# ICT Decision 2010-4

Grand Cayman, 23 March 2010

## Decision on Deep Packet Inspection and Similar Technologies in the Cayman Islands

***Overview***

*In this decision, the Authority determines that Digicel and WestTel's current uses of Deep Packet Inspection (DPI) are in breach of clause 12 of their respective ICT licences. Similarly, the Authority considers that LIME's proposed uses of DPI would be in breach of clause 12. Therefore, the Authority directs Digicel, LIME and WestTel to take steps to comply with clause 12 of their licences. The Authority believes that at least some uses of DPI are counter to the provisions of the Information and Communications Technology Authority Law and/or the Confidential Relationships (Preservation) Law. However, the Authority recognizes that a final determination is a matter for the courts rather than the Authority. The Authority also recommends that changes be made to the ICTA Law in order to significantly restrict the use of DPI in the Cayman Islands.*

(Note: This overview is provided for the convenience of the reader and does not constitute part of the Decision. For details and reasons for the conclusions, the reader is referred to the various parts of the Decision.)

## Background

1. On 10 July 2009 the Information and Communications Technology Authority ("the Authority") became aware that a licensee was planning to introduce Deep Packet Inspection ("DPI") technology on its network. As the Authority had not had the opportunity to examine the implications for the Cayman Islands of the introduction of DPI, it issued an immediate directive to all telephony licensees prohibiting the installation or implementation of DPI or similar technologies until such time as it could make a determination on the matter.

2. In that directive, the Authority noted that the use of DPI and similar technologies for public network traffic raises a number of significant public policy issues and, in the Cayman Islands, arguably breaches the provisions of section 75 (prohibition on the interception of messages) of the Information and Communications Technology Authority Law (2006 Revision) ("ICTA Law"). The Authority also noted that it would initiate a public proceeding on this topic, following which it would make a decision on the acceptability of the use of DPI or similar technologies in the Cayman Islands.

## Process

3. On 23 July 2009 the Authority launched a public consultation on the policy for DPI and similar technologies. The purpose of this public proceeding was to assess whether the use of DPI and similar technologies is legal under the ICTA Law and to evaluate its impact on personal privacy and "net neutrality".

4. The consultation document sought comment from Internet Service Providers ("ISPs") on the following questions:

    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.

5. From all stakeholders (including the General Public) the consultation document sought comment on the following questions:

    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?

6. The Authority received comments from four ISPs: Cable & Wireless (Cayman Islands) Ltd. ("LIME"), Digicel Cayman Ltd. ("Digicel"), TeleCayman Ltd. ("TeleCayman") and WestTel Ltd. ("WestTel"). Comments were also received from the following stakeholders: Appleby, BitTorrent Inc. ("BitTorrent"), Cayman Christian TV Ltd. ("CCTV"), Deloitte & Touche ("Deloitte"), dms Broadcasting ("dms"), Walkers, Niels Maybin, N.A. Pappadakis, Christopher Rose and John Stevenson.

7. Collectively, the comments received by the Authority offer both support for, and opposition to, the use of DPI and similar technologies. In the following section, the submissions received from ISPs regarding questions (a) through (d) are summarised. This is followed by a section summarising the salient points made by each party to questions (e) through (f).

***Questions (a) – (d)***

8. LIME submitted that it does not currently employ DPI on its networks in the Cayman Islands, but that it intends to do so in the near future. LIME noted that it intends to use DPI for the following purposes:

- Enforcement of agreements with customers with respect to download speeds and usage.
- Obtaining a better understanding of the IP traffic profile of its Internet backbone.
- More effective routing of traffic on its Internet network.
- Assisting in the development of customized services and billing.
- Protecting the network and the service quality offered from exposure to security threats.

9. LIME also noted that it already has taken steps to restrict its customers' bandwidth to the bandwidth of the package for which the customers pay, irrespective of the bandwidth available on the physical connection to the customer. For example, if a customer has an Asymmetric Digital Subscriber Line ("ADSL") connection that would permit 1MB/s bandwidth, but has only purchased a 256KB/s package, the bandwidth capacity for this customer is restricted to 256KB/s. LIME also mentioned that it employs selective routing on its Internet links to ensure that the Direct Internet Access ("DIA") traffic is always routed on the faster Internet links. This ensures that DIA customers will be the last to experience delays should a link or several links become congested or unavailable.

10. Digicel submitted that it uses a limited form of DPI on its broadband network to protect network integrity (for example to prevent denial of service, zombie and spambot attacks) and for congestion management purposes. Digicel stressed that it does not use any technology to restrict a customer's bandwidth, but does apply its traffic management policy to residential services to allocate bandwidth evenly among customers as part of its fair usage policy.

11. TeleCayman noted that it does not use DPI, does not have plans on employing DPI or similar technologies nor does it employ traffic management technology or techniques such as traffic shaping or traffic throttling.

12. WestTel confirmed that it employs equipment to manage its traffic loads efficiently and ensure that the majority of its customers experience expected bandwidth. WestTel noted that the bandwidth allocated to Peer-to-Peer ("P2P") usage for residential customers is limited to 4 to 12 KB/s upstream and 8 to 150 KB/s downstream. Among corporate customers, this equipment is only used upon request if a corporate customer wishes to manage its internal traffic in a more efficient manner.

***Questions (e) – (f)***

13. Appleby submitted that the very purpose of DPI is to monitor communications. As a result, in Appleby's view, the use of DPI is prohibited by section 75(1) of the ICTA Law. According to Appleby, the exceptions to the general prohibition set out in section 75(2) would not apply where an ISP is seeking to build profiles of consumers for marketing purposes or to prioritise the transmission of some packets over others.

14. Appleby submitted that the ICTA Law was never intended to apply only to the technologies available at the time it was drafted. In Appleby's view, the intent of the ICTA Law is to treat the transmission of data over the Internet in a similar manner as the sending of traditional letters. Since the Cayman Islands Post Office is not allowed to open letters and treat them differently according to the type of correspondence they contain, neither should the ISPs. Appleby argued that if DPI had been available at the time the ICTA Law was passed, the legislature would not have permitted its use.

15. Appleby recommended that sections 73 and 75 of the Law be amended so as to expressly prohibit the use of DPI for any purpose whatsoever, considering that: (*i*) the use of DPI would have a potentially detrimental impact on the confidentiality of communications sent to and from Cayman; (*ii*) it would never be possible to completely remove the risk that an experienced hacker, or a rogue employee at an ISP, might access and use the data for his or her own purposes; and (*iii*) the introduction of DPI is not necessary in order to enable law enforcement authorities to obtain information that they genuinely need to discharge their functions: they have sufficient powers already to obtain evidence from senders or recipients of data, by means of search warrants and the like. In Appleby's view, if the Authority decides to permit DPI, it should only be permitted for law enforcement purposes and not for any regular or routine commercial use by the ISP.

16. BitTorrent, a U.S. corporation that develops peer-assisted Internet content delivery technology based on the BitTorrent protocol (a peer-to-peer file sharing protocol predominantly used for distributing large amounts of data), noted that DPI raises significant privacy concerns given its capabilities and tendency to be used to block, delay, degrade or throttle a particular protocol or application in violation of network neutrality principles. However, it recognized that there are positive uses of DPI as well.

17. BitTorrent submitted that the Internet requires neutral network management that will preserve the power and incentives around innovation. While BitTorrent recognized that network management is essential to the preservation of Internet-based business models, it noted that these management practices are not required to be, nor should they be, discriminatory in nature. According to BitTorrent, discriminatory network management has the potential to stifle existing technologies in their infancy as well as new technology development.

18. dms stated that it does not consider the use of DPI or similar technologies to be permissible under the provisions of section 73 and 75 of the ICTA Law. However, dms submitted that it may be beneficial to amend the ICTA Law to ensure that it reflects the intricacies of DPI and other technologies. Accordingly, dms recommended that the ICTA Law be amended to outline the specific uses of DPI which are permissible.

19. Digicel submitted that DPI enables an ISP to monitor network traffic usage in real time to meet the ever increasing risk to the services provided. According to Digicel, 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 and it is not so offensive a precondition as to make it unavailable to the provider within the limits of section 73.

20. Digicel acknowledged that DPI can be used to carry out intentional interception, alteration, replication and monitoring of any messages sent by a subscriber, but it noted that it does not use DPI for these purposes. Rather, Digicel uses this technology to carry out the legitimate functions set out in section 75(2)(e). According to Digicel where the interception, or monitoring is incidental to the provision of telecommunications services then it is arguably not intentional in the true sense of the word.

21. Digicel argued that no amendments to section 73 and 75 of the ICTA Law are needed to deal with DPI. All providers should be able to use DPI within the confines of sections 12, 73 and 75 of the ICTA Law. Digicel noted that it can see no problems complying with the ICTA Law as it currently exists or envisions any mischief which cannot be so contained. Digicel considered that 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 Digicel safeguards all other confidential data currently captured.

22. Regarding measures that should be put in place to ensure that DPI is used only for legal purposes, Digicel submitted that this requires all stakeholders to give full and complete details on the capabilities of the DPI applied and the rationale for its application. In Digicel's view, a balance must be struck between the subscriber's right to privacy and confidentiality and 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. This may be achieved by setting appropriate benchmarks for the layer of inspection in DPI.

23. LIME submitted that DPI is required in 3G networks to ensure that the limited radio frequencies are managed in such a way that capital expenditure and operational costs can be reduced. Further, according to LIME, DPI is required to ensure that mobile operators are able to provide an acceptable customer experience. In the case where the functionality of DPI is significantly constrained by the regulator, LIME noted that it is likely to result in poor customer experience and increased churn for 3G networks.

24. LIME stated that use of DPI and similar technologies is permissible under the provisions of sections 73 and 75 of the ICTA Law. Section 73 allows a licensee to discontinue or to interrupt a service in accordance with terms of the contract with the customer. In LIME's view, DPI can be one of the tools used by licensees to enforce the terms of their retail contracts. LIME noted that the intent of section 75 of the ICTA Law is to protect the privacy of customers' information. Within that context, however, it recognized that there may be legitimate reasons for intercepting, replicating, monitoring or interrupting a message. LIME's interpretation of the ICTA Law is that, should it choose to use DPI for one of the purposes set out in section 75(2), it would be in compliance with the ICTA Law.

25. LIME was also of the view that the ICTA Law does not need to be amended. It submitted that the ICTA 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.

26. LIME submitted that a purposive interpretation of the ICTA 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 ICTA Law, as none of these activities involve the "data" created by the customer.

27. Finally, LIME was of the view that the penalties established under section 75(1) of the ICTA Law for illegal intentional interception, alteration, replication, monitoring or interruption of messages should suffice to ensure that DPI is used only for legal purposes.

28. Neil Maybin stressed that DPI technologies present a significant threat to the individual and commercial privacy and integrity of Internet communications. In his view, the use of DPI should be of particular concern to the financial sector. Mr Maybin noted that experience in the UK suggests that while existing laws could be applied to prevent nonessential DPI (such as DPI for targeted advertising), several factors prevent them from being enforced. In Mr Maybin's view new provisions are needed which expressly prohibit all DPI except for very specific exceptions such as state surveillance.

29. Mr Maybin recommended that section 75(2)(c) of the ICTA Law be changed to require the consent of both parties and remove the concept of implied consent. In addition, he recommended that the ICTA Law include further provisions covering ISPs and DPI, specifically that ISPs may: (*i*) only read header data and they must only use this information internally for specified purposes such as network optimisation and security; and (*ii*) never read packet data or provide it, or a digest of it, to any third party. In his view, only government bodies should have access to both header data and packet data and then solely for the purposes of state surveillance and crime prevention acting under appropriate warrants.

30. N.A. Pappadakis argued that DPI is intrusive and uncalled for. In his view, customers buy the use of a "pipe" and the traffic going through this pipe should not be available to others. He noted that privacy should be guaranteed and is better served by the ICTA Law as it stands at present.

31. Chris Rose noted that DPI and related technologies could not have been within the contemplation of those drafting the ICTA Law or the legislators who enacted it as these technologies have the potential to undermine privacy. According to Mr Rose, the present wording of the ICTA Law should be updated to clarify the use of DPI and related technologies. In his view, the Authority should consider The Computer Misuse Law, 2000, and in particular section 3 which prohibits unauthorized access to computer material. He also recommended that the Authority consider Article 8 of the European Convention on Human Rights, which states that an act or a failure to act by a public authority, including the ICTA, which deprives a person of the privacy of his or her communications may constitute a contravention of that Convention. Mr Rose further noted that section 9(1) of the Cayman Islands Constitution 2009 also provides for government respect for privacy in "correspondence" which is likely to be construed as including electronic communications.

32. Mr Rose recommended that an amendment of the ICTA Law should be broad in scope and generic in nature, rather than technology specific. In his view, it should be required that any technology which might compromise the right to privacy in communications only be deployed with the prior written consent of the Authority.

33. Walkers argued that section 73 is not directly relevant to the question of whether the use of DPI and/or similar technologies is permissible. However, it noted that section 73 may become relevant if a provider refuses to provide a service or network to a subscriber that objects to the use of DPI. In those circumstances, Walkers anticipates that a provider would seek to argue that such refusal is reasonable and non-discriminatory because there is no express prohibition against the use of DPI and/or similar technologies under the current ICTA Law.

34. Walkers further submitted that the use of DPI and/or similar technologies may be permissible under the exceptions set out in section 75(2). In particular, Walkers considers section 75(2)(c) may come into play if a contract between a subscriber and a provider expressly or impliedly permits the use of DPI and/or similar technologies. Further, section 75(2)(e) could be relied upon by a provider to authorise its use of DPI and/or similar technologies, if the information was to be used for the purposes of: (*i*) providing or billing for that network or service; (*ii*) preventing illegal use of the network or service (for example by monitoring the web sites accessed by users and the content of emails); or (*iii*) preserving the technical integrity of the network or system (for example enhanced virus detection).

35. Walkers argued that, even if a provider uses DPI technology for one or more of the purposes set out in section75(2), there would be nothing to prevent the provider from using the technology for collateral purposes, including profiling users and monitoring content. According to Walkers, this could have far reaching implications and is of particular concern to the financial industry, in which electronic communication frequently contains sensitive market information and/or may be subject to legal professional privilege.

36. Walkers submitted that the installation or implementation of DPI or similar technologies could be prohibited, either by legislation, regulation or amendments to the existing ICT licences. Walkers noted that implementing measures to further restrict the use of the information would be of great assistance. Once certain types of confidential information have been intercepted, monitored, replicated or stored, there may be no adequate remedy for the end user if the information is improperly used. Licence revocation and/or the imposition of a financial penalty would also be inadequate.

37. WestTel argued that the use of DPI is permissible under sections 73 and 75 of the ICTA Law. According to WestTel, the framers of the ICTA Law contemplated that ISPs would be afforded the ability to protect their networks and as such allowed them use reasonable efforts to prevent illegal uses and protect the integrity of their networks. In WestTel's view, these provisions adequately cover the use of DPI and there is no reason to amend the ICTA at this juncture.

## Legislative and Regulatory Framework

38. In reaching a decision in this proceeding, the Authority is guided by sections 73 and 75 of the ICTA Law which 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 therefore.*
>
> (…)
>
> *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.*

39. In addition, the Authority is guided by clause 12 of the ICT licence granted to Digicel, LIME, TeleCayman and WestTel which states[1]:

> *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 unlawful or fraudulent use of the Licensed ICT Networks or the Licensed ICT Services.*
>
> *12.3 The Licensee shall establish implement, and publish its procedures for maintaining the confidentiality of information subject to this Condition 12.*

40. Other statutory provisions may be relevant in determining the legality of DPI, or of a particular use of DPI. These provisions include, without limitation:

- Section 9(2) of Schedule 2 of the Cayman Islands Constitution Order 2009, which states that "*Government shall respect every person's private and family life, his or her home and his or her correspondence*". In addition, this section states that, subject to certain exceptions, "*no person shall be subjected to the search of his or her person or his or her property or the entry of persons on his or her premises*". The Authority notes that this provision is expected to come into force on 6 November 2012.

[1] The wording of clauses 12.2 and 12.3 in the Digicel, Infinity, TeleCayman and WestTel licences is similar, but not identical, to the wording of the LIME licence. The words "*...unlawful or...*" do not appear in clause 12.2 of the Digicel, TeleCayman and WestTel licences. Also, clause 12.3 of the Digicel, TeleCayman and WestTel licences is worded as follows: "*The Licensee shall establish and implement procedures for ...*".

- Article 8 of the European Convention on Human Rights, which provides a right to one's "*private and family life, his home and his correspondence*". This article also requires that there be "*no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*".

- Section 5 of the Confidential Relationships (Preservation) Law (1995 Revision) ("Confidential Relationships Preservation Law"), which criminalizes the unauthorized collection and disclosure of confidential information of the kind which professionals would be obliged to protect.

41. The Authority understands that the Cayman Islands Government is considering the possibility of enacting data protection legislation. If and when such legislation is enacted, it may also be relevant in determining the legality of DPI.

## Authority's Analysis and Determinations

42. The Authority wishes to express its appreciation for the comments received from both the public and licensees. In particular, the Authority is grateful for the members of the public who have taken the time to submit their written views on the issue. The Authority encourages the public to continue to make its views known on all issues facing the Authority as it exercises its mandate to regulate the ICT marketplace and to promote long-term sustainable competition in the Cayman Islands.

43. The Authority notes that, over the past decade, broadband Internet services have become increasingly prevalent in the Cayman Islands and the Caribbean as a whole.[2] In addition, the Authority is aware that Cayman Islands residents are becoming increasingly adept at using innovative new Internet services which, in turn, has led to steady growth in Internet traffic. Partly in response to this growth, Digicel and WestTel have implemented DPI[3] on their networks. LIME has also confirmed that it intends to implement DPI on its network in the near future.

44. The Authority notes that the Internet users who participated in this proceeding (including both residential and business users) were all of the opinion that the use of DPI threatens the privacy, confidentiality and integrity of Internet communications. These users noted that this potential threat is of particular concern to the financial sector which makes up a large proportion of the Cayman Islands' economy. As a result, they submitted that the use of DPI should be either

[2] International Telecommunications Union, *Yearbook of Statistics: Telecommunication/ICT Indicators – 1999-2008*, December 2009, at pp. 205.

[3] For avoidance of doubt, from here on forwards, DPI is understood as "DPI and similar technologies" unless otherwise specified.

entirely prohibited or severely curtailed in the Cayman Islands. ISPs, on the other hand, were generally of the view that DPI is an essential tool for managing, and preventing the misuse of, their networks. In their view, the use of DPI is currently permitted by Cayman Islands law and there is no justification for restricting their ability to use this technology.

45. The Authority notes that, as part of this proceeding, the ISPs have identified several possible uses of DPI including:

- *Traffic Management:* DPI can be used to better understand the traffic profile on the ISPs' Internet backbone. This understanding, in turn, enhances the ability of ISPs to route traffic and manage congestion on their network.

- *Network Threats:* DPI can be used to identify network threats such as malicious software, spam, denial of service, and insulate the ISPs' networks from such threats.

- *Enforcement of legal requirements:* DPI can be used to identify and restrict the availability of illegal content (e.g. copyrighted material, etc).

- *Advertising, Billing and Customer Service:* DPI can be used to tailor Internet advertising to the web-browsing patterns of individual subscribers. In addition, it can be used to introduce usage-based billing.

46. After careful consideration of all submissions filed in this proceeding, the Authority has concluded that these uses of DPI raise significant legal and policy issues. The Authority has two primary concerns with respect to DPI.

47. The first relates to privacy. Not only does DPI permit the examination of packet headers, including source and destination IP addresses (which, in some instances, may also be considered personal information), but allows an ISP to examine the content of an electronic communication. The Authority is not convinced that examination of content is essential for traffic management (or any of the other purposes listed above) and views this practice as an unreasonable invasion of an individual's privacy.

48. The second concern relates to net neutrality. In order to promote online innovation, it is crucial that the Internet remain "neutral", where ISPs may offer different levels of access at higher rates as long as that tier is offered on a non-discriminatory basis to every other content provider. The Authority does not support the creation of a "private Internet" granting exclusive or preferential access (i.e. higher bandwidth levels) to certain providers or applications selected by the ISP. The Authority considers that the use of DPI should not be permitted in the Cayman Islands if it undermines net neutrality principles, either directly or indirectly.

49. From a legal perspective, the Authority is not convinced by the ISP's claim that their use of DPI is permitted under Cayman Islands legislation. In particular, the Authority is concerned that the use of DPI may be in breach of the Confidential Relationships Preservation Law, irrespective of whether it is used for "traffic management", "security threats" or any other purpose. Further, with respect to the ICTA Law, the Authority is not convinced that the use of DPI is permitted in all the circumstances identified by the ISPs. For instance, the Authority doubts that DPI is permitted under section 75(2)(e)(ii) if an ISP seeks to prevent copyright infringement. In the Authority's view, such use of DPI is likely to be permitted only if the ISP has been directed to do so by a court order.

50. However, despite these serious reservations, the Authority recognizes that this consultation is not the appropriate forum to make a determination on the legality or illegality of DPI, or a particular use of DPI, under sections 73 and 75 of the ICTA Law and the Confidential Relationships Preservation Law. Although the Authority is concerned that certain uses of DPI may in fact violate these provisions, the Authority considers that the responsibility for such determination rests with the courts, not the Authority. Having said that, the Authority has the ability (and reserves the right) to refer these matters to the Attorney General for possible prosecution. Furthermore, the Authority retains the right under section 56(c) of the ICTA Law to apply for an order from the Grand Court in respect of any contravention of the ICTA Law, including sections 73 and 75.

51. However, the Authority notes that, under the ICTA Law, it is responsible for the enforcement of ICT licences. In particular, ISPs are required, in accordance with clause 12 of their ICT licences "to maintain the confidentiality" and "refrain from using or disclosing" any personal and subscriber information "unless consent has been given to such use or disclosure by the person entitled to the confidentiality of that information". In the Authority's view, the scope of this obligation is broad and the wording of this clause is clearly intended to cover a wide range of ISP customer information, including both packet header and packet data.

52. The Authority considers that Digicel and WestTel have not taken appropriate steps to ensure that their customers have consented to the use of their packet information, as required by clause 12. Similarly, the Authority considers that the steps taken by LIME to date to ensure that its Internet customers have consented to the potential use of their packet information (if LIME decides to implement DPI on its network) are insufficient to comply with clause 12. Whilst the contractual documentation posted on these ISPs web sites contains vague references to network monitoring, it does not adequately inform consumers about DPI and its potential impact on Internet services and customer privacy.

53. In the Authority's view, at a minimum, full and complete disclosure of the use of DPI is required in order to obtain a customer's informed consent under clause 12. Therefore, the Authority directs ISPs to disclose clearly and prominently on their

websites, information related to DPI. This information should be provided on the web pages that describe the ISP's actual retail Internet service offerings, and must be referenced in relevant marketing materials, customer contracts, and terms of service. For example, where speeds are described in marketing material, there should be links to information describing how DPI may impact these services. The ISPs' websites must include the following information, at a minimum:

- Reason(s) for the ISP's use of DPI.
- Information as to which customers are affected by DPI.
- What customer data is accessed by DPI.
- The purposes for which the data obtained by DPI is used.
- Information as to the specific time of the day when DPI will be used (if the ISP's use of DPI is time-sensitive).
- Details as to the specific types of Internet traffic (e.g. application, class of application, protocol), if any, subject to traffic management policies that make use of DPI.
- For each service, a detailed description of how the use of DPI will affect a user's Internet experience, including upload and download speeds.

Clear and prominent disclosure of the use of DPI on the websites of ISPs must be made within 30 days of the date of this decision and, in the case of future uses of DPI, at least 30 days in advance of it being implemented or an existing policy being modified.

54. Further, the Authority has concluded that Digicel and WestTel did not satisfy the Authority that their uses of DPI would be restricted to the permitted activities listed in clause 12.2 of the licence, namely to operate their networks or services, to bill and collect charges, to protect their rights or property or to prevent the unlawful or fraudulent use of their networks or services. Likewise, LIME did not satisfy the Authority that its proposed uses of DPI would fall within the scope of clause 12.2. The Authority considers that the wording of this clause, in particular the phrase "*to operate its Licensed ICT Networks or Licensed ICT Services*" is ambiguous. In the Authority's view, any ambiguity in this clause should be resolved in a manner that enhances the privacy rights of Internet users in order to comply with Article 8 of the European Convention on Human Rights. Section 9(2) of Schedule 2 of the Cayman Islands Constitution could also be viewed as requiring a similar interpretation, effective on 6 November 2012. Therefore, the Authority considers that clause 12.2 should be interpreted in a restrictive manner and should not be viewed by the ISPs as a blanket permission to implement all forms of traffic management.

55. In light of the above, the Authority hereby notifies Digicel and WestTel that their current uses of DPI, and LIME's proposed uses of DPI, are in breach of clause 12 of their respective ICT licences. In accordance with sections 32, 33, 57 and 58 of the ICTA Law, the Authority directs Digicel and WestTel to take steps to comply with clause 12 of their licences. More specifically, Digicel and WestTel are directed to demonstrate to the Authority, within 21 days of the date of receipt of this decision, that they have taken steps to ensure that their use of DPI will be restricted to the activities mentioned in clause 12.2 of their licences. If Digicel and WestTel wish to continue using DPI for any purpose not covered by clause 12.2, they must satisfy the Authority that steps will be taken within a reasonable timeframe to obtain the consent of their customers, as outlined in paragraph 53 above. LIME is also directed to provide this information to the Authority within 21 days of the date of receipt of this decision, if it wishes to implement DPI on its network.

## Recommended Changes to ICTA Law

56. Based on the record of this proceeding, the Authority has concluded that amendments to the ICTA Law are needed to significantly restrict the use of DPI in the Cayman Islands. As noted above, the wording of sections 73 and 75 of the ICTA Law is broad and could be interpreted as authorizing the use of DPI in a wide range of circumstances.[4] The Authority considers that this interpretation would be highly detrimental to all Internet users and, in particular, to Internet users in the financial industry.

57. Therefore, in accordance with its mandate to advise the Minister on ICT matters under section 9(3)(b) of the ICTA Law, the Authority intends to recommend to the Minister that the ICTA Law be amended to incorporate the following principles:

- *Transparency:* Consumers must have the ability to make informed decisions about the Internet services they purchase and use. Where DPI is employed, ISPs must seek and obtain the consumers' prior express consent.

- *Limited Uses of DPI:* DPI should only be permitted in limited circumstances. For instance, whilst it is appropriate to use DPI to intercept illegal material such as child pornography, this use of DPI should be authorized by court order. Conversely, the use of DPI should not be permitted for the purpose of tailoring Internet advertising to the web-browsing patterns of individual subscribers. The use of DPI to deal with network congestion should only be allowed if the ISP can demonstrate that

[4] Having said that, the Authority would consider such an interpretation to be inconsistent with Article 8 of the European Convention on Human Rights (and, in the future, section 9(2) of Schedule 2 of the Cayman Islands Constitution).

there is no other reasonable option. Where DPI is employed to deal with network congestion, it must be designed to address this need, and nothing more and, as discussed below, must be done in a non-discriminatory manner. Network investment should continue to be the primary solution that ISPs use to resolve network congestion.

- *Neutrality:* ISPs must ensure that their uses of DPI are not unjustly discriminatory nor unduly preferential. Internet users must be able to access the lawful Internet content of their choice, run applications and use services of their choice (subject to the needs of law enforcement) and connect their choice of legal devices that do not harm the network. Internet users must be allowed to benefit from enhanced competition among network providers, application and service providers, and content providers.

58. The Authority will initiate discussions with Government on these recommended legislative changes in the second quarter of 2010.