



## **Mandatory ISP Level Filtering**

### **Submission to the Department of Broadband, Communications & Digital Economy**

#### **Summary**

Google welcomes the opportunity to provide comments in response to the Mandatory ISP level filtering discussion paper released in December 2009<sup>1</sup>.

The Internet has evolved in recent years into a vital global platform for enabling greater access to information and free expression and so the proposal to implement mandatory ISP level filtering of online content is a significant Australian public policy issue that requires robust, open discussion.

In considering the Government's plans for Mandatory ISP level filtering we have listened to many views, but most importantly those of our users. We have talked directly with parents around Australia about their views on ISP level filtering. The strong view from parents was that the Government's proposal goes too far and would take away their freedom of choice around what information they and their children can access. The importance of a better effort to educate parents and children about online safety was repeatedly highlighted as the area where most effort should be focused.

As the Government has positioned Mandatory ISP Level Filtering as part of an overall policy approach to online safety<sup>2</sup>, we start our submission by looking at how we address this vitally important area. In short, when it comes to online safety, Google's approach is built around three key areas educating people about how to stay safe online, empowering people with tools (such as the recently-

---

<sup>1</sup> See [http://www.dbcde.gov.au/funding\\_and\\_programs/cybersafety\\_plan/transparency\\_measures](http://www.dbcde.gov.au/funding_and_programs/cybersafety_plan/transparency_measures)

<sup>2</sup> See [http://www.minister.dbcde.gov.au/media/media\\_releases/2009/115/](http://www.minister.dbcde.gov.au/media/media_releases/2009/115/)

launched Safety Mode on YouTube) to help them manage their online experience, and co-operation with law enforcement and industry partners.

In December 2009 the Government announced details of their plans to introduce mandatory ISP level filtering of Refused Classification (RC) content. As this announcement was the first formal confirmation of this important policy, we are taking this opportunity to respond to the entirety of the Government's filtering announcement.

Our primary concern is that the scope of content to be filtered is too wide. At Google we have a bias in favour of people's right to free expression. While we recognise that protecting the free exchange of ideas and information cannot be [without some limits](#), we believe that more information generally means more choice, more freedom and ultimately more power for the individual.

Some limits, like child pornography, are obvious. No Australian wants that to be available – and we agree. Google, like many other Internet companies, has a global, all-product ban against child sexual abuse material, which is illegal in almost every country, and we filter out this content from our search results and remove it from our products. But moving to a mandatory ISP level filtering regime with a scope that goes well beyond such material is heavy handed and can raise genuine questions about restrictions on access to information.

Another key concern is that the implementation of a mandatory filtering regime - across all of Australia's hundreds of ISPs, millions of Internet users, and billions of web pages accessed - is a massive undertaking which could negatively impact user access speeds.

Furthermore, the filtering of material from high-volume sites (for example Wikipedia, YouTube, Facebook, and Twitter) appears to not be technologically possible, as it would have such a serious impact on Internet access. There appears to be an expectation that such sites would voluntarily agree to remove or locally block all content judged to be RC under the Government's proposed system.

We believe it is important to clearly state our view on this issue. YouTube is a platform for free expression. We have clear policies about what is allowed and not allowed on the site. For example, we do not permit hate speech or sexually explicit material, and all videos uploaded must comply with our Community Guidelines. Like all law-abiding companies, YouTube complies with the laws in the countries in which we operate. When we receive a valid legal request like a court order to remove content alleged to violate local laws, we first check that the request complies with the law, and we will seek to narrow it if the request is overly broad. Beyond these clearly defined parameters, we will not remove material from YouTube.

We have a number of other concerns, including that filtering may give a false sense of security to parents, it could damage Australia's international reputation, and it can be easily circumvented..

We look forward to engaging further with Government on these issues.

## **About Google Australia**

Google's mission is to organise the world's information and make it universally accessible and useful. This means giving our users around the world access to the information they want, from the widest variety of sources, wherever they are. We believe this brings people greater choices, new freedoms, and ultimately more power.

Google Australia was one of the first Google offices. In June 2009, the Governor-General opened Google Australia's new headquarters in Sydney. It's now a vital sales hub for the region and R&D centre for the world. We have 350 employees in Australia in sales, engineering, and business support, and some of Google's most exciting new projects - like Google Wave - were developed here in Australia.

We help millions of Australians connect with information, customers, audiences, users and colleagues in Australia and throughout the world. Thousands of Australian businesses use Google products - Search, AdWords, YouTube, Google Maps and Google Apps - as a core part of their business. Online tools help businesses connect with local and overseas customers, stand out in competitive local markets and improve their workplace productivity. Marketing with Google AdWords allows businesses to maintain effective, targeted ad campaigns with virtually no start up costs. In particular, AdWords helps small and medium businesses grow their customer base and connect directly with people in Australia and around the world. We also help local online publishers make money from their content through Google AdSense. These tools grow the web ecosystem and power the digital economy.

Google's Australian engineers develop a wide range of global and local products and have an outstanding track record of innovative products and services. Our local engineers work on pioneering innovations in geospatial web applications, collaborative software, network infrastructure and more. Recent global products developed in Australia include Google Wave, Google Maps, and Real Estate Search for Google Maps. Our engineers localise Google products to make them available and relevant for Australians, such as Real Estate Search, Traffic and Transit in Google Maps.

## **Our Approach to Online Safety**

As the Government has positioned Mandatory ISP Level Filtering as part of an overall policy approach to online safety<sup>3</sup>, we think it's important to start this submission by looking at how we address this vitally important area. When it comes to online safety, Google's approach is built around three key areas:

### **Educating** people about how to stay safe online.

- We provide an online safety resource, Tips for Online Safety ([www.google.com/familysafety](http://www.google.com/familysafety)), which offers resources for families on how to use Google safely, and quick links to tools like Google SafeSearch.
- We have a localised Safety Centre for Australian users of YouTube, linked to from each page of YouTube, which provides information about a range of issues including YouTube community guidelines violations, cyber citizenship, teen safety, hateful content, harassment and cyberbullying
- Supporting educational efforts to increase awareness about child safety online. In Australia and New Zealand we support non-profit organisations including the National Association for Prevention of Child Abuse and Neglect (NAPCAN), The Allannah and Madelaine Foundation, KidsHelpline, Inspire Foundation, Bravehearts and Hector's World. We support these organisations in a number of ways, including by providing online public service announcements that promote access to resources about safety and other educational efforts. We actively support their efforts to raise awareness of child safety issues.

### **Empowering** people with tools to help them manage their online experience.

- Google SafeSearch is tool that empowers our users to filter unwanted content out of their search results. We understand that many people don't want to have adult content included in their search results, especially when children are using the computer. Google has developed its own SafeSearch filter, which uses advanced technology to block pornographic and explicit content from search results. Users can customise their SafeSearch settings by clicking on the "Preferences" link to the right of the search box on Google.com.
- On 11 February 2010, we launched YouTube [Safety Mode](#), an opt-in setting that helps screen out potentially objectionable content that our users may prefer not to see or don't want others in their family to stumble across while enjoying YouTube.

---

<sup>3</sup> See [http://www.minister.dbcde.gov.au/media/media\\_releases/2009/115/](http://www.minister.dbcde.gov.au/media/media_releases/2009/115/)

## **Co-operation with law enforcement and industry partners.**

- Removing child sexual abuse images. We use databases from designated organisations listing websites suspected of containing child sexual abuse images in order to remove these illegal URLs from our search results.
- Combating abuse. When we discover child pornography or are made aware of it, we respond quickly to remove it and report it to the National Center for Missing and Exploited Children or the appropriate law enforcement authorities.
- Cooperation with law enforcement to combat child exploitation. Google cooperates with child safety investigations, and has a legal team devoted to this effort 24 hours a day, 7 days a week. We respond to thousands of law enforcement requests for assistance, and hundreds of subpoenas, each year.

## **Our Content Policies on YouTube**

The popularity of YouTube in Australia gives it a high relevance in this debate. At YouTube we're committed to making the internet safe and enjoyable for everyone.

YouTube is a user-generated video sharing platform around which communities form, have discussion and interact. Over 6 million Australians use YouTube each month. These users view over 170 million pages each month. YouTube is the platform for a wealth of content, including premium media, educational, political, citizen journalism and Government communications. And it's growing rapidly - every minute 20 hours of video are uploaded to YouTube.

We maintain the integrity of YouTube through clear policies regarding what is and is not acceptable on the site; and robust enforcement mechanisms for these policies.

First, in relation to our clear policies regarding what is and is not acceptable:

- All users of YouTube must abide by the terms of use and the [YouTube Community Guidelines](http://www.youtube.com/t/community_guidelines), which are written in easy-to-understand language. They are designed to provide users with clear rules on what content is acceptable and what is not. For example, hate speech, pornography, images of drug abuse, and graphic violence cannot be uploaded to the site. The Community Guidelines are linked to on every page and are available at: [http://www.youtube.com/t/community\\_guidelines](http://www.youtube.com/t/community_guidelines)

Second, in relation to enforcement of these policies:

- YouTube has developed an innovative, reliable and user-friendly community policing system - users report potential violations of the YouTube Community Guidelines by “flagging” a video.
- Flagged videos are reviewed for compliance with the Community Guidelines 24 hours a day, seven days a week.
- Our YouTube review teams receive extensive training on an ongoing basis, including from law enforcement organisations and child safety organisations. This training enables our team to effectively and efficiently respond to flagged videos.
- When a video does not comply with the Community Guidelines, it will be removed from the site. When a video is removed, we advise the user and send them some tips to remind them of the rules regarding what content can be posted to YouTube. In appropriate circumstances, we will refer the matter to law enforcement.
- Users who repeatedly violate the YouTube Community Guidelines have their YouTube accounts terminated.
- YouTube has also developed digital hashing technologies to prevent the re-upload of files that have been removed, and is continually developing tools to promote this goal.
- In addition to the flagging system, users are able to contact YouTube directly with privacy, harassment, or bullying complaints through the [Help & Safety Tool](#).

### **The Government’s Proposal for Mandatory ISP Level Filtering Policy**

On 15 December 2009 Minister Conroy announced details of the Government's plans to introduce mandatory ISP level filtering of Refused Classification (RC) content<sup>4</sup>.

The Government plans to introduce legislative amendments to the Broadcasting Services Act to require all ISPs to block RC content hosted on overseas servers. The Government expects to introduce draft legislation during the Autumn 2010 parliamentary sittings. It is planned that there will be a twelve months process of implementation after the passage of the legislation.

We understand that the RC Content list will be compiled through a public complaints mechanism. The Government will also add the specific Internet addresses (URLs) of known child abuse material through sharing lists with highly regarded international agencies after an assessment of the rigour and accountability of classification processes used by these agencies.

---

<sup>4</sup> See [http://www.minister.dbcde.gov.au/media/media\\_releases/2009/115/](http://www.minister.dbcde.gov.au/media/media_releases/2009/115/)

We further understand that the Department of Broadband, Communications and the Digital Economy (DBCDE) and the Australian Communications & Media Authority (ACMA) will consult with ISPs on the detailed implementation of ISP-level filtering, including the updating of relevant industry Codes of Practice.

Further, the Government will allocate funds to the ACMA to enhance the security of the RC Content list and to automate its transmission to ISPs.

The Minister released publicly the Enex Test Laboratory report into the pilot trial of Internet Service Provider (ISP)-level filtering.

The underlying policy basis for the proposal, as outlined by the Minister in his statement, was that “ISP filtering reduces the risk of Australians being inadvertently exposed to RC-rated material when they are online”.

As the December announcement was the first formal confirmation of this important policy, we are taking this opportunity to respond to the entirety of the government's filtering announcement.

### **Our Views on The Proposals for Mandatory ISP Level Filtering**

In response to the Government's announcement, we issued our first substantive public comment on plans for Mandatory ISP Level Filtering via a [blog](#) posting on 16 December 2009. The blog focused on our primary concern, which is the wide range of content which could be blocked by mandatory filtering of RC content. In this section, we expand that commentary and highlight other concerns that we have.

#### **Filtering would block some important content**

Our primary concern is that the scope of content to be filtered is too wide.

At Google we have a bias in favour of people's right to free expression. While we recognise that protecting the free exchange of ideas and information cannot be [without some limits](#), we believe that more information generally means more choice, more freedom and ultimately more power for the individual.

Some limits, like child pornography, are obvious. No Australian wants that to be available – and we agree. Google, like many other Internet companies, has a global, all-product ban against child sexual abuse material and we filter out this content from our search results and remove it from our products. But moving to a mandatory ISP level filtering regime with a scope that goes well beyond such material is heavy handed and can raise genuine questions about restrictions on access to information.

Last year's report by Professors Catharine Lumby , Lelia Green, and John Hartley, [Untangling The Net: The Scope of Content Caught By Mandatory Internet Filtering](#)<sup>5</sup> found that a wide scope of content could be prohibited under the proposed filtering regime. RC is a broad category of content that includes not just child sexual abuse material but also socially and politically controversial material -- for example, educational content on safer drug use -- as well as the grey realms of material instructing in any crime, including politically controversial crimes such as euthanasia. This type of content may be unpleasant and unpalatable but we believe that the Government should not mandate the blocking of information which can inform debate of controversial issues.

Our services, particularly YouTube, contain a substantial amount of material related to controversial issues, some of which could be rated as RC. The Government's policy for filtering represents a direct threat to content uploaded by YouTube users and we are committed to advocating on behalf of our users and their right to express their views and gain access to information.

Exposing politically controversial topics for public debate is vital for democracy. Homosexuality was a [crime in Australia](#) until 1976 in ACT, until 1984 in NSW, and 1997 in Tasmania. Political and social norms change over time and benefit from intense public scrutiny and debate. The openness of the Internet makes this scrutiny and debate all the more possible, and should be protected.

The Constitution of Australia does not protect freedom of expression (other than a limited guarantee for political discourse) and as a result Australia does not have developed case law about acceptable limits to freedom of expression. There is a significant risk that filtering applied today to RC content could readily be extended by future governments to other forms of expression, whether related to sexual content or violence or not.

## **Negative Impact on Users**

The implementation of a mandatory filtering regime - across all of Australia's hundreds of ISPs, millions of Internet users, and billions of web pages accessed - is a massive undertaking and we remain concerned about the potential impact on user access speeds from filtering.

The Government's own analysis has acknowledged certain technical risks and we focus on two areas in this section.

Firstly, the filtering of material from high-volume sites (e.g. Wikipedia, YouTube, Facebook, Twitter) appears to not be technologically possible, as it would have such a serious impact on Internet access speeds.

---

<sup>5</sup> See <http://www.scribd.com/doc/24138351/Untangling-the-Net-The-Scope-of-Content-Caught-by-Mandatory-Internet-Filtering>

Minister Conroy made remarks acknowledging this reality at a Senate Estimates committee hearing earlier this week.<sup>6</sup>

The Enex Report also acknowledges this issue:

“However, in situations where there is a potential for very high traffic sites, such as YouTube, to have pages on the filtering list, this could result in significantly higher traffic rates passing through the filter, even though the specific pages being accessed are not those on the blacklist. This could cause additional load on the filtering infrastructure and subsequent performance bottlenecks”<sup>7</sup>

In addition, a report from Telstra highlights this issue in two separate references:

“It was noted that it is possible for the solution to fail if pages from a heavily trafficked site are added to the blacklist. This is due to volume limitations of a typical proxy server. These sites serve video content to end users. The volume of video traffic would be likely to overwhelm a proxy server.”<sup>8</sup>

and later in the same report (page 13)

*“Video clips from high traffic sites are very popular with typical Internet users, accounting for up to 10% of traffic. If any content from sites distributing these video clips were to appear on the blacklist the blocking solution would fail because 10% of 40Gb/s of traffic is greater than the 1Gb/s capacity of a proxy server.*

*This mode of failure is triggered by large volumes of data being directed via the proxy server. Popular video content sites (both now and future) are seen as the major problem here.*

*A mitigation to this problem is provided by Nomium’s software in the form of a “white list”. This feature is able to prevent an operator from adding “highly trafficked” domains to the blacklist.*

*Of course, this feature is optional and assumes a policy of not needing to block URL’s existing on highly trafficked domains.*

*The alternative to this approach is to block the entire domain and accept the end user consequences of over-blocking.”*

---

<sup>6</sup> See page ECA 88 of comments by Minister Conroy at the Senate Environment, Communications and the Arts Legislation Committee, Monday 8 February 2010 at <http://www.aph.gov.au/hansard/senate/committee/S12743.pdf>

<sup>7</sup> See page 19 at [http://www.dbcde.gov.au/funding\\_and\\_programs/cybersafety\\_plan/internet\\_service\\_provider\\_isp\\_filtering/isp\\_filtering\\_live\\_pilot](http://www.dbcde.gov.au/funding_and_programs/cybersafety_plan/internet_service_provider_isp_filtering/isp_filtering_live_pilot)

<sup>8</sup> See page 4 at <http://exchange.telstra.com.au/wp-content/uploads/2009/12/TBT-final-report1.pdf>

The issue is also acknowledged in the Frequently Asked Questions issued by the Department of Broadband as part of the December announcements on ISP filtering<sup>9</sup>. The FAQ notes state that consideration is being given to exempting high traffic sites from having their material included on the RC Content list if they implement arrangements to either take down identified RC-rated content or to block it from access by Internet protocol addresses in Australia.

These notes and more recent public comments by Minister Conroy (at a Senate committee hearing earlier this week<sup>10</sup>) point to an expectation that such sites would voluntarily agree to remove or locally block all content judged to be RC under the government's proposed system. With the entirety of 'Refused Classification' content coming within the scope of filtering, the likelihood of material on high volumes sites being assessed as RC and appearing on the blacklist is higher.

We believe it is important to offer a very clear view on this issue. As highlighted earlier in this document, YouTube is a platform for free expression. We have clear policies about what is allowed and not allowed on the site. For example, we do not permit hate speech or sexually explicit material, and all videos uploaded must comply with our Community Guidelines. Like all law-abiding companies, YouTube complies with the laws in the countries in which we operate. When we receive a valid legal request like a court order to remove content alleged to violate local laws, we first check that the request complies with the law, and we will seek to narrow it if the request is overly broad. Beyond these clearly defined parameters, we will not remove material from YouTube.

A second technical issue in relation to filtering is that the pilot/trials seemed to not follow the DBCDE's own 2008 [Technical Testing Framework](#) for ISP level filtering<sup>11</sup>. There are a number of important elements of testing which seem not to have been covered in the trials.

- testing a blacklist of up to 10,000 urls
- testing a representative cross section of ISPs
- testing new technologies such as IPv6
- gathering the costs of filtering

There is a risk that these factors limit the usefulness of the trials.

---

<sup>9</sup> See question 16 at [http://www.dbcde.gov.au/funding\\_and\\_programs/cybersafety\\_plan/internet\\_service\\_provider\\_isp\\_filtering/isp\\_filtering\\_live\\_pilot/isp\\_filtering\\_-\\_frequently\\_asked\\_questions](http://www.dbcde.gov.au/funding_and_programs/cybersafety_plan/internet_service_provider_isp_filtering/isp_filtering_live_pilot/isp_filtering_-_frequently_asked_questions)

<sup>10</sup> See ECA 90 at <http://www.aph.gov.au/hansard/senate/commtee/S12743.pdf>

<sup>11</sup> See [http://www.dbcde.gov.au/\\_data/assets/pdf\\_file/0006/89160/technical-testing-framework.pdf](http://www.dbcde.gov.au/_data/assets/pdf_file/0006/89160/technical-testing-framework.pdf)

## **The Broad Scope of Filtering drives a wider range of concerns**

Building on the two previous sections, which looked at our concerns with scope and some technical issues, it is worth highlighting briefly a way in which the two elements combine together.

Australia's peer countries worldwide have all considered the same policy issues. The FAQ document on filtering issued by the Department<sup>12</sup> confirms that the UK, Canada, Denmark, Finland and Sweden have all decided to implement systems focused entirely on blocking child sexual abuse material. We also believe that New Zealand is pursuing this path. Instead of drawing on those very relevant international examples, the Government's proposal goes well beyond that scope to the much wider category of RC.

Narrowing the scope of the Government's proposal for filtering would

- be very consistent with international peer countries
- remove or very substantially lessen the risk of material from high volume sites coming within the scope of filtering, thereby relieving the technical difficulty highlighted above
- eliminate most/all of the concerns about government censorship of material

## **Other Concerns**

In considering the Government's plans for Mandatory ISP level filtering we have listened to many views, but most importantly those of our users. We have talked directly with parents around Australia and their strong view is that the Government's proposal goes too far and would take away their freedom of choice around what information they and their children can access. The importance of a better effort to educate parents and children about online safety was repeatedly highlighted as the area where most effort should be focused.

We have a number of other concerns, including the following.

*May Give a False sense of security* - Mandatory ISP Level Filtering fosters dependency of users upon 'someone else' and therefore could create a climate of complacency among users as to safe Internet use. As acknowledged by the Government, filtering is not a 100% accurate solution, it is readily circumvented and it does not address all issues of online safety. Much more likely to promote safe Internet use than Mandatory ISP Level Filtering are:

---

<sup>12</sup> See question 10 at [http://www.dbcde.gov.au/funding\\_and\\_programs/cybersafety\\_plan/internet\\_service\\_provider\\_isp\\_filtering/isp\\_filtering\\_live\\_pilot/isp\\_filtering\\_-\\_frequently\\_asked\\_questions#16.0](http://www.dbcde.gov.au/funding_and_programs/cybersafety_plan/internet_service_provider_isp_filtering/isp_filtering_live_pilot/isp_filtering_-_frequently_asked_questions#16.0)

- user education,
- parental control mechanisms such as appropriate placement of Internet access devices within the home and use of (voluntary) client-side filters,
- public awareness raising campaign; and
- school based education programs.

*Could damage Australia's International Reputation* - Mandatory filtering by Australia could be argued to confer legitimacy upon filtering by other Governments. Australia is rightly regarded as a liberal democracy that balances individual liberty with social responsibility. The Governments of many other countries may justify, by reference to Australia, their use of filtering, their lack of disclosure about what is being filtered, and their political direction of agencies administering filtering.

*Mandatory ISP Level Filtering can be circumvented* – Not just by end users, but also by unscrupulous providers of unacceptable content, who will circumvent mandatory filtered URLs by re-badging those URLs, FTP or other measures to ‘underground’ that content. Further, a large proportion of child sexual abuse material is distributed via peer 2 peer technology which will not be affected by Mandatory ISP Level Filtering.

## **Transparency and Procedural Fairness**

Notwithstanding our clear opposition to the proposed Mandatory ISP level filtering regime, we offer some comments in response to the Government's specific request for views on how best to ensure accountability and transparency in a filtering system. Some high level views are set out in the following section and further detailed comments are offered in the Annex to this document.

### **Challenges in making ‘good decisions’ about mandatory filtering of RC content**

The Government has sought submissions on a number of options for measures to increase accountability and transparency in relation to the process that will lead to a decision to add RC material to the RC content list for Mandatory ISP Level Filtering and the means for reviewing those decisions.

There is a key difference between the current voluntary client-side filter regime, and mandatory ISP level filtering. This difference is, of course, that the decision as to what is be viewed and what is not is moved from a choice made by an individual to a compulsion imposed by a government agency, without transparency to the individual that a decision is being made.

There is, of course, a high level of compulsion that is inherent in implementation of a mandatory filter – the outcome is a national blackout of particular internet content. Use of compulsion rightly calls for special vigilance to ensure that denial of choice is fully justified. Special safeguards are appropriate and necessary where there is also no transparency to the user as to the decision that has been made – in this particular case, as to which URL is to be blocked - and the decision is being made by a government board or other agency and not by the judiciary or another independent body.

These special safeguards should go beyond the customary safeguards in relation to the making of administrative decisions. This is because a number of the safeguards that customarily protect individuals against poor decisions by administrative decision makers are not present in the case of the mandatory filter:

- the users affected by the decision are not even aware that a decision will be made and that they will be affected by the decision, as there is no prior public consultation;
- even if the individual becomes aware that a particular site is being blocked, there is not currently envisaged to be any publication of the case-specific reasons for blocking particular content;
- the discretions to be exercised are inherently broad and subjective.

A regulatory scheme without adequate safeguards also suffers a lack of predictability and certainty. Without these, regulation can never effectively deter an organisation or individual from contravention, as they would not have a sufficient understanding of what the scheme requires.

### **How can the making of ‘good decisions’ be safeguarded?**

Measures applicable to general administrative decisions include:

- decision makers being independent from the political process;
- ensuring that where decision makers seek to apply community standards, those decision makers are broadly representative of the community and the diversity of views within the community;
- decision makers having the necessary training to effectively respond to, investigate and make decisions in regard to complaints, especially where decisions are initially made by delegation;
- measures to ensure procedural fairness, especially notification to the organisation or individual affected that provides an indication of the substance of the complaint, any action that can be taken to address that complaint, and any right to appeal;
- clear criteria for decisions that can be applied consistently and objectively;
- providing reasons for decisions in order to ensure transparency and accountability;

- procedures for multiple levels of review;
- comprehensive documentation of the findings of investigations;
- providing a mechanism for oversight of the decision making body, particularly to ensure that there is special accountability in relation to any aspects of that decision making body's processes or practices in relation to which there is otherwise little or no transparency.

The measures listed above can also be used as criteria to assess whether a particular regulatory scheme adequately achieves transparency, accountability and procedural fairness.

We have already expressed Google's view that special measures, beyond those listed above as applicable to general administrative decisions, are appropriate in the case of decisions to blackout particular internet content by operation of a Mandatory ISP Level Filter.

### **Transparency and procedural fairness**

Transparency is best attained by making persons that will be affected by a decision aware of the procedures for the making of the decision and how it affects them. This involves publishing easily accessible information detailing the way that regulation works and the appeal processes available. Providing reasons for decisions is also effective in helping individuals understand why a decision that affects them was made. With this information, the individual may be more accepting of the decision, and in any case, will be able to make a more directed and efficient appeal, tying into accountability.

Procedural fairness (sometimes called natural justice) requires that an organisation or individual who is affected by an administrative decision is notified that the decision is being made and has a chance to respond and argue their case.

We believe that every person in Australia is affected by a blackout decision. In addition, there is at least one person or organisation, and often two persons or organisations, directly and immediately affected by the decision.

The first person or organisation is the person that posted the content on the Internet. In addition, for social networking and user generated content sites, there will be the operator of the website.

Both the uploader of the content, and (where appropriate) the operator of the site must be considered. In the absence of a complaint or other notice, the operator of a social networking or user generated content site will often not know that RC or potentially RC content has been uploaded to the site.

Publishers of material (for example print publications and video) that are subject to classification are afforded procedural fairness and transparency, and there is no reason to discriminate against an internet content owner.

A further reason making it imperative to notify, is that ISP level blocking of particular pages at high volume sites may lead to a significant reduction in speed of access to other pages at those sites. The performance of social networking and user generated content sites may be severely and adversely affected by a particular page being added to the RC content list.

Further, Classification Guidelines that were developed principally for entertainment “films” will be applied to instructional, educational, scientific or current affairs video material available on the Internet. As already noted, RC is a broad category of content that includes not just child sexual abuse material but also socially and politically controversial material - for example, educational content on safer drug use - as well as the grey realms of material instructing in any crime, including politically controversial crimes such as euthanasia. Decisions in relation to instructional, educational, scientific or current affairs video material will often be much more complex than in relation to entertainment “films”: scenes of war or terrorist activity may “offensively depict” “real violence” and rate RC when the video is not in any way “gratuitous violence” or posted for entertainment. It follows that decisions should be carefully reasoned and explained, as a safeguard to ensure that the decision maker is working through the right decision making process to make a ‘good decision’, and also to explain to a site operator why the content would be blocked.

Google therefore considers that any Mandatory ISP Level Filtering scheme should involve:

- prior notice to the apparent site owner as to a complaint;
- an explanation to the apparent site owner as to why the complaint may be considered to have a reasonable basis (i.e. the nature of the contravention of the Classification Guidelines, sufficiently categorised to enable the site owner to understand what is the nature of the alleged contravention of the Classification Guidelines;
- a period to implement take down before any blocking is imposed. Except in egregious cases such as child abuse and other manifestly criminal activity, a reasonable period should be allowed for the takedown to be implemented
- an explanation as to the review or appeal process available. This might include both an expedited process for escalation and review of any delegated decision prior to the blackout coming into operation, and a full merits review available after takedown;

Once the site is added to the RC content list, a blocking notice should be displayed to a user endeavouring to access the page, stating that the page is

blocked and (at least in summary form) why it is blocked, and ideally linking to a site at which sets out:

- an explanation of what the Mandatory ISP Level Filtering scheme is,
- the Classification Guidelines and FAQs about the Guidelines, and
- information about why the particular page was blocked.
- notification of the procedure whereby an end-user may seek review of the decision to filter the content.

We note that this would replicate for the Internet many of the features of the current classification scheme as applied to films and print publications. One feature of the current classification scheme for films and print publications is a high level of transparency as to reasons for decisions.

We again stress that:

- transparency for a site owner is particularly important given that many site owners operate social networking and user generated content sites and simply cannot be aware of content posted to their sites until a reasonable period after they are put on notice as to unacceptable content, and
- transparency to the content owner and site owner is also important because the user has no way to know that the blackout has been imposed, or why, unless the user is so informed. If full transparency cannot be effected for content uploaders where they are users of social networking or user generated content sites, it becomes even more critical to achieve it on the site owner side.

## **Accountability**

In *Best-Practice Guide 5: Accountability* (August 2007) the Administrative Review Council (ARC) stresses the importance of accountability and transparency measures, stating that:

“Although accountability processes can at times be burdensome for administrators, the need for them is well accepted in government circles. Factors such as the complexity of legislation and the volume of decision making mean that some decisions will inevitably be incorrect. External scrutiny and review are designed to enable errors to be corrected, to improve the way decisions are made, to ensure transparency, and to engender public confidence in the integrity of government administration.”<sup>13</sup>

---

<sup>13</sup> See page 1 at [http://www.ema.gov.au/agd/WWW/arcHome.nsf/Page/Publications\\_Reports\\_Downloads\\_ARC\\_Best\\_Practice\\_Guide\\_5\\_-\\_Accountability](http://www.ema.gov.au/agd/WWW/arcHome.nsf/Page/Publications_Reports_Downloads_ARC_Best_Practice_Guide_5_-_Accountability)

The ARC recommends that multiple levels of review are provided for administrative decisions. This includes both internal review of the decision by a senior officer of the agency in which the original decision was made, and external review by an independent body or tribunal like the Administrative Appeals Tribunal (AAT), with review by more than one body highly desirable.

Without accountability, decision makers are free to act in whatever way they see fit with no consequences. An unaccountable administrator making a decision that substantially affects the interests of an organisation or individual (for instance, their ability to access information or have others access their information on the Internet) is a cause for great concern.

To ensure accountability, it is imperative that the decision maker be subject to oversight and that an affected organisation or individual has a method to challenge a decision.

It is imperative that decisions about whether content would be classified RC are subject to robust appeal mechanisms. This would include review by the Classification Review Board (CRB) and merits review by the AAT and the courts. Further, standing to apply for review would extend to any organisation or individual who is materially affected by the decision, including the content host, actual content owners and end-users who are blocked from accessing the URL.

Independent oversight of the scheme is equally important to appeal mechanisms. Oversight might involve scrutiny of decisions and their processes by an independent body, such as a retired judge or ombudsman, or by the Parliament, or by a responsible and representative industry body.

The importance of accountability and oversight also means that international lists should be used with significant caution. International lists may be formed without there being any of the accountability measures described above: many countries accept a much lower level of accountability of government agencies and as to decisions of those agencies than Australians have come to expect. Providers of international lists are also not in any way subject to Australian oversight.

## **Annexure - Detailed Comments on Process and Transparency Issues**

In this Annex we outline some more detailed comments for the operation of a Mandatory ISP Level Filtering scheme. These comments attempt to retain as much of the existing structure and procedure of the ACMA and Classification Board (CB) and incorporate the options suggested by the DBCDE, while also ensuring an efficient process which complies with the above-mentioned transparency, accountability and procedural fairness principles.

### **Complaints to be processed by the ACMA**

Our view is that complaints should continue to be received by the ACMA. However, the ACMA would not have the broad discretion to deem material as potentially RC that it does under the current regime. When a complaint is received, the ACMA will ensure that the complaint is in the correct form (such as per cl 37 of Sch 7 of the BSA) and is not frivolous, vexatious or not in good faith. Once satisfied of this, staff members specifically trained in classification in accordance with CB procedures would assess the content of the reported URL against clear criteria in order to determine if there is any possibility that the URL contains RC content.

In the event that the complaint is frivolous, vexatious or not in good faith, or the ACMA is certain that the reported URL does not contain any RC content, the investigation will not progress further.

If the ACMA is of the opinion that the reported URL could possibly contain RC content, the matter is passed on to the CB so that the content can be classified. When the complaint is passed on, the ACMA will notify the content host (the owner of the URL which displays the content) as per the *Content host notification procedure* section below. This initial assessment by the ACMA should be completed as quickly as is possible, but in any case within 2 business days after the complaint is first received. Additionally, the ACMA must produce a short statement of reasons for their decision, for scrutiny by the independent oversight body (see section below).

This system utilises the complaints response system that is already established in the ACMA and combines it with the more transparent classification process of the CB, similar to *Option one* proposed in the DBCDE consultation paper. Ideally, this would ensure that decisions as to the classification of content proceed in a timely manner while still maintaining a high level of transparency, accuracy, and consistency. The fact that the ACMA makes an initial assessment of the content should reduce the number of complaints that pass onto the CB so that it does not become inundated.

### **No filtering to commence until the Classification Board makes its decision**

The suggestion in *Option one* that potentially RC material be placed on the filtering list whilst the CB makes its decision is not consistent with the principles of procedural fairness. The fact that a content host could be subjected to a substantial period of filtering even though that content may eventually be found to be entirely free of any RC material is extremely concerning. The impact of such a long and unwarranted filtering on the business and reputation of the content host could potentially be extreme.

Our view is that no URL should be added to the RC content list for filtering until the content host has a reasonable opportunity to respond to notice (see *Content host notification procedure* below), or in any case, until the CB makes a decision as to whether the reported content is indeed RC (if the content host cannot be notified).

### **Content host notification procedure**

#### *Notification pre-Classification Board decision*

When content is passed on to the CB for a determination of whether it is RC content, the ACMA will be tasked with notifying the organisation hosting the content. This notification should include:

- a statement that the URL in question is currently being assessed by the CB for RC content and potential filtering;
- a description of the substance of the complaint made against URL and the specific content in question;
- a brief explanation or link to an explanation of the decision making process currently underway, the criteria used by the CB to classify the content, and the appeal mechanisms available to the content host in the event that the decision is made to filter the content;
- the procedure for the content host to make submissions directly to the CB in order to support an argument that the content should not be subject to filtering; and
- an opportunity for the content host to voluntarily remove the content and by doing so avoid any filtering of their URL.

The ACMA should attempt to provide the content host with notification in a timely manner. The suggestion in *Option two* of the DBCDE that notification only be extended to content hosts who are “readily identifiable and contactable” is not sufficient as it gives the ACMA too much leeway in not providing notification. Due to the potential for filtering to have a significant impact on the business and reputation of content hosts, in terms of procedural fairness, it is imperative that the content host receives notification.

The content host should be given ample opportunity to consider this notice and make a response, either through submissions to the CB or a voluntary

removal. As such, the URL must not be placed on the list for filtering until (say) 5 days have passed since the content host *received* notification from the ACMA. If it is impossible for the ACMA to notify the content host, then the earliest the URL could be filtered is (say) 3 business days after matter was passed on to the CB. This notification scheme should be able to increase the efficiency of the filtering process. In many, and probably most, cases responsible content hosts will agree to take down the content rather than be subjected to filtering. Furthermore, if the CB was provided with submissions from the content host, they could make a more informed decision, possibly decreasing the necessity for review by the Classification Review Board (CRB)

#### *Notification after the Classification Board decision*

Provided that it is not impossible for the content host to be contacted, the ACMA would provide the content host notice that their URL has been classified RC and has been added to the filtering list. This notice will also include:

- the statement of reasons from the CB;
- the procedure for the content host to apply for review this decision (see *Review by the Classification Review Board* section) and a subsequent review application to the AAT (also see below); and
- the fact that the URL may be removed from the list if the content host provides the ACMA with notice that the RC content has been removed.

#### **All content determinations to be made by the Classification Board**

In our view the decision as to whether a URL contains RC content and should be filtered should rest with the CB, similar to what is suggested in Option one. Once the classification decision has been made, the CB will inform the ACMA of its decision as to whether the URL should be subject to filtering, and provide a short statement of reasons. If the content is indeed found to be RC, the URL will be placed on the RC content list for filtering (provided that the 5 day notice period has ended) The ACMA will then inform the content host as described in the *Content host notification procedure* section.

This is the most effective way to ensure that decisions to filter RC content are made consistently with the practices of the CB. The Board is currently better equipped than the ACMA to make determinations about the classification of content, due to the experience and representative nature of its members. Furthermore, the clear decision making process involved and the availability of review make the determinations of the CB far more transparent and accountable than those of the ACMA. Utilising the CB for this decision would also avoid the necessity of drastically reforming the practices and procedures that the ACMA currently uses to make decisions in regard to content.

A major concern with using the CB is the speed and efficiency of this referral, and the procedural fairness issues that arise as a result. It is clear that the ACMA and CB processes are very different, with the ACMA process constructed to make fast decisions in response to complaints, while the CB is designed for more measured and deliberated determinations. Currently, the only time limitation that the CB is subject to is a 20 day limit on a classification decision. With the possibility of a high volume of complaints to the ACMA and swift referral to the CB, it is not difficult to envisage the CB being inundated with a huge number of classification referrals which it is currently not equipped to deal with in a timely fashion.

This problem can be avoided by accelerating the current CB process and perhaps allocating the CB further resources and staff, or increasing the membership of the CB. Many of the filtering decisions will turn on whether a particular image or short video clip warrants a RC classification. The long process of viewing and discussing a literary work or film in its entirety will usually not be necessary for a decision based the content of a single URL, especially since the original complaint will contain a specific description of the questionable content. While such directed decisions on specified content will often be made quickly, our view is that the CB should have a 5 business day time limit for decision making. This allows for decisions which cannot be made so swiftly (such as long video clips or text) and also the high volume of URLs which may be referred to the CB; If the CB receives submissions from the content host (within the 5 day notification period) then it must consider this material, regardless of whether the Board has already classified the content. If necessary, the time limit for the decision will be extended by 2 days.

One other alteration to the procedure of the CB in this context is the removal of any power for the CB to delegate a decision concerning the classification of content outside the members of the CB. The possibility of such delegation is at odds with the principles of accountability and transparency.

### **The RC content filtering list**

The ACMA will update and distribute the RC content list to the ISPs on a daily basis. The ISPs will be required, either by legislation or an industry code, to filter the URLs contained on the list. To ensure transparency, the ISPs must submit a detailed summary of their filtering procedure to the ACMA. These processes will also be subject to scrutiny by the independent oversight body (see section below) In the event that the content host removes the RC content after the URL has been added to the filtering list, the ACMA must remove the URL from the list, after an assessment of the edited URL, no longer than 10 days after receiving notice of the removal from the content host.

For clarification, it is important to note that in our view, a URL should only be filtered if it actually contains the RC content. A website that provides a link to a

URL containing RC content should never be filtered. This will ensure that public access to information and an organisation's ability to display content are restricted as little as possible while maintaining the filtering of RC content.

### **Incorporation of URLs from international lists**

The incorporation of content from international lists presents a myriad of problems in terms of transparency, accountability and procedural fairness. Overseas agencies are not in any way accountable to the Australian public and may use vastly different criteria to classify content and determine what is to be filtered. While the options suggested by the DBCDE in *Option four* might help assuage these problems, they do not go far enough. Furthermore, it must be ensured that content hosts are given notice that they will be added to the filtering list, a point that is not made clear in *Option four*.

Our view is that URLs from international lists should be added to the filtering list in the same way as URLs which are the subject of an end-user complaint. The ACMA will process these URLs and then provide them to the CB so that any RC content can be identified. The same notification requirements apply, namely notice to the content host before and after the CB makes its decision. This approach is the most effective way to ensure that URLs from international lists are filtered in a manner that accords with the principles of transparency, accountability, and procedural fairness. It utilises the existing structure of the Expedited System and also avoids any need for scrutiny of the processes of the overseas agencies.

### **Blocking notification page**

A standardised blocking notification page should appear whenever an end-user seeks to access a URL on the RC content list, as outlined in *Option three*.

This page will contain:

- notification that the URL the user attempted to access has been classified by the CB as containing RC content;
- a brief explanation or link to an explanation of the decision making process and the criteria used by the CB to classify the content;
- notification of the procedure whereby an end-user may seek review of the decision to filter the content through the CRB or AAT; and
- a link to an explanation of the role of the independent oversight body and the procedure for making submissions to the body in regard to the overall RC filtering process.

As stated in the consultation paper, such a blocking notification page will be instrumental in ensuring that end-users understand why certain URLs are being blocked and how the process works. This will greatly aid transparency and ensure that members of the public are able to challenge a decision.

## **Review by the Classification Review Board**

Review of the decision of the CB by the CRB should be available as it is under the current Classification procedure (s42 Classification Act). Standing to apply for review would extend to any organisation or individual who is materially affected by the decision, including the content host, actual content owners and end-users who are blocked from accessing the URL. Applications would be made directly to the CRB, which would be required to make a decision within 10 business days and then provide notice to the applicant and the ACMA, including a short statement of reasons. Applications for review would only be refused if the CRB is satisfied that the application is frivolous, vexatious or not in good faith.

Slight changes to the CRB process would be required to improve its performance. This would include the removal of any delegation power in respect of a review of classification decision and also the addition of a requirement that the members of the Review Board who conduct the review actually view the content. Thus, accountability for the CB decision can be ensured without substantial change to the existing classification procedure, similar to the suggestion of *Option three* of the DBCDE consultation paper.

## **AAT merits review**

Our view is that decisions of the CRB should be subject to AAT merits review. This will ensure that a second level of review is available for organisations and individuals aggrieved by a decision to filter a certain URL. The AAT will be able to review the entire decision making process, including determinations and notice by the ACMA and the decisions of the CB and CRB. To attempt to avoid the needless review of decisions, the AAT would be afforded more discretion to refuse an application to for review of a classification decision than the CRB.

## **Transparency of decisions**

As mentioned above, all decision makers must record a statement of reasons for any administrative decision regarding the filtering of RC content. These statements must be compiled and submitted weekly to the oversight body. Additionally, the criteria and decision making processes must all be clearly stated and easily accessible, both through the websites of the ACMA and the CB and also from links on the standardised blocking notification page.

As an additional measure, each week the ACMA will publish a “breakdown” of the current RC content filtering list. This will contain the number of URLs on the list by general type of RC (i.e. child depiction, promotion of crime, sexual violence etc), similar to the list released by Senator Stephen Conroy in the Parliamentary Debates (3/2/2009 <http://www.aph.gov.au/hansard/senate/dailys/ds030209.pdf>)

and currently displayed on the ACMA website ([http://www.acma.gov.au/WEB/STANDARD/pc=PC\\_90105](http://www.acma.gov.au/WEB/STANDARD/pc=PC_90105)). For complete transparency, it would be preferable for the RC content list to be publicly available, but Google acknowledges that this is undesirable from a policy perspective, as it could aid end-users in accessing RC content URLs. A publicly available breakdown provides the next best measure of transparency.

### **Independent oversight body**

Implementing a significantly improved system requires the creation of an appropriately resourced independent oversight body which will regularly scrutinise the entire internet filtering process. The oversight body will review:

- the processes of the ACMA and the CB for making classification decisions (every 6 months);
- any submissions about RC content filtering from members of the public (each month);
- submissions from the ISPs and the IIA concerning the operation and outcomes of the Expedited System (each month); and
- the actual content of RC list to ensure it accords with procedures, with reference to the statements of reasons if necessary (each month).

The oversight body might be headed by a retired judge (preferably one with experience in classification matters) and should be sufficiently funded and staffed to deal with the task of reviewing this high volume of information. The oversight body will prepare a report of its findings and any recommendations every month (say, every 6 months in the case of process review) for presentation to the Minister and the Parliament.

The DBCDE makes a similar suggestion in *Option five* of the consultation paper. However, the suggested single independent expert would not be able to properly examine the entire filtering process in a manner that provides comprehensive accountability. Our view is that the independent oversight body will provide strong accountability and transparency for the System as a whole. The inclusion of submissions from the public in reports will allow members of the community to actively contribute to the regulation of RC content and will hopefully engender public confidence in the mandatory internet filtering system. Likewise, the ISPs and the IIA will have a means to provide regular reports on the process and voice any concerns, much as is suggested in *Option six* of the consultation paper. The fact that the oversight body will actually examine the RC content list and assess its validity is a crucial feature of the oversight considering that the list will not be available for public scrutiny.