**Walkers' response as a Stakeholder to the Information & Communications Technology Authority's public consultation on "A Policy for Deep Packet Inspection and Similar Technologies" (Ref: CD 2009-4)**

**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.**

Section 73 of the Information and Communications Technology Authority Law (2006 Revision) (the "**Law**") regulates the grounds upon which an ICT service or ICT network provider (as defined under the Law, a "**Provider**") may refuse to provide an ICT service or an ICT network to a subscriber or discontinue or interrupt the provision of such an ICT service or ICT network to a subscriber pursuant to an agreement with that subscriber. A Provider may only refuse to provide such service or network or discontinue or interrupt the provision of such service or network on grounds which are reasonable and non-discriminatory.

We do not consider this to be directly relevant to the question of whether the use of Deep Packet Inspection ("**DPI**") and/or similar technologies is permissible. However, it 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, we anticipate 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 Law.

Section 75 of the Law generally provides that a Provider cannot intentionally intercept, alter, replicate, monitor or interrupt messages by any means unless one of the exceptions set out in sub-section (2) applies. We consider that section 75 (2)(c) and section 75 (2)(e) are relevant here. These subsections provide that:

"A person shall not be guilty of an offence under this section if-
...(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; (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 the 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."

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. This will be a question of fact in each case.

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) to preserve the technical integrity of the network or system (for example enhanced virus detection).

Conclusion – in our view, the use of DPI and/or similar technologies may be permissible under the exceptions set out in section 75 (2)(and in particular, subsections (c) and (e)) to the general prohibition against interception of messages.

**f. Given that the 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 believe that there is a public interest need to review the provisions of section 75 of the Law given the introduction of DPI and similar technologies.

Even if a Provider uses the technology for one or more of the purposes set out in s.75 (2), there would be nothing to prevent the Provider from using the technology for collateral purposes, including profiling users and monitoring content. 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.

An ISP could potentially eavesdrop on a customer's internet traffic in order to build a profile on the customer's internet preferences e.g. types of websites visited, online shopping preferences and the like.

We note that confidentiality of customer information is currently covered by section 12 of all ICT Licences, although it is not clear how the ICTA enforces these provisions. In any event, the end user has no control over the use or storage of the information once it has been accessed and inspected.

Section 75 could be amended as follows:

(2) insert the following words "Subject to subsection (3)," immediately before "A Person shall not be guilty of an offence under this section if – …" and replace "A" with 'a".

Insert a new subsection (3) For the purposes of this section, a person shall not be permitted to use Deep Packet Inspection and/or similar technologies.

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

The installation or implementation of DPI or similar technologies could be prohibited by legislation or regulation by the ICTA. The terms of existing licences could presumably be modified under section 31(3) or section 31(4) of the Law.

We do not consider 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. Revocation of the Provider's licence and/or the imposition of a financial penalty would also be inadequate.

We do not know the extent to which the ICTA has requested ISPs to disclose the purpose for which they intend to deploy DPI. However, we note the following:

(i) Many Internet applications were not designed to make use of DPI traffic shaping functionality.

(ii) Net Neutrality is also a concern as ISPs will presumably attempt to give priority to traffic from specific subscribers based on their type. Voice packets for example are typically given higher priority than email. This could provide an unfair advantage to certain ISPs and their subscribers over others that do not use DPI or similar technologies. If ISPs begin giving priority to specific types of traffic, this could cause application developers to begin camouflaging their traffic as other types of traffic in order to receive higher priority. In the long-run, this would make DPI less effective. It may be better to allow individual subscribers to decide how they wish to manage their traffic (for example by using packet acceleration appliances to prioritise network traffic across offices).

(iii) DPI is not an end to end solution so even if it is being used for traffic prioritisation, there is no guarantee that it will be effective. There is no established mechanism for different ISPs to share the same DPI traffic priorities or to even employ the same DPI technology. There are no standards between ISPs, therefore traffic that is being prioritised within one ISP's network will not have the same priority as it passes to another ISP and in the worst case will not be prioritised if

the ISPs are not using DPI. This means no one ISP can guarantee improved network performance using DPI as an end to end solution.

(iv) DPI is an inherently complex and error-prone technology, and the likelihood of false positives is high. Packets of one type could easily be mistaken and prioritised as another type. An end to end solution such as diffserv provides works the same as DPI with less complexity.