
# Position Paper

# on

# Internet Filtering

# and

# the DIA's Digital Child Exploitation Filtering System

**26 January 2010**

# Introduction

In August 2009 InternetNZ created a Working Party to formulate its position on Internet filtering and consider specifically the Department of Internal Affairs' Digital Child Exploitation Filtering System.

InternetNZ supports consideration of all avenues in the effort to stamp out the scourge of child abuse. It is excellent to see that the Government is attempting to take preventative action rather than be "the ambulance at the bottom of the cliff". However, InternetNZ has significant reservations about the proposed approach.

Any proposed filter, including that developed by the DIA, disrupts the end-to-end principle of Internet operations; creates privacy concerns; and risks giving people false security about the level of protection they have from child abuse material.

InternetNZ does not support centrally operated filtering in New Zealand.

This paper explains the background to this position. It is divided into five sections:

- The first deals with principles that InternetNZ considers important in any discussion of filtering.
- The second is a discussion of the principles that guide InternetNZ's response to filtering.
- The third considers the costs and benefits of the DIA's filtering system.
- The fourth looks at the technical and operational risks in implementation of the DIA's filter.
- The fifth summarises InternetNZ's view of filtering and the DIA filtering system.

**About InternetNZ:**

The mission of InternetNZ (Internet New Zealand Inc) is to protect and promote the Internet for New Zealand. We advocate the ongoing development of an open and uncaptureable Internet, available to all New Zealanders.

The Society is non-partisan and is an advocate for Internet, and related telecommunications, public and technical policy issues on behalf of the Internet Community in New Zealand - both users and the Industry as a whole.

# 1. Principles

### End-to-end

The "*end-to-end principle*" is the fundamental principle that InternetNZ supports in advancing an Internet that is open and uncaptureable. This means the citizen on the end of an Internet access service can access the whole Internet without obstruction. InternetNZ does not support policy or practice that disrupts or degrades the end-to-end Internet. This is fundamental to ensuring the network remains an open platform for innovation and development and continues to benefit from the economies of scale provided by keeping intelligence at the edge of the network.

### Illegal content

InternetNZ does not support or condone the presence of illegal content on the Internet. Child abuse material is clearly illegal and abhorrent. Consumers should have ready access to products and services that reduce the risk of access to illegal and abhorrent material on the Internet. ISPs should assist their customers through provision of, and information about, such products and services. Consumers should not be led to believe that filtering products and services can be 100 per cent successful in protecting them.

### Private communications

Communication is a fundamental human function that has been extended by technology. Due to the face-to-face origins of our communications, privacy is an expectation - it is possible in face-to-face conversation to see who is within earshot. Violation of privacy, eavesdropping, bugging, letter opening, and line tapping have always been regarded with distrust and distaste. The expectation of privacy has only been violated by the State under significant restraint by the judiciary in the most serious of cases.

### Implications of these principles

On balance, considering the principles set out above, InternetNZ cannot support centrally operated filtering of the Internet. Filtering should be implemented by individual choice and in a way which does not compromise the end-to-end principle. A system that diverts legitimate traffic could easily be extended to filter undesired political comment or other content that is less repugnant to the community than child abuse material is.

Such filtering disrupts the end-to-end Internet; puts in place a technology that can be used for purposes that are incompatible with a free and democratic society; and creates a risk that, even if introduced as a voluntary system, the filter may well end up covering all Internet users in New Zealand and/or be mandated. In general, InternetNZ prefers that citizens are educated about the availability and quality of filtering services and offered these services by their service providers.

# 2. General discussion of DIA system

Having considered from a principled standpoint above, we apply below the principles in respect to a filtering system of the type the DIA is proposing, to see if there are mitigating factors.

### End-to-end

A centrally-operated filtering system that diverts legitimate traffic alongside illegitimate traffic will to some degree degrade the end-to-end principle. The DIA system uses IP routing to divert a wider list of addresses than the specific content it seeks to block.

The DIA has stated that for its solution there will be no impact on performance. However it is unknown in practice what the impact will be and how services will be affected, particularly if there is wide adoption of the service. Customers should be made aware if their legitimate traffic is being diverted, as any performance degradation may be otherwise unexplained by their ISP.

ISPs could choose to run two parallel internal networks – one connected to the DIA system and one not. Customers could choose which network they selected. This would also give an opportunity, among other things, to consider the performance impact of the filtering system but may be an expensive option for ISPs.

### Illegal content

There are a variety of ways to set up a filter. Options include individual desktop solutions, hosted individual solutions from third parties or ISPs, voluntary filtering across all or a subset of an ISP's customers or a mandatory requirement on ISPs. InternetNZ believes that ISPs should assist citizens in being safe on the Internet through provision of (or advice about) desktop or hosted filtering solutions.

Where an ISP makes a blanket decision to adopt a filtering system for a segment or all of its customers, it is making a choice on their behalf. If ISPs choose this then they must be open with their customers about the fact they are using the filter. Whatever system is chosen, ISPs should advise their customers that no filtering technology is fail safe.

### Private communications

It is a concern that the DIA filtering system has been developed with no particular statutory mandate, creating a readily exploitable "thin end of the wedge" in respect to potential extension of scope. This would also appear to sidestep the checks and balances that apply to censorship of literature and films.

We note reports that in the UK an initially voluntary filtering system is now to be made mandatory and would be very concerned if *de facto* or *de jure*, the DIA's or any filtering system were to become mandatory. In a legal sense we believe a mandatory filter would require primary legislation.

However, in a de facto sense it will be difficult, where a voluntary solution is provided by the Government, for ISPs to take a position that they will not filter for child abuse material. Hence we could anticipate a very wide adoption.

We cannot support the blanket imposition of centrally operated filtering, particularly because it makes the community vulnerable to scope extension into less clear cut areas.

## 3. Costs and benefits

The major benefit of a filtering system is that some people will not access child abuse material that they would otherwise have accessed. This is without question a benefit: the production and distribution of child abuse material follows from and supports real harm to real people.

This benefit is however severely qualified by caveats that are mentioned in the draft Code paper to which this submission is responding. Sections 8 ("What the system won't do") and 9 (Safety Message) note the following issues:

- Website filtering is only partially effective – it does not prevent the production of child abuse material, the exploitation of children, and is only effective once the material has been discovered and filtered by the DIA.
- Website filtering can be evaded – any person with a reasonable degree of technical skill can evade the filter and obtain the material in any case.
- Most illegal material of this nature is traded on peer-to-peer networks or in chatrooms, which are not covered by this filter.
- Due to its low incidence, accidental viewing of such material is not a major source of harm for the population.
- Parents could be given a false sense of security through hearing about the operation of a filter, and the Department notes that parental supervision of Internet use is the best guarantee of online safety for kids.

Given these caveats, it is apparent that the benefit accruing from the filter is very narrow. Only a non-technically savvy user who was using the World Wide Web to seek child abuse material by downloading web pages (this system does not address peer-to-peer or chat rooms) would be stopped by the filter from accessing known child abuse material.

In considering the costs of the filter, these include:

- The cost to the Government of setting up and maintaining the system and associated tasks.
- The cost to ISPs of reconfiguring their networks to pass routing requests through to the DIA and of the customer information management task
- Potential cost incurred through error in the system, whether through inclusion of non-infringing websites or collateral damage from the technical breakdown of the system.
- Potential cost to society if the system is extended later beyond the original mandate.

# 4. Technical and operational risks

If the DIA is intent on proceeding with the filtering system in spite of issues raised in the preceding discussion then the risks of doing so should be seriously considered.

### Stability

The DIA system is a bottleneck for the diverted traffic, whether to illegitimate traffic or to legitimate sites served from the same IP addresses. This could impair the stability of the Internet, by creating traffic distortion or disruption and a single point of failure. Bugs in the system that broadcasts routes could cause the DIA systems to be swamped. Failures in DIA fallover systems could leave legitimate traffic essentially blocked (routed to a down DIA system).

### Expansion of Interceptions

Routing of legitimate traffic to a Government agency creates potential for misuse of the process, irrespective of best intentions. For example, the Government could reroute traffic to identify visitors to activist websites it was suspicious of. This can only be mitigated by publicising the list of diverted IP addresses and the domains to which they correspond.

### Confidentiality

The system as currently defined does not keep identifying information about the intercepted requests, as it is intended to serve as an educative early brake for the slippery slope that ends in viewing of child abuse material. Because of popup and popunder ads, malware, and shared wifi, not every web page fetched from an IP address has been requested by the person who pays for that IP address's Internet connection. The risk is that information, such as IP address, will be logged and cast suspicion upon a user. Regular technical audits are necessary to ensure the system is not misused in this way.

### Scope Creep

To some degree, the list of objectionable sites will be able to be reverse engineered. If the list of objectionable sites is to be treated as confidential then, to the degree that it can be maintained as such, there is a risk of error and non-notified scope creep. If there is to be a secret list, there must be truly independent oversight of that list and with strict processes and proper resourcing to maintain its integrity. For example, acknowledging that the material itself is not subject matter that other Government agencies will wish their staff to have to view, it would be useful to have the Office of the Auditor General or the Office of Film and Literature Classification check the processes that are applied, or have the audit performed by another nations' investigative unit.

**Arms race**

Using a technological solution to prevent access to child abuse sites may have the unintended side effect of encouraging more use of technology such as encryption, ultimately making it harder for the DIA to do its job in this and related areas such as P2P.

**Misleading impressions**

There is a risk that parents may assume the filter is broader and more comprehensive than it is. A significant communications effort will be required from the Government to advise parents that the filtering being applied to their web feed is not perfect and does not cover all objectionable content let alone all child abuse material. NetSafe would be a suitable organisation to advise and assist in such a communications project.

Further, the public may begin to believe that website filtering of child abuse material is a more effective tool against child abuse than it actually is, impacting on proposals for funding of services or solutions that may be more effective yet cost more.

# 5. Summary

InternetNZ supports a safe environment for people online and supports the Government's aims in fighting child abuse. However, any centrally operated filter, including that developed by the DIA, disrupts the end-to-end principle of Internet operations; creates privacy concerns; and risks giving people false security about the level of protection they have from child abuse material. It is not subject to the usual checks and balances that apply to the censorship of other broadcast or published media, film or literature.

For these reasons, InternetNZ does not support the proposed filtering system developed by the DIA.

InternetNZ is very concerned about the lack of analysis or apparent consideration of total cost in the proposed filtering scheme, particularly where that may be incurred on wider society through error or scope creep. In respect to these, InternetNZ regards the risks to the nature of the Internet and to democratic society as too high to justify introduction of the system as designed.

InternetNZ is also concerned that the DIA is about to introduce this filtering system, given the following matters:

- its own documentation says website filtering is largely ineffective and futile in respect to child abuse material;
- the lack of evidence in respect to the anticipated impact of the filter on the larger problem; and
- the potential that it will encourage more encryption to the detriment of law enforcement.

**InternetNZ proposes that a study be undertaken to pinpoint the level and nature of the problem of accessing child abuse material on websites and whether there are better ways of addressing it, such as supporting ISPs in providing individual voluntary filtering, and in educating the public.**

If the filtering solution is proceeded with, regardless of these conclusions, then consequential issues emerge involving confidentiality of the list and external auditing. In InternetNZ's view the cost of confidentiality in terms of the loss of transparency and loss in trust in Government is of serious concern. InternetNZ will lodge a formal submission responding to the Department's recently published draft Code of Practice, which deals with some of these issues.

Furthermore if an attempt is made to have a confidential list then there must be a solid process of external auditing involving, for example, the Office of the Auditor General and/or the Office of Film and Literature Classification, with public disclosure of any deviations from the criteria for inclusion on the list.

InternetNZ offers these comments in good faith and is happy to discuss the points made with officials in the Department or elsewhere. In keeping with our open and transparent approach, this submission will be published on our website and to media after it is lodged.

With many thanks for your consideration,

Yours sincerely,

Jordan Carter
**Policy Director**

+64 4 495 2118, jordan@internetnz.net.nz