Gartner

Report Prepared for

Internet Industry Association – Australia

Blocking Online Gambling – Technical Study

May 2001

Engagement #: 220026820

Gartner Consulting

Level 7, 40 Miller Street, North Sydney NSW 2060
+61-2-9459-4600

Confidentiality

The deliverables prepared under this agreement have been prepared for external use by the Internet Industry Association (IIA). IIA will be free to circulate the deliverables for a period of 12 months. IIA agrees that it will distribute the entire report and/or presentation external to IIA unless another use is explicitly authorised with prior written consent by Gartner. Gartner will need to review the usage context of the desired quote or excerpt in the near-to-final materials. IIA will need to clearly indicate the location of quote. Gartner may tend to grant permission to use excerpts from the deliverables in the following situations:

- The quote or research is generic as it applies to the industry.
- The quote and information is factual in nature (market size, market share).
- Excerpts taken are used in their entirety and verbatim.
- Above factors and the quote is taken from research less than 6 months old.
- If permission is granted, Gartner requires that proper attribution is included and depending on the circumstances, that the material is reprinted with permission. For example: "Source: Gartner, custom research commissioned by IIA, January 2001. Reprinted with permission."

Gartner retains all title and interest to the data and report or presentation associated with the Agreement, except for data and confidential information provided by IIA.

Gartner reserves the right to reuse the non-proprietary data and the analysis of industry-related information in its continuing analysis of the industries covered.

Gartner retains all title and interest to the benchmarking and related data and methodology used to develop the report.

Table of Contents

1 EXECUTIVE SUMMARY – BLOCKING IS NOT FEASIBLE 3

2 SCOPE AND OBJECTIVES OF STUDY...5

3 INTRODUCTION...6

3.1 REPORT STRUCTURE...6
3.2 AUDIENCE 6
3.3 WHAT IS TECHNICAL FEASIBILITY? 6
3.4 WHAT IS FILTERING?...6

4 BLOCKING ACCESS BY FILTERING IS NOT FEASIBLE...................................7

4.1 EACH TYPE OF FILTERING HAS FLAWS 8
4.1.1 IP Blocking...8
4.1.2 List-Based Filtering...9
4.1.3 Content Keyword Filtering 9
4.1.4 Rating and Classification Filtering...10
4.2 BOTH USERS AND SITE OWNERS CAN CHOOSE TO AVOID FILTERING......................12
4.2.1 User Approaches to Avoiding Filtering 12
4.2.2 Site Owner Approaches to Avoiding Filtering 15
4.3 THERE ARE FLAWS WITH CURRENT FILTERING TECHNOLOGY 17
4.4 A BEST PRACTICE FILTERING MODEL WILL NOT BE EFFECTIVE...............................20
4.4.1 The Model Consists of a Combination of Filtering Techniques 22
4.4.2 However, this Model is not Technically Feasible 24
4.4.3 Other issues with the Best Practice Filtering Model 25

5 CREDIT CARD BLOCKING IS TECHNICALLY NOT FEASIBLE.....................27

5.1 BLOCKING VIA THE IP ADDRESS OF A MERCHANT CAN BE BYPASSED.....................27
5.2 BLOCKING VIA MERCHANT AUTHORISATION CODES HAS SOME ISSUES 27
5.3 GAMBLING SITES CAN OFFER MANY OTHER TYPES OF REMITTANCE METHODS 28
5.3.1 There are Current Methods that Use a Completely Different Channel...............28
5.3.2 New Online Methods are Emerging...28

6 THE GOVERNMENT'S PROPOSED BILL HAS SOME ISSUES 29

6.1 AUSTRALIAN-BASED CUSTOMERS COULD AVOID FILTERING..................................30
6.2 OFFSHORE-BASED INTERNET GAMBLING SERVICES COULD AVOID FILTERING.......30

1 Executive Summary – Blocking is not Feasible

The Internet Industry Association (IIA) asked Gartner to write a report on the technical feasibility of preventing the use of online gambling web sites through two approaches:

- Blocking of access to these sites through filtering.
- Stopping the processing of credit card payments.

Each of these approaches has technical flaws.

1.1 Blocking of access by filtering is not feasible

1.1.1 What is filtering?

Filtering is the ability to limit what content a user has access to on the Internet. Filtering can be applied to the user's own PC through products such as NetNanny or it can be applied by the Internet Service Provider (ISP). However, filtering at the user's own PC would be self-regulation.

1.1.2 Each type of filtering has flaws

In this report we have identified four types of filtering (IP blocking, list-based filtering, content keyword filtering and rating and classification filtering). All types of filtering suffer from a common set of flaws. These flaws include:

- Difficulty in maintaining accurate lists of prohibited sites (for instance, off-shore gambling sites can change their Internet addresses frequently);
- Incorrectly classifying sites (for instance a filter could accept only classified sites); and
- Inadvertently prohibiting sites (for instance, US web sites have been blocked for containing articles about gambling).

1.1.3 Both users and site owners can choose to avoid filtering

Filtering can be avoided simply, by those who wish to do so using proxy servers and new Internet protocols such as "peer-to-peer".

Proxy Servers

Web sites, such as, MultiProxy.org advise users how to avoid filtering with a proxy server or relay service[1]. The user's ISP will not allow access directly to the prohibited content due to filtering being applied at the ISP but will allow access to a proxy. The user's ISP does not know what the proxy is allowing access to, thus bypassing the filter mechanism.

New Internet Protocols

Evidenced by Napster (www.napster.com) new Internet protocols such as "peer-to-peer" allow secret communities of users to be established. Such peer-to-peer communities could include online gambling communities, which cannot be detected by filtering.

1.2 Credit card blocking is technically not feasible

Online gambling merchants could avoid being detected by Internet payment gateways (an online method for credit card payments) in a similar way to a user wanting to avoid filtering. (Refer 1.1 above)

There are many other ways to make payments to online gambling merchants for example, via the telephone, third party clearing houses, bank transfers, off-shore accounts, and many new technologies including debit cards and e-cheques.

1.3 The Government's proposed bill[2] has some issues:

- Australian-based customers could avoid filtering; and
- Offshore-based Internet gambling services could avoid filtering.

Gartner concludes that it is currently not technically feasible to block access to online gambling sites or associated payment mechanisms.

[1] "Relay service" is a termed used in the "Report of the investigation into the feasibility and consequences of banning interactive gambling" by the National Office for the Information Economy (NOIE). 27 March 2001.

[2] "Interactive Gambling Bill 2001"

2 Scope and Objectives of Study

This study provides an independent analysis of the technical feasibility of preventing Australians from using online gambling sites both onshore and offshore.

This report covers the technical feasibility of the technology, associated costs and impacts to the network and performance.

The key questions that Gartner examined were:

Is it technically feasible to control access of Internet users to web sites?

Where is the best place to apply filtering?

What type of filtering will be the most effective?

Can these users circumvent the restriction?

What would be the impact to the overall network performance for an ISP?

How would financial institutions stop credit card payments to gambling web sites?

Gartner's discussion is confined to a technical scope and makes no comment on political, ethical, economic or social issues.

As this document is targeted specifically to online gambling, it does not cover blocking access to other types of content. Parental restrictions on children's access to information are also in a different category, and not covered here.

N.B. At the time of preparing and researching this report the Government's "Interactive Gambling Bill 2001" had not been published. Section 6, "The Government's Proposed Bill has some Issues" on page 29 has been added to acknowledge and comment on what has been proposed in the bill.

3 Introduction

The Internet Industry Association (IIA) has asked Gartner to write a report on the technical feasibility of preventing the use of online gambling web sites through two approaches. The first is the blocking of access to these sites through filtering, while the other is to stop processing credit card payments for such sites. Each of these approaches has technical flaws.

3.1 Report Structure

This report first looks at the technical feasibility of blocking access to online gambling via filtering, and then blocking of credit card transactions to impede the gambling users ability to process a payment. The report explains the types of filtering and proposes a possible model for Australia. Filtering avoidance techniques are discussed in the context of the filtering types. The report describes online credit card processing to put into context the issues with card blocking and avoidance techniques.

3.2 Audience

The report is for use by people who wish to understand technical issues related to the restriction of online gambling.

3.3 What is Technical Feasibility?

Technical feasibility in this report means "how effective the technology used to block access to online gambling sites will be against technology that avoids or otherwise defeats such blocking."

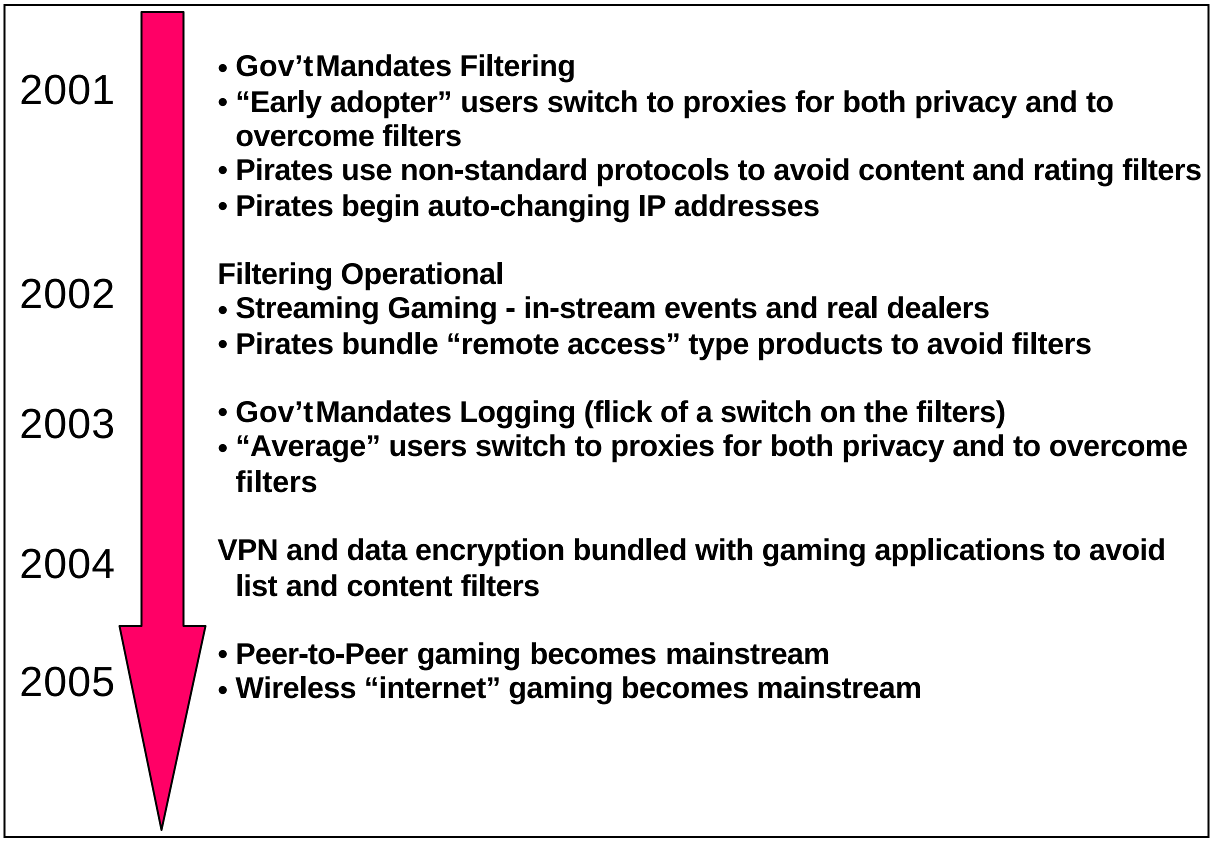
3.4 What is filtering?

The Internet contains a wide range of materials, from the useful, informative and valuable to some that are offensive or illegal in many countries. The Internet provides all types of material through the same medium, which is far different to traditional media and physical world environments. While restricted content or activities, such as gambling, can be regulated by age and other legal measures in the physical world, the Internet does not have any obvious tools for segregating material based on content and markets.

Blocks are implemented through "*filters*", which provide the Internet equivalent of physical world limitations to manage access to prohibited content. In the case of the average Internet user, filtering operates at the user's PC through the Internet browser or software applications such as NetNanny or CyberSitter. In these cases, the user decides what should be prohibited. Some ISP's provide filtering at the ISP as an additional service. The ISP then decides what content should be prohibited. Many corporations filter employee access to stop time-wasting "surfing" or to ensure that sensitive corporate content does not pass outside the company's private network.

4 Blocking Access by Filtering is Not Feasible

Filtering is currently limited by its effectiveness to deny access to online gambling sites, because of flaws with the four basic types of filtering and the ease of bypassing the filtering altogether.



2001

- **Gov’tMandates Filtering**
- **“Early adopter” users switch to proxies for both privacy and to overcome filters**
- **Pirates use non-standard protocols to avoid content and rating filters**
- **Pirates begin auto-changing IP addresses**

2002

Filtering Operational

- **Streaming Gaming - in-stream events and real dealers**
- **Pirates bundle “remote access” type products to avoid filters**

2003

- **Gov’tMandates Logging (flick of a switch on the filters)**
- **“Average” users switch to proxies for both privacy and to overcome filters**

2004

VPN and data encryption bundled with gaming applications to avoid list and content filters

2005

- **Peer-to-Peer gaming becomes mainstream**
- **Wireless “internet” gaming becomes mainstream**

Figure 1 – Ways around Filtering

Looking at a timeline of ways around filtering (Figure 1 – Ways around Filtering), some users today, should they choose to, can avoid filtering. Some users will gain access due to flaws in the filtering techniques. Looking forward in time, filtering will very quickly be obsolete due to the adoption of new technologies by the online gambling vendors and the ability of the average Internet user to bypass filtering.

Therefore, blocking access by filtering is not feasible.

There are four main types of filtering. See Figure 2 – Types of Filtering (below).

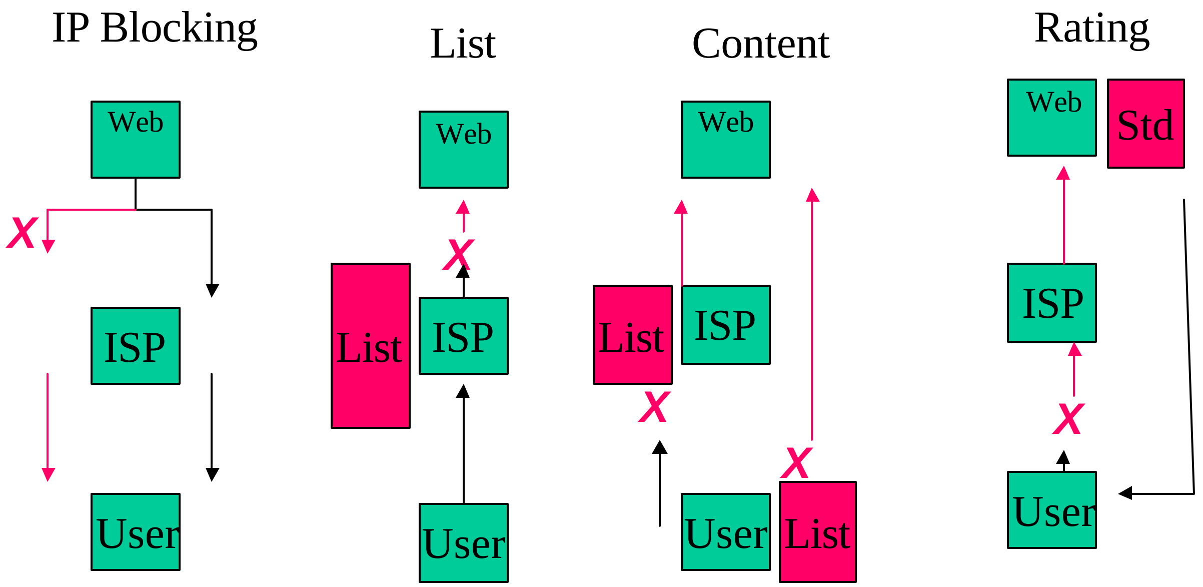


Figure 2 – Types of Filtering

4.1 Each Type of Filtering has Flaws

For the purposes of this section, unless noted, we are not differentiating between software and hardware filtering, as the processes and technologies are very similar.

4.1.1 IP Blocking

A common means to filter traffic is to block IP addresses associated with restricted content from passing through a server. This is much simpler than any of the methods presented above. However, this solution has limited usefulness. Some IP addresses have multiple web sites with the same IP address. Hosting services can provide many web sites from the same IP address. Blocking an IP address with multiple web sites will block all the web sites at that IP address.

Advantages	*Disadvantages*
Useful for blocking groups of IP addresses such as all Australian users	IP address list requires constant updating
Fast	Carrier owner can add IP addresses at will
Applied at the carrier level	Easily bypassed by user or site owner
	Cannot filter sites or web pages within the same IP address

4.1.2 List-Based Filtering

List based filtering works by comparing a request for information against a pre-determined list of Internet addresses such as Internet Protocol (IP) or Universal Resource Locators (URL). If the requested information is classified as undesirable, then the user is notified that access is denied or that the information is not available.

Some lists are categorised and have sublevels, similar to the *Rating and Classification* system detailed below, that break down categories into varying degrees. Most of the personal filtering packages support list based filtering. Nearly all server based filters are in the form of an add-on to a server based product such as content caching engines, fire walls, proxy servers, traffic monitoring tools and Internet appliances. There are very few server products designed solely for filtering.

List based filtering is usually provided through the use of "proxy servers[1]". Many corporations direct all of their web traffic through a proxy server, which use content caching techniques to optimise network performance. A proxy can also deny access to material that is unrelated to the user's work, such as gambling or adult content sites.

Advantages	***Disadvantages***
Provides greater level of filtering to IP Blocking	List based filters are created using programs which search the Internet and sometimes misclassify content
Can operate at the ISP level or user level	Carrier owner can add IP addresses at will
	Easily bypassed by user or site owner
	Lists require constant updating
	Some lists are classified by content type, such as gambling, however, this is a very broad category and may omit anything related to gambling

4.1.3 Content Keyword Filtering

Keyword based blocking uses text searches to categorise sites. A site will be blocked if it contains objectionable words or phrases.

Smarter systems try to use context proofing technologies to provide a more sensitive and workable solution. An example would be to allow the phrase "chicken breast" but block

[1] A proxy server is a type of firewall that communicates with the Internet on behalf of a private network. As a firewall it protects the private network from viruses or unwanted "attacks".

"woman's breast". Other filters try and look for additional words and if a number of the words are found, then the site is blocked.

Advantages	***Disadvantages***
Can operate at the ISP level or user level	Keyword filters are created using programs which search the Internet and sometimes misclassify content
At the user level gives the user control over content. For example, parental	Carrier owner can add IP addresses at will
Relatively cheap solution for users	Easily bypassed by user or site owner
	Cannot filter graphics and other media or programs embedded in the web pages
	Some lists are classified by content type, such as gambling, however, this is a very broad category and may omit anything related to gambling

4.1.4 Rating and Classification Filtering

A rating system uses a series of categories to classify Internet content and web sites. Depending on the source of the rating there may be a number of sublevels for each category. Using sublevels, content of a specific nature can be classified at a more granular level, for example "Romance; no sex" or "Explicit sexual activity", and varying levels in between.

A number of different groups and organisations create and maintain such ratings. Some of the more prominent are RSACi, SafeSurf, NetShepherd and WebSense. The most common standard for content rating is PICS (Platform for Internet Content Selection). RSACi, SafeSurf and NetShepherd are based on this standard.

Unlike list based filtering, rating based filtering is based on a certification given for a specific page or site that is embedded in the content itself. Rating systems are protocol based, and do not contain any information regarding which sites or type of sites to block, instead they have a pre-defined method to find the information that describes the content and means to interpret it. Such systems are voluntary.

Many different software applications, the most common being Netscape and Internet Explorer use ratings. Other software applications are readily available, such as CyberSitter or NetNanny.

Some countries, such as Singapore and China, have policies and systems in place that filter based on government ratings. For example, China recently released a suite of software products called "Internet Police 110" with solutions for ISP's, Cyber Cafes and individuals.

However, most software that uses rating systems is designed for personal use and has significant performance and scalability problems when executed in a high performance environment such as an ISP.

Advantages	***Disadvantages***
No infrastructure changes required by the ISP	Web site owner can misclassify the site
No additional software required by user	Relatively few sites are rated
User can set-up	Easily bypassed by user or site owner
Support by most leading web browsers	Classification of sites is too broad. For example, if classified as gambling it could restrict access to articles on gambling

4.2 Both Users and Site Owners Can Choose to Avoid Filtering

IP blocking is relatively the most effective technique for filtering. However, there are a number of ways that end users and site owners can bypass each type of filtering. This section describes the main current technologies and some of the coming technologies that will bypass filtering, or be impractical to filter.

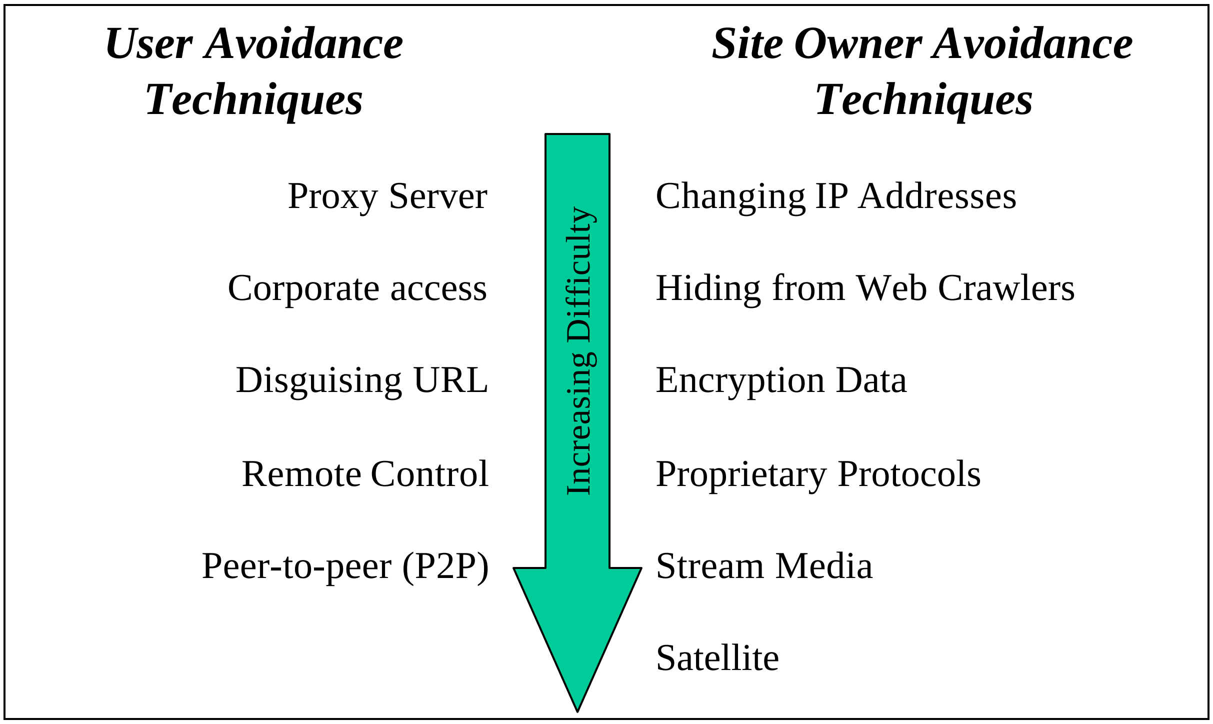


Figure 3 – Techniques to Avoid Filtering

Figure 3 – Techniques to Avoid Filtering (above), summarises the avoidance techniques and the ease of use.

A user can bypass a filter in a range of ways. The easiest of which is the use of a proxy server. Although more difficult, peer-to-peer (P2P) is rapidly becoming popular amongst communities of users with a common interest. P2P activity is not detected by filtering.

Site owners will most commonly constantly change IP addresses for avoidance.

4.2.1 User Approaches to Avoiding Filtering

Peer-to-Peer

Evidenced by Napster (www.napster.com) new Internet protocols such as P2P allow secret communities of users to be established. Such peer-to-peer communities could include online gambling communities, which cannot be detected by filtering.

In a P2P scenario, online gamblers would be invited to join a P2P community. Someone in the community (or an organisation) would act as the "house". Payment would be arranged separately.

Gartner's research predicts that more than half of global Internet users will regularly sign on to at least two P2P Internet applications by 2002.[1]

Disguising the URL

A web page's URL can take a number of forms, many of which are rather obscure. There are a number of different naming conventions used in the URL, that offer for some interesting variations in how an Internet address can be expressed. These techniques are used regularly by spammers and scammers and are used most in unsolicited email messages.

Data travelling across the Internet is converted to a binary number (series of '1's and '0's), including web site addresses. If a web site address is converted to a binary number, it will pass through most filters because they do not identify such numbers. Programs to convert names to numbers are readily available. We tested this technique on a leading filtering product, and bypassed it.

There are many other ways to disguise a URL, which will also pass through most filtering systems. Depending on the user's environment, some of these methods may not work. However, the methods can be used in conjunction to increase their effect.

Proxy Servers

Filtering can be avoided simply, by those who wish to do so. There are web sites, such as, MultiProxy.org, that advise users how to avoid filtering with a proxy. A proxy server will mask the identity of a user and will use ports[2] not monitored by filtering software.

A proxy server acts like a relay - it takes a request from one site, then relays the request to another site, or another proxy server. Proxy servers route traffic such as HTTP and other protocols, thus anonyming the original requester. Hackers commonly pass through numerous proxy servers in multiple countries, to cover their tracks. But one does not need to be a hacker, or even an advanced user to use a proxy server.

Figure 4 – Example of an Australian accessing an Australian Gambling Site, shows how an Australian user can appear from another country using a proxy server. The six steps to do this are:

1. User makes request to ISP
2. Request passes through filter
3. Request received by proxy server

[1] "P2P Applications: New Internet Bandwidth Monsters", John Girard, Gartner, 8 Dec 2000

[2] A port is an endpoint to a TCP/IP connection devoted to a particular type of Internet traffic. There is a port used for HTTP that most filters monitor.

4. Proxy redirects request using new IP address
5. Proxy traffic returns to Australia
6. Gambling site receives Proxy traffic and allows non-Australian IP address to acccess content

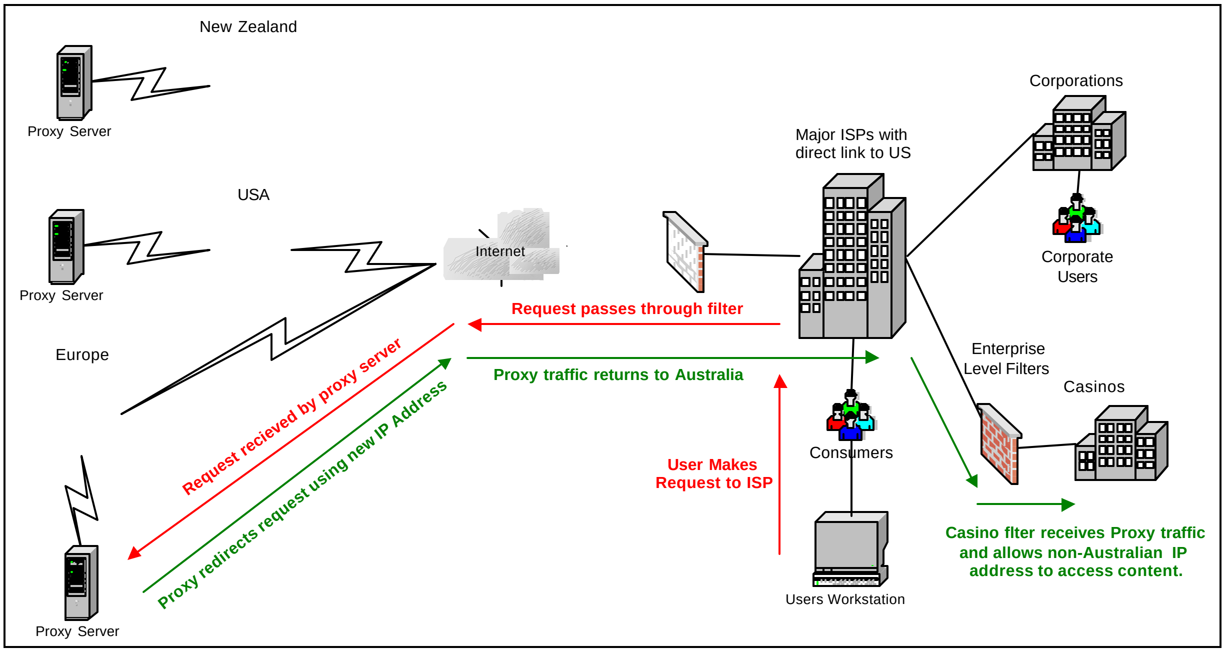

New Zealand
Proxy Server
USA
Proxy Server
Europe
Internet
Request passes through filter
Proxy traffic returns to Australia
Request recieved by proxy server
Proxy redirects request using new IP Address
Proxy Server
Corporations
Major ISPs with direct link to US
Corporate Users
Enterprise Level Filters
Casinos
Consumers
User Makes Request to ISP
Users Workstation
Casino flter receives Proxy traffic and allows non-Australian IP address to access content.

Figure 4 – Example of an Australian accessing an Australian Gambling Site

This technique can be used to change the identity of an Australian user.

Using a proxy server is easy for those who wish to do so. For instance anonymizer.com allows such access directly without the need to change browser settings. Sites such as MultiProxy.org provide lists of several thousand proxy servers that are accessible to the public.

Remote Control

Computer systems have features that allow a third person to access them and control them. This is usually for the purposes of remote administration.[1] Such features can have vulnerabilities that allow an unauthorised person to take control. An unauthorised person could then use this computer system to access other computer systems or gambling sites Their true identify would not be known.

Corporate Access to the Internet

Medium or large corporations commonly consolidate Internet access through a few points to minimise cost and improve manageability. Access to the Internet for employees in Australia

[1] e.g. Telnet, PC Anywhere and Virtual Network Computing (VNC, http://www.uk.research.att.com/vnc/).

may not originate within Australia and so would bypass any filtering applied to Internet access within Australia. In each instance the user would appear to be an international user and so allowed past all blocking mechanisms.

While it may not be in the interests of the corporation to allow access to these sites, it would be at the discretion of the corporation to block access to them, and what degree of rigour to apply to the blocking process.

4.2.2 Site Owner Approaches to Avoiding Filtering

Constantly Changing IP Addresses

Gambling sites continuously change their IP address and domain names to bypass content filters. When the URLs or IP addresses appear in a prohibited site list, they are changed, so that it is impossible to keep these lists current. Gambling site owners can put routines in place so that this can happen automatically.

It is very easy for a gambling site owner to change the IP address of a server, or a web site within a single server. Internet hosting companies often have several hundred to several thousand web sites on a single server, each with its own unique IP address. The same site may also have multiple IP addresses, and multiple domain names. An example is demonstrated in “Misclassification” (page 17), where www.mysportsbook.com and www.my-sportsbook.com both point to the same gambling web site.

Encryption of Data

Internet data is encrypted by many methods. These include technologies such as Point to Point Tunneling Protocol (PPTP) and IPSec[1], a framework of open standards that provide security for the transmission of sensitive information over the Internet and other unprotected networks. Because the data is encrypted before it is transmitted, data cab be transmitted across a public network without fear of observation, monitoring or filtering as there is no way to knowing its destination or content.

Encryption technology can be used by the online gambling sites directly, by shipping it as part of a download for a gambling application, or by users to make secure connections to external servers.

It is not feasible to block IPSec, PPTP and other encrypted data protocols as they have many legitimate uses, including virtual private networks (VPNs), extranets, and remote user access.

Streaming Media

Streaming media technologies such as those provided by Microsoft and Real Networks, have the ability to send data along with video and audio.

[1] IPSec provides the ability for the sender to encrypt packets before transmitting them across a network

Online gambling is suited to the use of streaming media. Real dealers sit at real tables, dealing to people, all of which is visible on the screen, transmitted via streaming media. Data will accompany the video and users will be able to interact with the video stream, even talking to other people who are playing in the same game.

It is not practical to filter streaming media, both from a performance perspective, as well as a technical perspective.

Proprietary Protocols and Ports

The Internet can be thought of as a highway, with each of the types of information travelling down a lane – these lanes are known as "ports", and the rules for travel are "protocols". There are ports and protocols for web pages (the common "HTTP"), and many other uses, including news groups, chat and file transfers. Filters need to monitor ports and understand protocols. However, there are a large number of applications that have developed their own protocols and use custom ports.

Increasingly online gambling is being executed either via downloadable applications, or via Java applets embedded in the web browser. Either of these methods has the ability to talk to any server on the Internet via any port or protocol that it chooses. As filtering is only applied to common ports, these can avoid filtering.

Hiding from Web Crawlers or Spiders

Web crawlers or spiders are programs used by producers of lists to scan the Internet for specific words and produce a "hit' list of sites. As discussed later in 'Misclassification' on page 17, many sites detect the fact that a crawler is interrogating the site's content and automatically respond in a different manner, returning data to cause a misclassification of the content. Thus a gambling site could trick a web crawler into classifying it as non-gambling.

Satellite Communications

Telstra offers satellite access to the Internet through its BigPond subsidiary. This is a downstream only system and still requires a local ISP for upstream traffic. That is a user can receive information via the satellite, such as streaming media, but must land based communications to send information or interact with a site. The technology does exist to make this bi-directional. There is currently no filtering solution for satellite.

4.3 There are Flaws with Current Filtering Technology

Filtering is not fully effective. This section discusses some of the more significant flaws associated with filtering. These flaws effect each of the types of filtering, as described above, in varying ways. Figure 5 – Filtering Flaws, summarise this.

	IP Blocking	List	Content	Ratings
Misclassification	N/A	High	High	Low
Outdated Lists	Moderate	High	N/A	N/A
Keywords Misapplied	N/A	N/A	High	N/A
Non Text	Nil	Low	High	N/A
Limited Sites Rated	N/A	N/A	N/A	Moderate
Filter Abuse	High	High	High	High
Categories too wide	N/A	High	High	High

High - high impact or risk of flaw occurring
Moderate - moderate impact or risk of flaw occurring
Low - low impact or risk of flaw occurring
Nil - No impact or risk of flaw occurring
N/A - not applicable

Figure 5 – Filtering Flaws

Misclassification

Producers of filtered lists and filter technology err on the side of caution by creating broad lists, which can, block access to legitimate material. The producers create these lists quickly by running programs called “Web Crawlers” or “Spiders” that scan the Internet against specified words to produce a “hit’ list of sites. Most crawlers cannot examine pages within frames, which are popular on web sites. Also, many sites detect the fact that a crawler is interrogating their content and automatically respond in a different manner, returning data to cause a misclassification of the content. To save time, vetting of the hit lists is minimal so some legitimate and prohibited sites are classified incorrectly.

As an example, Gartner took a random sample of different gambling related web sites and checked them on the WebSense (www.websense.com) database.

Location	Actual Type Of Content	WebSense Classification
www.wherecanibet.com	Gambling related articles and information	Unclassified
www.luckystudcasino.com	Online casino	Unclassified
www.casino.com	Publication on gambling	Gambling
www.mysportsbook.com	Sports betting site	Gambling
www.my-sportsbook.com	Same site as above, only difference is the hyphen in the domain name.	Unclassified
www.worldwidegamble.com	Online casino	Gambling
www.entercasino4.com	Online casino	Gambling

www.the-casino-net.com	Online casino	Gambling
www.excalibur-casino.com	Casino (not online)	Travel
www.casino.org	Online casino	Entertainment
www.gambling.com	Gambling related articles and information	Gambling
www.clustertraffic.com	Hosting site with gambling content on a sub-site	Unclassified

Table 1 – Results Gambling Sites run against WebSense database

From Table 1 – Results Gambling Sites run against WebSense database, above, at least two out of the ten sites provide online gambling. WebSense does not have any sub-classifications for gambling, so it classifies all content related to gambling, including physical casinos, online casinos, gambling related legal documents on government web sites, gambling publications and gambling related news articles are all classified under the single category of "Gambling".

Filtered Lists

Filtered lists require regular maintenance to add new sites. Online gambling sites can change their Internet address or name in order to avoid blocking. Individual sites can add or remove content at any time, and so change categories. Keeping pace with these changes presents a challenge for any organisation responsible for maintaining lists. This can be compared with virus protection applications. The vendors of such applications provide regular updates but there is always a gap between the appearance of a new virus and the appearance of protection from it.

Keyword False-Positives

With content keyword searches a false positive can be returned. That is a keyword-based filter may block access to legitimate content. Some examples of this are:

- Cyber Patrol blocks access to the HIV/AIDS information page of the Journal of the American Medical Association.

- America Online's keyword searches blocked a breast cancer support group.

- A US government physics archive was blocked because the URL began with the letters XXX.

- Recently several politicians have had their websites blocked, including US Congressman Dick Armey.

Keywords cannot be turned off.

Non-Text Information

Technology can identify locations and keywords, but cannot identify the presence of unwanted content within non-text data such as pictures, Java or Microsoft ActiveX[1] objects.

Keyword searches cannot interpret graphics and other multimedia content. It is not currently possible to "search" the contents of a picture. Therefore, a page containing gambling graphics will be blocked only if the text on that page contains one or more words from the list of words to be blocked.

Limited Number of Sites Rated

Microsoft's Internet Explorer and other similar software provide users with the option of blocking access to any site that does not have a rating. Currently only 40,000 sites are rated by RSACi and 300,000 sites are rated by NetShepherd. By blocking non-rated sites, the user’s experience of the Internet becomes very restricted.

Site rating is voluntary. The information tag headers must be included by the site owners or designers for the rating scheme to work. In general if the site objects to forms of blocking, it will be unwilling to voluntarily include rating information within its web pages.

Filter Abuse

Filters are open to abuse by the vendors that create the lists and ISPs that maintain them. Most recently, eMarketer[2] reported that “AOL's filtering software blocked out e-mail sent from the number two ISP, Earthlink. PeaceFire.org, a free speech advocate, maintains information on filtering abuse by various filter software products.

Filter Categories too Wide for Gambling

List filters, content filters and rating filters currently use a broad category for gambling. This means that much non-online gambling content could be blocked. For example the NOIE Report on this subject could be blocked since it mentions the word “gambling”. A list manufacturer would use a broad category such as ‘gambling’ to create the list, therefore any site with the word ‘gambling’ mentioned could be placed in the list. The cost of vetting every item in the list does not warrant the effort by vendors providing these lists.

[1] Java and Microsoft ActiveX are programs that can be embedded in web pages to cause moving graphics, downloads or other applications to appear.

[2] “All Blocked up and Nowhere to Go”, by Jonathan Jackson, 26 March 2001, eMarketer

4.4 A Best Practice Filtering Model will not be Effective

A best practice filtering model has been created to test the issues around filtering effectiveness. Gartner has considered the following in the design of a best practice filtering model:

- The model will block access to gambling by users within Australia, while allowing international traffic to access Australian online gambling.
- The model will provide the least overall cost.
- The model will have the least impact on smaller ISP's.
- Filtering in Australia, will not impact countries such as New Zealand and Fiji that have direct connections with Australia before passing through to the USA.
- The model will provide for fault tolerance to allow for devices to go offline transparently.
- The model will be scaleable for increased Internet traffic.

The most practical approach is to block the Australian traffic where the online gambling is hosted within Australia. This would block Australian user's from accessing online gambling in Australia, allow non-Australian traffic to travel freely within the backbone[1], and not burden smaller ISP's with the task

In order to block Australian users from accessing online gambling outside of Australia it would be appropriate to filter traffic at the primary carrier[2].

Many international corporations have their own dedicated international lines, most of which are terminated in the US. Employees of these corporations could gamble at home via their corporate networks. To a site in Australia they would appear to be coming in from the US. Therefore, these companies will also need to install filtering software to block such content.

In summary there are three points in the network at which filtering must be applied:

- At online gambling site within Australia
- At the major gateways to International pipes / lines
- At major corporations with dedicated international lines

However, even this model will not be effective due to avoidance techniques as discussed above in, 4.2 Both Users and Site Owners Can Choose to Avoid Filtering, page 12.

[1] The backbone is the main network that carries most of the traffic for the Internet in Australia.

[2] The primary carrier is the major ISP that owns part of the backbone and access to international connections.

4.4.1 The Model Consists of a Combination of Filtering Techniques

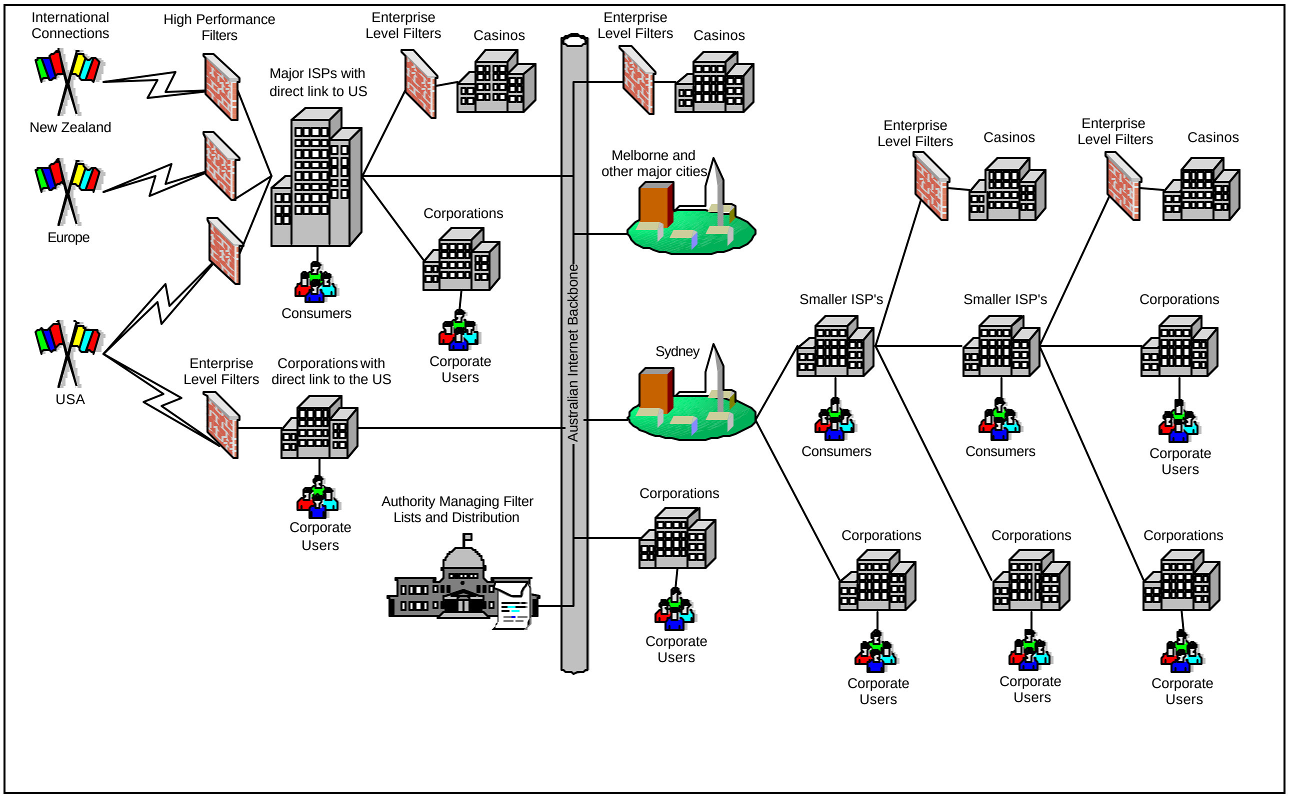


Figure 6 – Best Practice Filtering Model

IP Blocking (4.1.1 IP Blocking, page 8) has been used at the online gambling site since only Australian IP addresses need to be denied access. *Filtered lists* (4.1.2

List-Based Filtering, page 9) have been used at the major ISPs and corporations with direct links to the US as the amount of traffic travelling through these networks is likely to be significant. Only HTTP traffic should be filtered as the load created by graphics and [1]streaming media could slow the systems.

Note: Figure 6 – Best Practice Filtering Model was designed to specifically address the issue of gambling. No consideration has been made for any other form of content, and it may even be impractical or even ineffective to filter other forms of content using this architecture.

The online gambling sites use the IP Blocking technique to block access by local Australians.

The Asia Pacific Network Information Centre (APNIC) allocates IP address blocks for Australia and the rest of Asia. With its co-operation, it would be possible to build an exclusion list of IP address blocks and install them in a filter such as a firewall that would block traffic from any of the IP addresses within the block range.

This is a very fast and efficient form of filtering, as a table of address blocks is stored in the firewall and no other processing is required. The advantage of doing the blocking at the online gambling sites is that it reduces the burden on ISP's, particularly smaller ISP's for which filtering costs could be significant.

Major ISP's, providing international gateways, would use a filtered list technique to block access to international online gambling sites.

Australia has several major ISPs, which act as major gateways providing services to other ISPs and corporations. These major gateway providers have dedicated international connections as well as interconnections with each other. In order to filter the traffic leaving the country, each of these ISPs needs to install and manage a carrier class filtering solution such as that provided by Inktomi. There are very few products at this level, as the scalability and performance considerations are completely different to that of a corporate filtering solution.

Corporations with direct access to the USA, would use a filtered list technique to block access to international online gambling sites.

Unlike at the Major ISP level, there are a large number of products that are able to perform such filtering solutions. Solutions range in price from the free open-source Squid to NetCache at US$25,950[2]. Performance also varied significantly between product lines, with NetCache claiming to support up to 155Mbps

[1] Whilst streaming media cannot be filtered it may still pass through the filter server.

[2] http://www.isp-planet.com/equipment/cache_conclusion1.html

4.4.2 However, this Model is not Technically Feasible

“There are Flaws with Current Filtering Technology” (see page17) such as IP blocking and filtered lists. “Both Users and Site Owners Can Choose to Avoid Filtering” (see page 12).

4.4.3 Other issues with the Best Practice Filtering Model

Gartner have identified a number of issues with this model:

- Performance, scalability and fault tolerance
- No packaged solution
- High cost to Australian ISP industry
- Smooth migration from non-filtered to filtered environment
- Filter list management and distribution

The major ISP's, that have designed the primary gateways for performance, would require a complete redesign for filtering. This redesign would cost up to US$300 million for the industry because no packaged solution exists and a parallel network would need to be built alongside the existing one. Once built, regular maintenance of the offshore online gambling site 'hit' list would be required.

Performance, Scalability and Fault Tolerance

During a system failure, traffic must continue to flow as usual. In the case of a catastrophic failure where the filtering servers are completely unavailable, the issue arises as to what to do with the traffic. Without the filters, the traffic can still flow while the filter service is restored, however doing so may be in violation of the law. On the other hand, not doing so would deny millions of users access to the Internet.

The system should be designed to handle most types of failure. The usual approach is to build a server farm. Servers within a "farm" can be taken offline one or two at a time, allowing for the load to be carried and shared by the other servers that remain in the farm. While this will offer fault tolerance features, it also has the side effect of slowing down traffic.

The same "farm" approach can be applied to address scalability issues. Currently there are more than 12 million Australian Internet users. As traffic increases, additional servers can be added to the farm at any point in time to handle the increase in server load. This is also going to become a bigger issue as more users become connected via broadband. The amount of traffic will increase as the amount of bandwidth available for consumption increases from 28Kbps or 56Kbps using analogue modems to high speed digital modems delivering content at speeds in excess of 2Mbps capacity.

No Packaged Solution

There is currently no solution that can simply plug in and operate. Inktomi Traffic Server is widely deployed in some of the world's most demanding networks such as America Online, AT&T, and Excite@Home, but will need customisation to meet Australia's filtering requirements. America Online has approximately 300 servers running Inktomi's filtering solution. These servers contain terabytes of data in cache, and are estimated to have cost in excess of US$50 million. In addition to the filtering software itself, Australian ISPs would require additional infrastructure to be purchased to facilitate the filters.

High cost to Australian ISP Industry

Gartner interviewed several major Australia ISPs and observed that they have optimised their network architecture for performance. It was acknowledged that while installation of filtering is possible, it would require a complete re-architecture of the entire infrastructure, as filtering was not allowed for in the design.

Based on the use of Inktomi traffic servers, Gartner have estimated the cost of the best practice filtering model to be approximately US$300[1] million.

Smooth Migration From Non-Filtered to Filtered Environment

Maintaining services without disruption to consumers is the most important issue in a migration. It is not practical to disable access to the Internet for users while these systems are implemented. In order to transfer traffic to such a system, it would need to have almost total redundancy in many areas of the network architecture.

Filter List Management and Distribution

A consistent list of prohibited sites would need to be maintained and distributed to the ISPs providing the filtering. The list would be maintained using a program to search for potential sites. Because a high number of false positives will be returned a person would need to review the list. Gartner estimates that even on conservative estimates, it would take a team of 19 people working full time just to classify the content and keep the list up to date.

[1] US dollars have been quoted based on filtering software offered in the US.

5 Credit Card Blocking is Technically not Feasible

There are two technical methods to blocking a credit card payment:

1. Blocking via IP address
2. Blocking via merchant authorisation code

Both these methods have issues.

Also, gambling sites can offer many other types of remittance methods. Some methods are currently available while others are emerging.

The issues with credit card blocking, the opportunity for other types of remittance methods and new online methods emerging make credit card blocking technically not feasible.

5.1 Blocking via the IP Address of a Merchant Can be Bypassed

Although the credit card processor[1] can track and block authorisation requests from merchants by filtering.[2] The technical feasibility of this approach is not effective since merchants could bypass the filtering. See section 4.2.2 “Site Owner Approaches to Avoiding Filtering”.

5.2 Blocking via Merchant Authorisation Codes has some Issues

Credit card processors can also track authorisation codes issued to existing gambling merchants. However, on an ongoing basis there are issues:

- Who identifies the organisations that offer online gaming? The identities of these organisations may change over time, as may the activities of organisations. Organisations that don't currently provide online gaming activities may offer these in the future. Significant work is required to monitor the activities and identifies of these organisations.

- What is the definition of "Online Gaming"? Is this is defined by a regulatory body or does this depend on the individual credit card processor1?

- Who will be asked to bear the additional cost?

  – A new process may need to be put in place to manage online gaming merchant baring. This may require additional staff at the bank.

[1] A credit card processor would reside with a bank, card association or third party.

[2] Filtering would be via IP address blocking.

  - Additional staff, infrastructure, new development required. Most banks already have limited facilities and resources for new product development and are having difficulty developing current projects. The impact of Y2K and GST development is still being felt.

5.3 Gambling Sites Can Offer Many Other Types of Remittance Methods

Although currently, Credit cards are the dominant payment method used for Internet purchases and account for over 90 percent of electronic Internet retail transactions.[1] There are a number of options to remit funds.

5.3.1 There are Current Methods that Use a Completely Different Channel

Online gambling sites can offer a range of different remittance methods. These include:

- Payment by phone using a credit card
- Using a phone account to pay for services
- Paying via cheque up front into a gambling account from which a user can draw down
- Buying a product or service at an increased price, the excess monies being used to deposit into a gambling fund.

5.3.2 New Online Methods are Emerging

Future payment methods such as stored value cards, debit cards and e-cheques will provide alternative payment mechanisms for online gamblers.

- Stored value cards are increasing in popularity in the US and will eventually be accepted in Australia. It will be difficult to track what these cards are used for.
- Currently, debit cards face security, standards, infrastructure and regulatory hurdles, but once these are eliminated, both merchants and customers will begin to accept and use debit cards for online purchases.
- E-cheque is an electronic version of a paper cheque. The main difference is the medium - e-cheques are sent through e-mail and require a way to provide a digital signature. E-cheques will require customers to have smart card readers hence this may impact uptake.1

[1] "Enabling Retail Payments on the Internet" by K.Kerr, Gartner

6 The Government's Proposed Bill has some Issues

The "Interactive Gambling Bill 2001" states in section 3 that:

> "This act regulates interactive gambling services by:
>
> (a) prohibiting Australian-based interactive gambling services from being provided to customers in Australia; and
>
> (b) establishing a complaints-based system to deal with Internet gambling services where the relevant content (***prohibited Internet gambling content***) is available for access by Customers in Australia.
>
> A person may complain to the ABA about ***prohibited Internet gambling conten***t.
>
> If prohibited Internet gambling content is ***hosted in Australia*** and the ABA considers that the complaint should be referred to an Australian police force, the ABA must refer the complaint to a member of an Australian police force.
>
> If prohibited Internet gambling content is ***hosted outside Australi***a, the ABA must:
>
> (a) if the ABA considers that the content should be referred to a law enforcement agency—notify the content to a member of an Australian police force; and
>
> (b) notify the content to Internet service providers so that the providers can deal with the content in accordance with procedures specified in an industry code or industry standard (for example, procedures relating to the provision of regularly updated Internet content filtering software to subscribers).
>
> Bodies and associations that represent Internet service providers may develop an industry code.
>
> The ABA has a reserve power to make an industry standard if there is no industry code or if an industry code is deficient. "

This means that Australian based Internet gambling services must restrict access to customers based in Australia but are allowed to offer services to offshore based customers.

Offshore based Internet gambling services that offer services to Australian based customers will be dealt with on a complaints based system. ISP's based in Australia will be required to "prevent end-users from accessing the content."[1]

Some form of filtering would need to be used to enforce these requirements.

This approach has two issues:

[1] "Interactive Gambling Bill 2001", Division 3 – Action to be taken in relation to complaint about prohibited Internet gambling content hosted outside Australia.

- Australian-based customers could avoid filtering
- Offshore-based internet gambling services could avoid filtering

6.1 Australian-Based Customers Could Avoid Filtering

Australian-base customers could avoid being barred from Australian-base gambling services through the use of proxy servers and remote control[1]. The NOIE[2] report references these technologies as "relay service" and "IP spoofing" respectively. Figure 4 – Example of an Australian accessing an Australian Gambling Site, page 14 of Gartner's report gives a simple example of how an user could avoid being barred. IP spoofing or remote control is for very advanced users of the Internet.

For users with access to the Internet via their corporate accounts it could be possible to access an Australian-based gambling service if the corporate access originates outside Australia. Refer to footnote 1.

6.2 Offshore-Based Internet Gambling Services Could Avoid Filtering

"4.2.2 Site Owner Approaches to Avoiding Filtering" on page 15, describes several techniques that offshore based gambling services could use to avoid filtering.

[1] Refer to 4.2.1 User Approaches to Avoiding Filtering on page 12

[2] "Report of the investigation into the feasibility and consequences of banning interactive gambling" by the National Office for the Information Economy (NOIE). 27 March 2001

7 Appendix - References

1.	Recreational Software Advisory Council (RSAC)	http://www.rsac.org
2.	SafeSurf	http://www.safesurf.com
3.	Comparison of RSACi and SafeSurf	http://www.icehouse.net/jim_d/ratings.html
4.	List of products that incorporate WebSense categorized database.	http://www.websense.com/products/integrations/index.cfm
5.	Web Sense Master Database Categories List	http://www.websense.com/products/about/datasheets/pdfs/database.pdf
6.	Amnesty Intercepted	http://www.peacefire.org/amnesty-intercepted
7.	Study of Average Error Rates for Censorware Programs	http://www.peacefire.org/error-rates
8.	Ease of Access in the Internet	Upcoming report by Ashley Bray, Intrusion Detection Analyst and Network Security Specialist.
9.	Web Robots Database	http://info.webcrawler.com/mak/projects/robots/active.html
10.	6 Bone Information	http://6bone.net
11.	Quantex WebXL	http://www.isp-planet.com/equipment/qtx_intro.html
12.	InfoLibria DynaCache	http://www.isp-planet.com/equipment/dcache_intro.html
13.	Compaq TaskSmart	http://www.isp-planet.com/equipment/compaq_intro.html
14.	CacheFlow 545	http://www.isp-planet.com/equipment/cflow_intro.html
15.	NetCache C720s	http://www.isp-planet.com/equipment/ncache_intro.html
16.	Squid 2.3	http://www.isp-planet.com/equipment/squid_intro.html
17.	Australian Broadcasting Authority (ABA)	http://www.aba.gov.au
18.	IPSec	http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/ipsec.htm
19.	AboveNet Filter Abuse	http://www.peacefire.org/abovenet
20.	CyberNOT Site Lookup	http://www.cyberpatrol.com/cybernot
21.	WebSense Site Lookup	http://database.netpart.com/site_lookup
22.	Smart Filter Site Lookup	http://www.securecomputing.com/cgi-bin/filter_whereV3.cgi
23.	Net Nanny Site Lookup	http://www.netnanny.com/CheckURL.asp
24.	Can Congress Censor the Internet	http://www.fmew.com/archive/censor
25.	PICS, Censorship, & Intellectual	http://www.w3.org/PICS/PICS-FAQ-

Freedom FAQ	980126.html
26. The Internet Filter Assessment Project	http://www.bluehighways.com/tifap
27. The Net Censorship Dilemma	http://libertus.net/liberty
28. Internet regulation doomed: US expert	http://www.theage.com.au/news/20000816/A6072-2000Aug15.html
29. Censorship and Free Speech	http://www.efa.org.au/Issues/Censor
30. Australian IT - School accused of using 'spy' software	http://australianit.news.com.au/common/storyPage/0,3811,1040695%255E442,00.html
31. Invisible Web Gets Deeper	http://www.searchenginewatch.com/sereport/00/08-deepweb.html
32. Dion Wiggins, Independent Consultant, USA	
33. “Enabling Retail Payments on the Internet” by K.Kerr, Gartner	
34. “Gambling online becoming a tougher bet to make”, by Libby Wells, Bankrate.com	
35. “ABCs of online gambling”, by Libby Wells, Bankrate.com	
36. Inktomi, Richard Hair	
37. Telstra Corp	
38. Cable & Wireless Optus	
39. Ozemail	
40. Iprimus	
41. National Australia Bank	
42. Westpac	
43. AMEX	
44. Commonwealth Bank	
45. “Electronic Commerce”, G.P.Schneider and J.T.Perry, Course Technology	
46. “All Blocked up and Nowhere to Go”, by Jonathan Jackson, 26 March 2001, eMarketer	http://www.emarketer.com/analysis/email_marketing/20010326_email.html
47. “Peer-to-peer Economics”, Nikos Drakos, Gartner, 23 Feb 2001	
48. “P2P Applications: New Internet Bandwidth Monsters”, John Girard, Gartner, 8 Dec 2000	

8 Glossary

ABA	Australian Broadcasting Authority
ASP	Application Service Provider
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
IMAP	Internet Message Access Protocol – A newer protocol to POP
IP	Internet Protocol
IP Blocking	Known as "packet filtering" in the NOIE report
ISP	Internet Service Provider
NNTP	Network News Transport Protocol
NOIE	National Office for the Information Economy
POP	Post Office Protocol – used for retrieving e-mail from a mail server.
Proxy Server	A proxy server is a type of firewall that communicates with the Internet on behalf of a trusted network. As a firewall it protects the trusted network from viruses or unwanted "attacks". Referred to as "relay service" in the NOIE report.
Remote Control	Known as "IP spoofing" in the NOIE report.
SMTP	Simple Mail Transfer Protocol – used for requesting mail from a mail server.
Spammer	Person who slows up a network by sending junk mail to a large number of users who then forward on to others.
TCP/IP	Transmission Control Protocol / Internet Protocol
URL	Universal Resource Locators
VPN	Virtual Private Network
WAP	Wireless Application Protocol

9 Appendix - Contact Information

Joe Sweeney
Research Director, Gartner Asia Pacific
+852-3402-0329
joe.sweeney@gartner.com

Martin Stubbs-Race
Consulting, Gartner Asia Pacific
+61-2-9459-4745
+61-2-9459-4640 (fax)
martin.stubbs-race@gartner.com