SENATE
QUESTION

QUESTION NUMBER: 2821

Senator Ludlam asked the Minister representing the Minister for Home Affairs upon notice, on 11 February 2013:

(1) Has the Australian Federal Police (AFP) issued notices or requests, under section 313(3) of the Telecommunications Act 1997 (the Act), to any Internet Service Providers (ISPs) that require the recipient ISP to block access to domains/web sites on the Interpol 'worst of' list; if so: has the AFP agreed to pay the costs of any ISP (in accordance with section 314 of the Act) that are incurred in complying with the AFP notice or request issued under section 313(3).

(2) If an ISP declines to implement blocking of access, unless the AFP pays the ISP's costs (in accordance with section 314 of the Act), does the AFP intend to pay such costs.

(3) What is the AFP's estimate of total costs to the AFP, if any, in the 2012 13 financial year, in connection with paying ISPs' costs incurred in complying with the requirements of the AFP notice or request issued under section 313(3).

(4) Has the AFP calculated an estimated total cost to the AFP in relation to payment of costs of initial implementation of blocking by all Australian ISPs, and/or in relation to paying ISPs' ongoing annual maintenance costs thereafter; if so, what are the amounts of the AFP cost estimates.

(5) Has the AFP issued notices or requests to any ISPs, under legislative provisions other than section 313(3) of the Act, that require the recipient ISP to block access to domains/websites on the Interpol 'worst of' list; if so:

(a) under which particular section and subsection of what legislation were such AFP notices or requests issued;

(b) has the AFP issued such a notice or request to any ISP prior to the particular ISP informing the AFP of willingness to voluntarily implement blocking of access;

(c) on what date was the first such notice or request issued, and under which particular section and subsection of what legislation; and

(d) how many ISPs have been issued with such requests.

(6) In regard to the Minister for Broadband, Communications and the Digital Economy's media release on 9 November 2012, titled 'Child abuse material blocked online, removing need for legislation', stating that Australia's largest ISPs have been issued with notices requiring them to block these illegal sites in accordance with their obligations under the Telecommunications Act 1997 and that [t]he Australian Federal Police (AFP) will now begin issuing notices to smaller ISPs': are the AFP 'notices' being issued under section 313(3) of the Act; if not, under which specific section and subsection of what legislation are the notices being issued.

(7) If an ISP fails to implement the blocking of access required by an AFP notice, what powers do the AFP have to force compliance, and/or to have sanctions or penalties applied to the ISP, and under what specific sections of what legislation.

(8) Do the notices issued by the AFP refer to any particular obligation/s of ISPs under the Act with which ISPs are being notified to comply; if so, what are the specific section and subsection numbers of the Act that set out the obligation/s referred to in the AFP's notices.

(9) If subsection (1) of section 313 of the Act is included in the answer to question (8), what particular provisions of what legislation empower or otherwise authorise the AFP to determine what constitutes, in the case of any particular ISP, doing their best in regard to section 313(1) and then notifying the particular ISP to comply with what the AFP determined.

(10) As at 9 November 2012, how many ISPs had received the AFP notices referred to in the Minister's 9 November 2012 media release, and what are the names of those ISPs.

(11) Since 9 November 2012, how many additional ISPs have received such notices from the AFP, and what are the names of those ISPs.

(12) Do the numbers of ISPs equal the total number in Australia who provide Internet access services to the general public; if not, how many ISPs have not yet received AFP notices, and why not.

(13) In regard to the AFP's answer to question no. 25, taken on notice during the 2011 12 Supplementary Budget estimates hearing of the Legal and Constitutional Affairs Legislation Committee, which states that, as participation by ISPs is voluntary, a section 313 request is made by the AFP when the ISP has indicated their participation and have/are readying their technical infrastructure to implement blocking of the list: were the section 313 requests being made under section 313(3) of the Act; if not, under which subsection of section 313 were the requests being made.

(14) In regard to ISPs who received a section 313 request in connection with the voluntary blocking trial, has the AFP subsequently issued a section 313 request to any of those ISPs that requires the ISP to block access, regardless of whether the ISP continued to be voluntarily willing to do so.

(15) In regard to the statement in an AFP document titled 'Talking Points - Senate Estimates October 2011' (released by the AFP under the Freedom of Information - AFP Disclosure Log No. 10/2011), that 'Consultation with all stakeholders revealed that a formal request for assistance under section 313 of the Telecommunications Act 1979 [sic] was the most appropriate vehicle to initiate the trial of the blocking scheme', what were the reasons for deciding that 'a formal request for assistance under section 313 of the Telecommunications Act 1979 [sic] was the most appropriate vehicle.'

(16) How many of the consulted stakeholders were representatives of:

(a) particular ISPs;

(b) associations or organisations comprised of telecommunications industry members;

(c) government and/or government departments or agencies.

(17) Were any other types of stakeholders consulted; if so, what types and how many.

(18) In regard to Mr Neil Gaughan's statement, made during the 2011 12 Supplementary Budget estimates hearing of the Legal and Constitutional Affairs Legislation Committee (18 October 2011), that 'the first review' of the voluntary blocking trial 'will actually take place in December of this year which will be oversighted by the Child Protection Committee which is part of ANZPAA', was a review of the trial conducted in December 2011, and/or at any later time; if so, can a copy of the review report/s be provided.

(19) Has the voluntary blocking trial ended; if so:

(a) on what date did the trial end; and

(b) did the AFP decide to cease operation of the trial; if so, why; if not, who made the decision that the trial would cease to operate.

(20) In relation to the Interpol 'worst of' list of domains/websites that the AFP distributes to ISPs, what procedures and/or requirements has the AFP implemented for the purpose of ensuring that the list will not be used by any staff member of any ISP for the purpose of personal access to child abuse material, nor provided by any ISP staff member to anyone else.

(21) How many domains were on the Interpol 'worst of' list as at:

(a) 31 January 2012;

(b) 30 June 2012;

(c) 9 November 2012; and

(d) 31 January 2013.

Senator Ludwig– The Minister for Home Affairs has provided the following answer to the honourable senator's question:

(1) Yes, the AFP has issued notices or requests under section 313(3) of the Telecommunications Act 1997 (the Act), to Internet Service Providers (ISPs) that require the recipient ISP to block access to domains/web sites on the Interpol 'worst of' list.
As at 22 February 2013, the AFP has not agreed to pay the costs of any ISP (in accordance with section 314 of the Act) that are incurred in complying with the AFP notice or request issued under section 313(3) .

(2) The AFP has not received advice from any ISP that they are declining to block based on cost. If such advice was received, the request would be treated in the same manner as a compensation claim and the AFP would examine each matter on a case by case basis giving consideration to the relevant provisions of the Act, the Commissioner's Financial Guidelines and the Financial Management and Accountability Act 1997.

(3) No costs are anticipated at this time for the 12/13 FY.

(4) No, the AFP has not made any calculations of potential costs at this time.

(5) No.

(6) The Notices issued are pursuant to section 313(3) of the Act.

(7) Section 313(1) of the Telecommunications Act 1997 imposes standing obligations on ISPs to do their best to prevent telecommunications networks and facilities from being used in relation to the commission of offences against the laws of the Commonwealth. Matters of compliance with the provisions of the Telecommunications Act 1997 by carriers or carriage service providers are best addressed to the Australian Communications and Media Authority'.

(8) The notice refers to Sections 313 and 314 of the Telecommunications Act 1997 as a whole. No subsections are referred to. Blank notice attached see Appendix A.

(9) Matters of compliance with the provisions of the TI Act by carriers or carriage service providers are best addressed to the Australian Communications and Media Authority.

(10) Eight (8). The names of the ISPs have not be made public as it would prejudice ongoing Law Enforcement action and may lead to offenders moving to ISPs which are currently not participating. Furthermore, disclosure of the names of the participating ISPs may have a substantial adverse effect on the proper and efficient conduct of the operations of the AFP and would be contrary to the public interest.

(11) Thirteen (13). The ISP names have not been made public for the same reasons outlined in question 10.

(12) No. According to figures from the Australian Bureau of Statistics (ABS) , as at 30 June 2012, there were 81 ISP's with over 1,000 subscribers operating in Australia. This includes some major well known ISPs such as Telstra and Optus, and some very 'small single' operator type providers. Some are also 'wholesale' providers with their services on-sold by retailers. Given the nature of the industry, ISP's change regularly and are bought, sold or taken over on a regular basis.
The AFP to date has focussed on the major providers to gain maximum coverage, estimated by the ACMA to be over 90% of Australian's internet users, through the market share of those providers, thus ensuring maximum effect to the blocking initiative.

(13) The requests were made under section 313(3) of the Act.

(14) Yes, s313 articulates the requirements of the ISP's.

(15) A number of reasons were uncovered during this consultation process, however the more notable reasons were:
- ISPs concerns that implementing blocking without some form of legal liability coverage should the blocking of a website have a detrimental effect;
- ISPs concerns that without formal direction from law enforcement they would in effect "be put into the position of judging whether or not to take specific law enforcement action", which is of course a matter for law enforcement.

(16)
(a) 4 initially, thence 4 in consultation with IIA
(b) 1 Internet Industry Association IIA
(c) Australian Communications and Media Authority and the Department of Broadband, Communications and the Digital Economy.

(17) No.

(18) The review was not finalised in December 2011 due to ISP's not being able to provide the detailed feedback requested. The AFP conducted its own internal assessment and a redacted copy of the report prepared is at Appendix B.

(19) The trial has not ended, more that the blocking is moving to a more Business as Usual arrangement given the benefits derived in crime prevention by preventing this known criminal content from being accessed cease to operate.

(20) The AFP requires each participating ISP to sign a Deed of Confidentiality requiring the ISP to take measures to prevent unauthorised disclosure of the list and the workings of the blocking.

The list is only available via a secure mechanism with access control and authentication processes and requirements.

(21)

(a) 472
(b) 1285
(c) 1396
(d) 1216

The number of domains on the Interpol list changes regularly as sites are taken down or shifted in attempts to avoid law enforcement action.

Appendix A:

HIGH TECH CRIME OPERATIONS

GPO Box 401 Canberra City ACT 2601
www.afp.gov.au
ABN 17 864 931 143

Date:

Appropriate Office Holder
Internet Service Provider

Scheme to reduce the online availability of Child Abuse material -

Request for assistance in accordance with sections 313 (1) and 314 Telecommunications Act 1997

The Australian Federal Police (**AFP**), as a member of the Australian and New Zealand Police Advisory Agency Child Protection Committee (**ANZPAA CPC**) is working together to take viable steps to limit access to child exploitation material via Australian telecommunications services. The central intention of the activity is to prevent Australian telecommunications networks and facilities being used to commit offences related to the access of child exploitation material in contravention of various Commonwealth, State and Territory legislative provisions.

The access limitation scheme (**the Scheme**) operates at the Internet service provider (**ISP**) domain name server level. Interpol compile a 'worst of' list (**the blacklist**) of websites which have been detected as containing the most severe child abuse material. The criteria utilised by Interpol for inclusion of a domain in this list means that the subject material is considered child pornography or child abuse material under all Australian legislation. This list is distributed to all national police agencies for distribution to domestic ISP's in accordance with local legislation and policies.

The access limitation works by the ISP operated domain names servers redirecting the user to a stop page rather than directing the internet user to the correct IP address of the website. The stop page is predominately Interpol branded and advises the user the requested website contains child exploitation material. As the primary purpose of this scheme is to prevent and deter, no recording of identifiable information relating to the requesting user is necessary.

Section 313(1) of the *Telecommunications Act 1997* imposes obligations on ISPs to do their best to prevent telecommunications networks and facilities from being used in relation to the commission of offences against the laws of

the Commonwealth. The *Criminal Code Act 1995* details a number of offences that relate to the inappropriate use of telecommunications, including using a carriage service to access, distribute or make available child abuse material.

Similarly, Section 313 of the *Telecommunications Act 1997* imposes obligations for telecommunications carriers and carriage services to provide such assistance as is reasonably necessary to assist authorities of the Commonwealth enforce the criminal law and other associated matters. The AFP considers this request for [insert company name] to participate in the Scheme to be a request under Section 313 of the *Telecommunications Act 1997*.

Section 314 of the *Telecommunications Act 1997* requires the parties to agree the terms and conditions of such assistance. Outlined below are the terms and conditions of the assistance to be provided by [insert company name] as agreed between the AFP and [insert company name] in accordance with the requirements of section 314.

The AFP request [insert company name] to implement the Scheme by undertaking ISP level filtering on its network or networks based on the INTERPOL blacklist of internet domains which have been verified as containing child abuse images.

The Scheme:

- commenced on 30 June 2011;
- involves Australian based Internet service providers and their subsidiaries, internet gateway and filtering manufacturers;
- will only utilise the Interpol blacklist which will be distributed by the AFP to participants. The transmission of the list will be effected via secure file transfer;
- will be reviewed by ANZPAA CPC as to the effectiveness of the scheme;
- will be subjected to a formal review by the AFP every 6 months, where the AFP may request relevant information from the provider;
- requires participants enter into a specific deed of confidentiality (non–disclosure) with the AFP regarding publication of the Interpol 'worst of' list;
- permits participants, at their own election and cost, to publicise their involvement in the access limitation scheme;
- provides that all participating ISP's can implement the scheme, in a manner appropriate for their own network infrastructure;

- requests the appearance of the 'stop page' to which users are re-directed to be based upon the sample page provided by Interpol;
- is managed by the ANZPAA CPC on behalf of all Law enforcement agencies; and
- activity undertaken by the parties will be open to inspection by each participating entity's statutory ombudsman.

To enable the AFP to provide the Interpol blacklist to [insert company name] please have the relevant person complete the attached Deed of Confidentiality and return it to Detective Superintendent Todd HUNTER, National Coordinator, Child Protection Operations.

Once received, the AFP will provide [insert company name] with the blacklist in the form outlined above.

I look forward to your co-operation in this additional measure to protect the Australian community.

N. Gaughan
Assistant Commissioner
Australian Federal Police

Appendix B:

AFP
AUSTRALIAN FEDERAL POLICE

Minute

Addressee NM HTCO
Via MCCO
NC CPO

Title **Review of Interpol 'worst of' list blocking scheme – December 2012.**

Action required:

For information.

Deadline:

Nil.

Reasons for proposed actions:

In June 2011, a number of Australian Internet Service Providers (ISP's) commenced access blocking to limit the distribution of child exploitation material centred upon the Interpol 'worst of' list of websites confirmed as containing the most severe child exploitation material. The 'worst of' list is distributed to national police agencies for distribution to domestic ISP's in accordance with local legislation and policies.

The access limitation works by the ISP operated domain names servers redirecting the user to a stop page rather than directing the internet user to the correct IP address of the website. The stop page is Interpol branded and advises the user that the requested website contains child exploitation material. As the primary purpose of the scheme is to prevent and deter, no recording of information relating to the requesting user is necessary.

At 31 December 2012, the blocking scheme:

- Two large ISP's (Telstra and Optus) continue to actively block;
- One network gateway manufacturer ([redacted] [redacted]) is incorporating the blocking capability into their product and it is being utilised by customers;
- One small ISP ([redacted]) no longer blocking as the entity has subsumed by a larger ISP upon purchase in late 2012;
- Two large ISP ([redacted]) continue technical preparations to activate blocking with both anticipating commencement by early February 2013;
- One medium size ISP ([redacted]) has not responded to a Section 313 Notice;
- One large ISP ([redacted]) has refused to comply with a Section 313 Notice and the matter has been referred to ACMA for adjudication;

- Norfolk Island Telecom has commenced technical preparation for blocking after they approached AFP to participate in the scheme. This ISP is not subject to the *Telecommunications Act 1997* and is voluntarily participating.

The primary method of distributing the 'worst of' list remains via a secure FTP server. No problems have been reported by the ISP's. Internally, the FTP server is maintained by a HTCO member located in Melbourne office. This member advised that consideration should be given to reviewing the FTP server situation. The current FTP server set up was designed and instituted as an interim measure until a permanent solution was devised/installed. The member advises the FTP server is operating perfectly, however it does not contain any redundancy measures in regards to web connectivity or data. Additionally, the ongoing increase in participating ISP's will generate a corresponding increase the workload of the member in administrating the access and security of the FTP server, which may not be sustainable in the long term.

No complaint regarding either the operation of blocking scheme itself or websites which are being blocked has been received by the AFP from the public, ISP's or Interpol.

As advised to the DBCDE Cyber Working Group in September 2012, development of a referral to counselling link on the stop page has commenced. Interpol confirmed they encourage such links on the stop page. Informal consultation with AFP investigators, psychologists, legal and with ISP's and NGO's operating in the field suggest the most effective (and least contentious) is text which highlights any medical/psychological consultation is not automatically reported to authorities and provides a link to identify a medical professional. Consequently, discussions have been initiated with the Queensland branch of the Australian Medical Association to embed a link on the stop page to their "locate a doctor" website.

On 9 November 2012, the Communications Minister (Mr Conroy) released a media statement publicly supporting the Interpol 'worst of' blocking scheme and formally disregarding the proposed mandatory filter scheme.

Although outside of the review period, it is worth noting that on 14 January 2013 a further 12 section 313 notices were issued to ISPs. At time of writing, 8 have indicated they will participate with 3 having commenced technical preparations.

Resource implications:

Nil additional human resources continue the Interpol 'worst of' list blocking scheme. The scheme has yet to create a detectable increase of referrals to Law enforcement.

Consultation:

Interpol Trafficking in Human beings Sub-Directorate [redacted]

Expected Reaction:

Political and Media interest in the scheme is remains high, following the endorsement of the blocking scheme by the Communications Minister in November 2012. Some early groundswell is appearing in some elements of the electronic media for increased transparency or civilian oversight of the scheme.

Recommendation:

- Continue to operate the Interpol 'worst of' list blocking scheme;
- Continue to add ISPs to the scheme;
- Commence an internal review of the FTP server currently in use.

[redacted]
Child Protection Operations

29 January 2013