reasonableness.

### DPI in the UK

BT in the UK stepped away from a partnership that was intended to target advertising to its customers based on their Internet behaviour. Apart from this matter there has not been much further discussion of DPI in the UK.

## RESPONSES TO THE AUTHORITY'S QUESTIONS

The Authority asked all stakeholders to respond to the following questions at paragraph 25 of the Consultative Document:

### 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.

### LIME's Response

Yes. The use of DPI is permissible under sections 73 and 75 of the Law.

LIME agrees with the comments filed by Walkers on 28 August 2009 that section 73 is not particularly germane here. Section 73 appears to address a refusal to provide service or a decision to discontinue or interrupt the provision of service to a particular customer. Nevertheless, section 73 allows a licensee to discontinue or to interrupt a service in accordance with terms of the contract with the customer. DPI can be one of the tools used by licensees to enforce the terms of their retail contracts.

It is clear that the intent of section 75 of the Law is to protect the privacy of customers' information. Within that context, however, it is recognized that there may be legitimate reasons for intercepting, replicating, monitoring or interrupting a message.

Inter alia, the Law holds LIME blameless of an offence where:

> 75 (2) (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.*

LIME had stated in its response of 28 August 2009 that among its objectives for deploying DPI are:

- Customised services and billing.

- Protecting the network and the service quality offered from exposure to security threats.

LIME's interpretation of the Law then is that, should it choose to use DPI for one of the purposes set out in subsection 75(2) of the Law, it would be in compliance with the Law. LIME could not customize and bill services today in the manner facilitated by DPI, nor can it preserve the integrity of its network in real time, without the use of DPI.

**Question F**

Given that DPI and other 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.

**LIME's Response**

LIME is of the view that the Law does not need to be amended. The Law is not about governing technologies but about establishing a framework of principles which create the legal framework governing the use of technologies. These principles are independent of technology and the issues raised by DPI and similar technologies have not defeated the provisions of the law as to require a review of section 75.

LIME notes that the Internet existed at the time this provision was originally enacted in 2002. Further, the operation of the Internet in 2002 involved investigating the header of the packet to determine the destination of the packet. Based on the definition of "message" in the Law, this could be construed as "monitoring" the messages of a customer. However, at no time has any person suggested that providing Internet services is a breach of section 75 of the Law. As we noted earlier, the primary purpose of section 75 is to protect the confidentiality and privacy of customers' information. A purposive interpretation of the Law would suggest that looking at the fields in the header of IP packets, whether these are the fields traditionally reviewed by Internet routers or the additional fields reviewed by DPI technologies, is not a breach of the Law, as none of these activities involve the "data" created by the customer.

**Question G**

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

LIME's Response

> LIME is of the view that the penalties established under section 75(1) of the Law for illegal intentional interception, alteration, replication, monitoring or interruption of messages should suffice.

## CLOSING REMARKS

Please send any communication in relation to this consultation to:

Melesia Sutherland Campbell  
melesia.Campbell@time4lime.com  
876 936 2860 (O)  
876 919 1731 (M)  
876 511 7874 (F)

Frans Vandendries  
frans.vandendries@time4lime.com .  
345 747 3644 (O)

345 916 0831 (M)

345 949 1876 (F)

**END**