ICT Authority Consultative Document on Deep Packet Inspection (CD 2009-4)

Response on behalf of Appleby

28 September 2009

Question 25e

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.

We consider that the use of DPI is currently prohibited by section 75(1) of the Law, which provides that it is an offence to intentionally intercept, alter, replicate, *monitor* or interrupt any message during its transmission over an ICT network or by means of an ICT service. The very purpose of DPI is to monitor communications.

There are certain exceptions to the general prohibition, which are set out in section 75 (2). These may apply to the use of DPI for some of the purposes which are contemplated, for example to intercept communications at the request of law enforcement and to enforce copyright laws. However, they would not apply to the use of DPI for the other uses to which it has been suggested that DPI would be put, such as to build profiles of consumers for marketing purposes, or to prioritise the transmission of some packets over others.

Question 25f

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.

We do not believe that the Law was framed in the way that it was merely because DPI was not available at the time. On the contrary, we believe that the philosophy behind the Law was to apply to the transmission of data over the internet as closely as possible the principles applicable to the sending of traditional letters. No-one would seriously suggest that the Cayman Islands Post Office should open letters and treat them differently according to the type of correspondence they contain. We believe that if DPI had been available at the time the Law was passed, the legislature would not have permitted its use. Since the issue has now arisen, we would recommend that sections 73 and 75 be changed so as to expressly prohibit the use of DPI for any purpose whatsoever. This is for the following reasons:

- We have serious concerns as to the effect the use of DPI would have on the confidentiality of communications sent to and from Cayman, and the level of trust that clients feel able to place in the integrity of the system. It is notable in this regard that, as far as we are aware no other offshore financial centre deploys DPI.

Doing so would therefore risk imposing on Cayman a significant competitive disadvantage.

- Communications sent from and received by this firm's Cayman office are frequently sensitive and covered by legal privilege. If the use of DPI were permitted, this might enable such communications to be read by parties other than the intended recipients. Legitimate client confidentiality is of the utmost importance to the legal and financial services sector, and any threat to that confidentiality would be extremely damaging to the reputation of that sector. We can ill afford this damage at a time when there are a number of other significant pressures on the jurisdiction. Further, as set out below, we do not believe that this risk is justified by the potential commercial benefits which the use of DPI may hold for a certain group of stakeholders (i.e. the ISPs).

- Whatever security measures were put in place to safeguard the data recovered by DPI, these would never be completely foolproof. It would never be possible to completely remove the risk that an experienced hacker, or a rogue employee at the ISP, might access and use the data for his or her own purposes, and the victim (be it this firm or clients of this firm) may have no adequate remedy if such information were intercepted and subsequently misused.

- Further, the use of DPI may also place ISPs in a position of conflict of interests or otherwise difficult or inappropriate situations. For example, if an ISP were itself a party to legal proceedings or engaged in a sensitive commercial transaction, it would have the ability to read confidential and legally privileged communications sent over its network by its opponent in the proceedings, or its counterparty in the transaction as the case may be. Whilst it would of course be illegal and improper for it to do so, it places an ISP in an invidious position having to deny itself the exercise of a power that it in practice possesses. It is easy to imagine a situation where an ISP innocently receives otherwise confidential information from another source, and then comes under suspicion of having improperly obtained it by using DPI.

- It is not necessary to introduce DPI 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.

- Given the status of ISPs as subsidiaries of companies incorporated in other jurisdictions, there is a risk that courts or other authorities in those other jurisdictions might require those who exercise corporate control over Cayman ISPs to obtain from their subsidiaries and pass on information to which those subsidiaries would have access through DPI, without the courts or authorities in the Cayman Islands having the opportunity to exercise any control in the matter.

Without DPI, those ISPs are relatively immune from such improper extra-territorial bullying.

- We do not consider that the use of DPI to give priority to different types of usage is in any event a desirable aim. We subscribe to the principle of 'net neutrality.' Even if, however, one accepts that 'throttling' is in principle desirable, it is not necessary to use DPI for this purpose. Such a result can achieved equally effectively simply by identifying, from the particular port being used by the packet, the type of usage to which the packet relates. Further, we do not believe that throttling, whether based on ports or by using DPI, would be successful anyway: high bandwidth users who found their usage constricted would soon find ways of sending their traffic in ways that prevented DPI from identifying the nature of the use and downgrading its priority of access to the ISP's bandwidth, just as they could 'spoof' the port being used. To use DPI for this purpose would in summary be an ineffective way, with significant negative side-effects, of doing something that should not be done anyway.

- If, on the other hand, the aim is consumer profiling, we do not see that there is any social justification for this that would justify the potential damage to the jurisdiction. We do not consider that the benefits of DPI for network operators, as outlined in the Consultative Document, justify the potential damage to the legal and financial services industry outlined above.

Question 25g

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

As set out in our response to Question 25f above, we consider that the use of DPI should be expressly prohibited by legislation. We do not consider that it is possible to put sufficient protective measures in place to prevent its use undermining the confidentiality of communications, which in turn would cause significant damage to the legal and financial services sector in Cayman.

If, contrary to our strongly-held view that DPI should not be introduced at all, the Authority is minded to permit it, we would urge that it be permitted *only* for law enforcement purposes and *not* for any regular or routine commercial use by the ISP, with a requirement for a court-issued warrant whenever access to the data is required, and for the presence of an officer above a certain rank when the data extraction process is carried out. The strongest possible measures should be put in place to restrict access to the server containing the data obtained through DPI, including systems to log all access and changes and extreme physical security of the server room in question.