Response to Cayman Islands ICTA enquiry
A Policy for Deep Packet Inspection and Similar Technologies
CD 2009-4

From: Neil Maybin
Address: 6 Albany Terrace, Albany Passage, Richmond TW10 6DN, UK.
Email: nm@neilmaybin.com
Phone: +44 20 8940 8510
Mobile: +44 7979 802614
Date: Friday 28th August 2009

Summary

Deep Packet Inspection technologies present a significant threat to the privacy and integrity of Internet communications. While most of the discussion so far has focussed on individual privacy, commercial confidentiality is also threatened by such technologies. This should be of particular concern to the financial sector which makes up much of the Cayman Islands' economy.

Experience in the UK suggests that while existing laws could be applied to prevent non-essential DPI (such as DPI for targeted advertising), several factors prevent them from being enforced. This submission argues that while there may be scope to tighten up existing legislation, new provisions are needed which expressly prohibit all DPI except for very specific exceptions such as state surveillance.

Background

In 2006 and 2007 in the UK, BT in conjunction with former spyware company[1,2,3] Phorm ran secret trials of a DPI based targeted advertising system[4,5]. Despite public outcry they ran a further trial in late 2008[6], this time asking their customers whether they wanted targeted advertising but not informing them that to do this their web activity would be intercepted and read[7].

That there are now no current plans by any UK ISP to deploy DPI for targeted advertising has been the result of the public response, and not UK legal action. Consequently much time and energy has been wasted and controversy generated in preventing a threat to privacy and commercial confidentiality which should have been clearly illegal in the first place.

I run inphormationdesk.org which aims to explain this area to the general public and also provide a repository of information and detailed attributions on Phorm and DPI. My background is in IT, having spent nearly three decades working for companies such as IBM, Andresen Consulting, NCR and Teradata.

For clarity, however, I should emphasise that I am submitting this response in a personal capacity supported by the knowledge I have built up over the last eighteen months as the Phorm controversy has progressed in the UK. Also, as webmaster for several websites covering matters of general interest, I am a stakeholder since the material I have created may be scraped and copied by DPI targeted advertising schemes operating in any jurisdiction without my permission.

Principles

In planning the legal response to DPI it is important to be clear about the basic principles which need to be in place to ensure the privacy and integrity of communications.

Internet Interception is no different from Postal or Telecoms Interception: A useful analogy is to ask whether we would be comfortable if any proposed Internet scheme were applied to communications by mail or telephone. Would we be happy if the postal service had the ability to open letters to determines who should receive which junk mail, even if we had not opted into that service? Would we be happy if our telecoms provider had the ability to listen in to our conversations and call us later with commercial offers?

Personal Privacy: Companies offering DPI targeted advertising schemes claim that personal data is anonymised. However they have not subjected data collected to formal analysis. Traditional means of anonymisation – such as those used for AOL clients – have proved ineffective[8]. The same companies say they will not scan data about certain subjects. They have not explained how they will identify sensitive information by context or for all languages. How then can users be expected to give informed consent, even if their permission is sought, and even if the interception of their internet activity is described in the request for permission?

Privacy of Material Published to a Limited Group: Although the privacy of the user who may or may not have opted into a DPI targeted advertising scheme has so far been the key focus of campaigns against Phorm in the UK and NebuAd in the US, what about the privacy of people who publish information for their Facebook Friends, one of whom may be opted into a DPI targeted advertising scheme?

Commercial Confidentiality: And what about the commercial position of a company whose web pages are intercepted by a DPI targeted advertising scheme for the benefit of their competitors? For example, in the 2006 BT/Phorm trials a BT broadband customer visited Sainsburys Bank, HSBC and Hometown web pages looking for auto insurance. Later the customer was shown an advert for MORE TH>N auto insurance[9]. It's no wonder then that Amazon, who present offers specific to individuals, has banned Phorm from scraping their content[10].

Financial Integrity: The Cayman Islands relies heavily on the Financial sector for its economic success. It would seem highly imprudent to allow any organisation between the sender and recipient of messages across the Internet to intercept and read (and maybe change) data. Indeed Nationwide Building Society in the UK has banned Phorm from scraping their content[11].

In summary, the privacy and integrity of communications whether by post, phone or internet, is essential not just for personal freedom but for commercial success. Any safeguards offered by schemes which intercept communications are likely to be fragile and not withstand future economic pressures. Today's DPI for targeted advertising is already unacceptable; tomorrow's free-for-all by anyone in the communications chain would be unmanageable and unauditable.

Legal lessons from the UK experience

Effectiveness: The experience of how UK Law has addressed the issue of DPI for targeted advertising carries important lessons for jurisdictions planning legislation in this area, such as the Cayman Islands. Several UK laws appear to make DPI for targeted advertising illegal. However in practice they have not been enforced because of four problems (i) fragmentation of who is responsible for enforcement, (ii) low priority given to interception offences by the enforcing bodies, (iii) ignorance of the law by the enforcing bodies and (iv) insufficiently tight specification of the laws.

Laws: There are several laws covering DPI for targeted advertising, and a good description of these is set out in two papers by Nicholas Bohm[12,13]. The three main areas are:

- ◊ Interception – RIPA: owned by the Home Office and enforced by the Police
- ◊ Personal Privacy – DPA, PECR: owned by the Ministry of Justice and managed by the Information Commissioner
- ◊ Copyright – CDPA: owned by the Department for Business, Innovation and Skills, generally civil but with some criminal provisions

Interception: DPI-based schemes should first be governed by interception law. In the UK, RIPA makes unauthorised interceptions of communications illegal unless **both** parties agree, subject to some exceptions. The following issues have prevented enforcement:

- ◊ Initial advice given by the Home Office[14] assumed wrongly that a web page served to a user was a publicly available document. However, many (if not most) web pages served are customised for a given user and so form a private communication between the website and the user. Under RIPA the website's permission should be needed for interception as well as that of the user.
- ◊ In response to a complaint by members of the public (Crime Reference Number: 5253/08) the City of London Police cited a lack of criminal intent by Phorm and BT (the ISP carrying out the interceptions), implied consent by the users whose communications were intercepted, and a lack of priority in pursuing the case. They wrongly advised contacting the Interception Commissioner, as his jurisdiction covers only interceptions by state bodies[15]. Although this complaint is now with the Crown Prosecution Complex Cases Unit[16] it is unlikely that any further action will be taken.
- ◊ Number 10 Downing Street in responding to a 21000-signature petition, incorrectly stated that the Information Commissioner regulated interception[17].

Data Protection: The use of data gathered by DPI for targeted advertising is governed by the laws managed by the Information Commissioner. However the ICO only has powers to stop existing practices, and even these are weak when faced with an organisation unafraid of public opinion or acting in bad faith.

Copyright: On the face of it, systems which use DPI for targeted advertising create copies of web pages which have an independent economic significance, a breach of CDPA. However this aspect of the law has never been tested, and it is likely that at least some interested parties will be prepared to argue that CDPA is not in fact breached in such circumstances.

In summary, UK law, although outlawing DPI for targeted advertising in theory, has proved ineffective to apply in practice. Relevant laws are split across multiple government departments. The Police, who are responsible for enforcing the 'front-line' interception law do not fully understand it or regard it as a priority. In order to be enforceable, UK interception law needs to include specific provisions covering DPI. I would recommend that Cayman Islands law includes specific provisions covering DPI as well.

Cayman Islands Law and DPI

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 Cayman Islands law (ICTAL 2006 Revision) as specified in the consultation document offers inadequate protection against the deployment of DPI systems in general and those for targeted advertising in particular. Specifically:

Section 75 Subsection (2) item (c) allows one party to a communication to consent to interception without the other party being aware that it is taking place. It admits an argument that consent to interception can be assumed. These are far weaker provisions than are present in the relevant UK law, RIPA, which normally requires consent from both parties. And in practice, RIPA itself has proved ineffective in discouraging DPI for targeted advertising.

Section 75 Subsection (2) item (f) allows an argument that the message was intended to be received by the public. This is insufficiently specific to cover the range of web material available, much of which is customised for a given user or user cohort. It leaves open whether the website serving the material intended it to be a private or public communication.

Moreover even if the communication could be regarded as 'public', Section 75 Subsection (2) item (f) does not address the issue that if a given user requested material from a given website, or a given website served it to a given user, that fact alone may be personal or confidential regardless of the contents of the communication.

It is for these reasons that further specific provisions expressly covering DPI are likely to be more effective than just amending existing provisions of the law.

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?

Yes, for the reasons set out in the answer to (e) above, and also given the ineffectiveness in practice of more stringent UK law in this area.

If so, please detail the changes you would recommend and provide your rationale for these changes.

Recommendation 1: Section 75 Subsection (2) item (c) of the Cayman Islands ICTA Law needs to be changed to require the consent of both parties and remove the concept of implied consent:

> *(c) the person by whom the message is sent **and** to whom the message is sent **have both** expressly ~~or impliedly~~ consented to the interception, monitoring or interruption;*

Recommendation 2: The Law needs to include further provisions covering Internet Service Providers and DPI very specifically:

- ISPs may *only* read header data. They must only use this information internally for specified purposes such as network optimisation and security. They may not disclose it to third parties in detailed or digested form unless all the subjects of that information (who may be users or websites or both) have given their express permission.
- ISPs may *never* read packet data or provide it, or a digest of it, to any third party. Only government bodies may 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.

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

One of the biggest challenges of DPI is that in practice it is essentially an unauditable technology. This underlines the need to minimise its use as far as possible.

ISPs should report annually to the ICTA on their use of DPI. In addition the ICTA should have powers to engage technical auditors to investigate DPI violations in ISPs, although I would expect these to be used only in exceptional circumstances and as a last resort.

Other DPI-related Topics Raised in the Consultation

Net Neutrality: The consultation raises the question of Net Neutrality. This is a far wider issue than that of DPI, although it is closely related to it.

The principles of Net Neutrality support and enhance personal and commercial privacy, commercial fairness, free competition, and political freedom. I would therefore recommend that the ICTA encourage new legislation to support Net Neutrality in the Cayman Islands. This should be based on proposed US legislation (H.R. 3458, the Internet Freedom Preservation Act 2009) or proposed EU legislation.

One issue which has been raised in both the US and Europe is whether ISPs may prioritise certain traffic. The legal consensus appears to permit this *providing* the rules of such prioritisation are publicly available. Prioritising some kinds of traffic (e.g. Skype phone calls or gaming) may legitimately form part of an ISP's offering. However the intentions of some operators to prioritise some content providers over others would restrict free competition amongst content providers. Any law on Net Neutrality should prohibit this kind of prioritisation.

Copyright Enforcement: In Europe particularly there have been calls by record and film companies for ISPs to monitor breaches of copyright arising from file-sharing. They claim substantial financial losses as a result of file-sharing, though the magnitude of these is questionable since there is no certainty that much of the content would be bought were it not available for copying.

Conceding the principle that ISPs should monitor communications for copyright breaches is a dangerous option. It sets a precedent (with all that implies) that a third party must on request intercept and read communications in a civil dispute without any legal warrant. It introduces a process which may result in fines or other sanctions without proper legal oversight. In its worst case where disconnection is proposed it could result in the parents of a file-sharing teenager losing their livelihood if they relied on the Internet for their employment.

The Cayman Islands should reject any pressure from the record and film industry for such monitoring. It is up to the industry themselves to find more forward-thinking ways to safeguard copyright. DPI should not be used for this purpose.

Censorship: DPI is also used to enforce censorship. Generally in the West this has been limited to material most would find offensive (such as child abuse), though in countries such as China and Iran it has been used to stifle free speech.

It is worth noting that while phishing websites impersonating banks are generally removed in a couple of hours, the mean lifetime for a website hosting child abuse images is almost a month.[18] There appears to be considerable scope for more effort to be put into take-down and less into DPI and censorship.

Takedown of illegal material is the only transparent and safe way of addressing these kinds of crimes in a free society. DPI should not be used for this purpose.

References

[1] F-Secure classifies PeopleOnPage and ContextPlus as Spyware:
http://www.f-secure.com/sw-desc/peopleonpage.shtml

[2] Symantec classifies PeopleOnPage and Apropos as Spyware
http://www.symantec.com/security_response/writeup.jsp?docid=2004-113018-3823-99

[3] Computer Associates classifies PeopleOnPage as a Hijacker (Published 16th August 2004):
"Changes browser settings other than homepage, without user permission. Can't be uninstalled by Windows Add/Remove Programs and no uninstaller is provided with application."
http://www.ca.com/us/securityadvisor/pest/pest.aspx?id=453074934

[4] http://www.theregister.co.uk/2008/04/01/bt_phorm_2006_trial/

[5] http://www.theregister.co.uk/2008/02/27/bt_phorm_121media_summer_2007/

[6] http://www.theregister.co.uk/2008/09/29/bt_phorm_trial_go/

[7] UK Information Commissioner said: "Shortly before this pilot began they sent us a copy of the 'invitation' page on the basis of which customers would choose whether or not to take part in the pilot. We made clear to BT that we had strong reservations about the nature of the explanation provided, largely because it concentrated on security advantages rather than on the targeted advertising."
https://nodpi.org/forum/index.php/topic,1013.msg10173.html#msg10173

[8] *New York Times*: "A Face Is Exposed for AOL Searcher No. 4417749"
http://query.nytimes.com/gst/fullpage.html?res=9E0CE3DD1F3FF93AA3575BC0A9609C8B63

[9] British Telecom Phorm PageSense External Validation report (Page numbered 44)
http://www.wikileaks.org/wiki/British_Telecom_Phorm_Page_Sense_External_Validation_report

[10] *BBC*: "Amazon blocks Phorm Adverts"
http://news.bbc.co.uk/1/hi/technology/7999635.stm

[11] *The Guardian*: "Nationwide building society opts out of Phorm services"
http://www.guardian.co.uk/business/marketforceslive/2009/jul/21/phorm

[12] FIPR Legal Analysis of Phorm (Nicholas Bohm, 23rd April 2008)
http://www.fipr.org/080423phormlegal.pdf

[13] FIPR Profiling Web Users -- Some Intellectual Property Problems (Nicholas Bohm, 25th November 2008)
http://www.fipr.org/0811SCLarticle.pdf

[14] Home Office Note on Phorm Spyware (11th March 2008)
http://cryptome.org/ho-phorm.htm

[15] *NoDPI*: "City of London Police – Too complex to spend public money".
https://nodpi.org/2008/09/22/city-of-london-police-to-complex-to-spend-public-money/

[16] *NoDPI*: "CPS Review of BT's Covert Trials"
https://nodpi.org/2008/11/25/cps-review-of-bts-covert-trials/

[17] *The Times* (19th May 2009): "UK Government Phorm response is a complete waste of webspace"
http://timesonline.typepad.com/technology/2009/05/uk-government-responds-to-phorm-petition.html

[18] The Impact of Incentives on Notice and Take-Down (Moore and Clayton)
http://www.cl.cam.ac.uk/~rnc1/takedown.pdf