August 14, 2012

Report on
Internet Filters

For the:

Reformed Congregations in North America

By the:

Media and Technology Awareness Committee

Of the RCNA-Chilliwack Consistory

(MTAC)

Contents

1. The Internet and Our Community

The internet is a global system of computer networks that are able to communicate and share data. Started in the 1960's by the US Department of Defense, it has expanded into nearly every aspect of culture and commerce. Developments and growth over the past two decades have been exponential. Radical changes in communication and information access have resulted. Many aspects of Western society have been altered irreversibly as a result of the internet; large-scale and lasting disruptions of the internet could potentially be devastating.

The World Wide Web, where people can access websites, is only one facet of the internet. Other services powered by the internet include email, VoIP (a telephone over the internet, e.g. Skype), file transfer/sharing, and online games.

1.1 Our community's relationship with the internet

Officially the position of the RCNA and the Gereformeerde Gemeenten in Nederland (GGiN) has been that internet is only permitted if necessary for studying or business use. The actual use of the internet in both denominations is far beyond that.

During the October 18, 2011 RCNA-Chilliwack members meeting, MTAC conducted an internet survey of the male members present (over 170 responses were received). Valuable information was obtained from this survey. Figure 1 below shows the distribution of which internet filter the members have. Only 14% of the members did not have internet. The other values were disappointing: only 40% of the members used Caylix[1] and 15% had no internet filter at all.

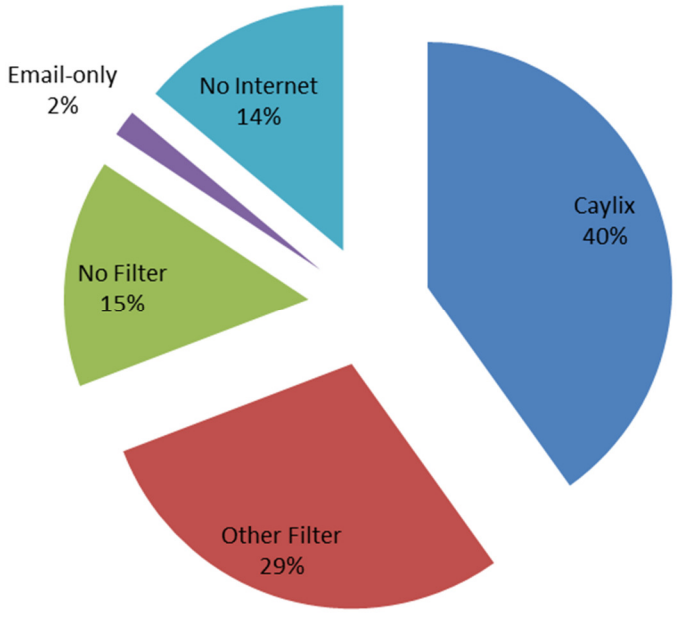

Figure 1: Distribution of internet filtering in RCNA-Chilliwack

[1] Caylix Internet Inc. was the internet filter previously required by the RCNA. Since July 31, 2012, Caylix has terminated all ISP and internet filtering services.

In this same survey the members were also asked to identify their top uses of the internet. The following figure shows this distribution.

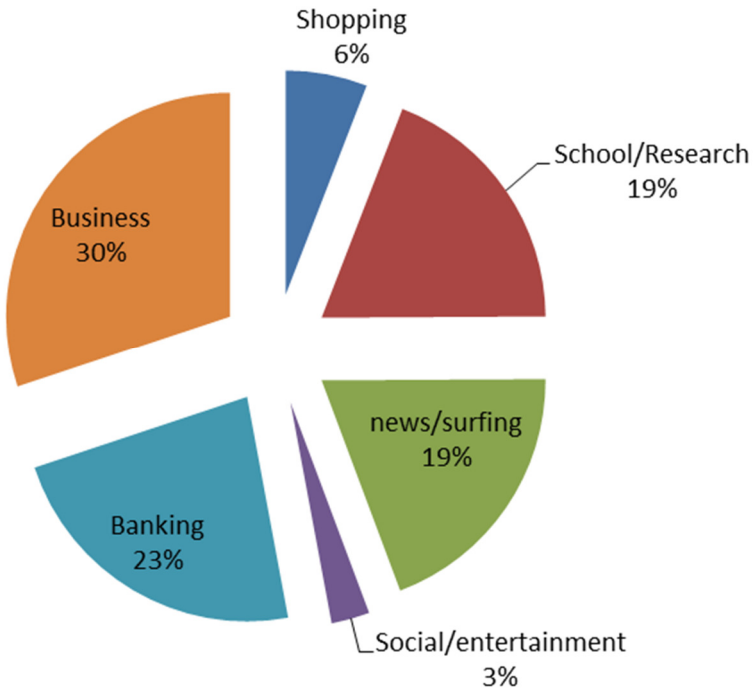

Figure 2: Internet use in RCNA-Chilliwack

It should be noted that this usage distribution is based on the top two uses selected by the male members present. It is likely that the usage distribution is significantly different for the women and baptised members.

Other survey questions identified that on average every household has 2 computers and 2 cell/smartphones. Only 5% of the members do not have any computers in their household.

From these survey results it quickly becomes apparent that computers and the internet have deeply pervaded our community.

1.2 Internet uses and dangers

The internet as a medium has many benefits and acceptable uses including:

- Contains a wealth of good information, including medical information
- Is a very powerful and fast study tool
- Current weather and road conditions, maps, addresses, driving directions
- Business, banking and bills, research
- Skype, email, maintain business connections
- How-to videos for work, training
- Remote access to other computers, file sharing between users
- Rare and other good books

Every type of media can be used for evil purposes, but the internet has enabled people to have access to soul-destroying content more than any other media ever has. Some examples of the sinful content on the internet and uses include:

- Pornography, extramarital relationships
- Occultic material, Satanism, witchcraft
- Movies, TV shows
- Inappropriate music
- Hate and violence
- Drugs and other addictions, gambling
- Warez/hacking sites (sites and tools used to steal software)
- Sports, entertainment, gaming
- Most social networking, chat rooms
- Illegal activities (modifying weapons, making bombs, credit card fraud)
- Virtual worlds (e.g. Second Life)

Other dangers that also lurk on the internet include:

- Viruses and malicious software (software that is often installed unknowingly and performs a wide variety of harmful and/or criminal activities)
- Phishing (emails that fraudulently trying to obtain personal information while pretending to be someone else. For example pretending to be a bank and having a fake website)
- Sexual predators
- Cyber bullying
- Identity theft
- Cyber warfare and espionage

Another insidious aspect of the internet is how much time is wasted on frivolous things and how easily it becomes an addiction. Thus, having an internet filter in place is of extreme importance, but as will be discussed later in this report, should not be considered to be an answer in itself. In addition, no filter will prevent all this objectionable content from entering our homes via computer or smartphone.

1.3 Internet statistics and use of the internet for pornography

A brief comment on the prevalence of pornography on the internet may serve to illustrate the threat posed to our community by access to unfiltered internet, even though pornography is but one of many evil uses of this medium. There are currently over 150 million sites (places to visit) on the internet, which together contain somewhere between 25 billion and 1 trillion pages of information. If you print off these pages and stack them up, the stack of paper would stretch from Earth to Pluto, 10 times. Some 2 (out of 7) billion people on the world currently use the internet. As of 2011, 2.5 million sites (260 million pages) were devoted to pornography. This does not include nudity or other obscene material, but pages devoted to sexual content, often of the basest and most revolting types.

These numbers are difficult to grasp. Put another way, each year 100 million in North America watch pornography, every day 68 million searches are made for pornography, and every second 28,258 people are

watching pornography on the internet. In addition, some 34% of internet users have experienced unwanted exposure to pornography through ads, pop ups, and emails. There is no censorship of the internet. Whatever can be imagined, can be found on the internet.

2. Internet filtering

Internet filtering consists of evaluating internet content to determine if it complies or contravenes with specific criteria. Internet filtering is commonly done either by the Internet Service Provider (ISP) (for example Caylix, Telus or Shaw), or by third-party software installed on the computer (or even Google SafeSearch). The filter criteria are usually broken down into different categories such as violence, hate, pornography, gambling, social media, videos, etc.

This internet filter evaluation is based on filtering of the World Wide Web (web) which is only a portion of the entire internet. The web consists of the websites users access on their computer or smartphone using a browser (such as Internet Explorer, Firefox, or Chrome). As mentioned in the previous section, there are many other services and technologies provided by the internet that are not part of the "web". (Such as email, Skype, and file sharing). Thus the "internet" and the "web" are not the same thing even though we often use the words interchangeably. Thus unless clearly identified otherwise, for the remainder of this report the "internet" is used to mean the "web".

Several different layers are typically used in the actual filtering. First, the website is blocked if it is included in the *Blacklist* or permitted if included in the *Whitelist.* If the site is not included in the white or black list, some filters employ a *URL[2] filter*. This is a huge database of many internet websites that have been categorized. If the category in which the site falls is blocked, the site is denied. If the site has not been previously categorized, most filters will block the site by default. This method does not review the actual content of the website after it has been categorized. A better method is a *dynamic content filter*. A dynamic content filter attempts to determine the suitability of the webpage each time it is accessed. A score for the website or page is determined based on the presence of predefined words or phrases. If this score exceeds a threshold, the filter will block the site. Dynamic filtering is done at the moment the user requests the website so sites that are constantly changing (like newspapers) can be effectively filtered.

The quality of any internet filter is based on two components: the dynamic filter engine, and the criteria or rules employed by that engine. The actual quality can of the filter is determined by the level of under-blocking and over-blocking. **Under-blocking** occurs when sites are permitted that should be blocked. **Over-blocking** is blocking of sites that should be allowed. It is obviously safer to over-block than to under-block, but too much over-blocking severely limits the usefulness of the internet[3].

[2] Universal Resource Locator is the address of a World Wide Web page.

[3] Considerable research of internet filters was done around 2003 with the introduction of the Children's Internet Protection Act (CIPA) in the USA. This act requires "that K-12 schools and libraries in the United States use internet filters and implement other measures to protect children from harmful online content as a condition for the receipt of certain federal funding." (Wikipedia.org) However, much of this research focused over-blocking since this could violate patrons' First Amendment rights. Although this research provides valuable insight it is of limited value for two reasons: First it places

2.1 ISP filter vs Software filter

As mentioned above, there are two basic ways in which internet filters work: either as an ISP filter or as a software filter. Internet filtering provided by an ISP is an effective option because it is easy to implement. The client simply subscribes to an internet connection with that ISP and all internet traffic through that ISP is filtered. With respect to circumvention there are advantages and also significant disadvantages. The huge disadvantage is the presence of alternative, unfiltered internet connections including free wireless internet (WiFi). (The issue of circumvention and bypassibility is further discussed in a later section of this report). Kliksafe is an example of an ISP filter. Unfortunately, Canadian ISPs including common providers such as Telus, Shaw, Rogers, and Bell do not provided a filtered option. Caylix Internet Inc was also an ISP filter. However, with the combination of a small customer base, lack of a single universal internet connection type, and resulting support costs, this has proven to be a financially unfeasible business model.

Software filters consist of software that is installed on each computer by the user. This software either filters the internet directly on the computer, or forces all a computer's internet traffic through a proxy server (a large centralized computer on the network/internet) controlled by the filter company where the filtering is done. The big advantage is that any internet connections including WiFi are filtered. The disadvantage is that the software must obviously be installed in the first place and secondly, it is possible for the administrator to potentially uninstall the software filter.

2.2 Additional Features

Other desirable features that complement the actual filtering include **accountability reports**, **time controls** and **custom white/blacklists**.

- **Accountability reports**: provide the administrator/customer with a list of all the internet activity for a given period. Some filters have the ability to provide a detailed report including web browsing activity and chat logs for different users. In addition, some filters claim to provide real-time reports or alerts when users attempt to access certain sites or input specific information (such as personal details).
- **Time control:** a powerful tool provided by some software filters that enables the software administrator to set predefined limits on when different users can access the computer or internet. For example the internet could be disabled between 9pm and 6am and on Sundays.
- **Custom white and black lists:** allow administrators to block or allow specific sites or terms for different users. For example, the administrator could block all sites except a select few for small children (custom whitelist) or decide to block additional sites for other users (for example facebook.com).

3. Filter Evaluation

This internet filter evaluation focuses on a filter's ability to effectively block clearly objectionable sites. Thus, the evaluation score is heavily weighted towards the under-blocking of the filter. Over-blocking was considered for some complex social media sites. MTAC feels that over-blocking is more acceptable than under-blocking. The following sections will outline the implementation of the filter evaluation.

---

more importance on low over-blocking. And secondly, over ten years many things change, especially with respect to software.

A number of sites were compiled for several different categories including:

- search engines
- alternative lifestyles
- dating
- gambling
- drugs
- games
- music
- occult
- pornography
- social media
- sports
- Peer-to-Peer (P2P) networks/torrents
- video
- violence/hate.

The actual categorization of the site was not deemed too important because most sites fall within several categories and the filter score is not affected by the assigned category. An average of about 110 tests (sites/search terms) were done for each filter evaluated. Special attention given to search engines and popular social media sites is described in further detail in the following sections.

There are numerous ways to assign a value to any given site. MTAC decided to determine a site's 'risk' to the viewer by multiplying the *danger* the site poses with the *likelihood* it is visited. Although these numbers are subjective, the same values were used for each filter.

MTAC feels that sites with occult/blasphemous content are very dangerous for the eternal welfare of the users. Thus these types of sites were assigned a higher *danger* value (typically a value of 2). While other types of sites such as file sharing, and alternative lifestyles are wrong, they were considered to be less dangerous and so were assigned a lower *danger* score (typically a value of 0.5 or 1). Most sites categorized as pornographic were assigned a *danger* score of 1.

For the likelihood of access, MTAC feels that the likelihood of attempting to access pornographic websites is greater than occult or alternative lifestyles. Thus pornographic sites were typically assigned a *likelihood* score of 2, while most other sites were assigned a value of 1.

If the filter correctly identified whether the site should be blocked or allowed it was given the value assigned to that site. The summation of these values provided the score for each filter. For each filter the maximum possible score was computed. The 'Success Rate' percentage of the filter is computed as the filter score divided by the maximum possible score. So a filter that correctly identified each site would receive a 'success rate' of 100%.

3.1 Search Engines

Search Engines such as Google, Bing, and Yahoo constitute a very important part of the web experience. These sites are effectively the portal to the World Wide Web. Search engines suggest websites that most closely appear to match the given search terms. Among other things, search engines can also be used to search for images and videos. It is likely that search engines would be used to find the inappropriate content. Thus it is critical how the internet filter manages these search engines.

Some of the larger and more reputable filters (Google, Bing, and Yahoo) have built in filters. With these filters set to strict, much of the inappropriate content becomes more difficult for the user to find. Ideally the internet filters lock these search engines onto strict safe-search. Many other search engines exist that do not have this

feature or do not implement it as effectively. Thus it is important that the internet filter either blocks such search engines or effectively filters the actual search terms (using dynamic content filtering).

Since the dangers are high if the popular search engines are not locked to safesearch, MTAC assigned higher *danger* and *likelihood* scores for each of these filters. Thus for example if the filter allows the Google search engine and locks it to SafeSearch-strict it receives 9 points (*danger* = 3, and *likelihood* = 3). For other search engines (excite.com, dogpile.com, baidu.com, vinden.nl), the *danger* and *likelihood* were set to 1 with points awarded if the filter blocked these search engines. It should be noted that this does penalize filters such as NetNanny that allows these engines but does perform quite well at filtering specific search terms. For the search engines permitted, several in-appropriate search terms were tested to evaluate the response.

3.2 Social Media, Social Networking

Social media is a broad category that includes sites that are built on social interaction. Over the past five years this component of the internet has exploded in popularity, also in our community. Common examples include Facebook, Twitter, and YouTube. Other examples considered in this evaluation include: MySpace, Vimeo, Pinterest, and 4chan. At this time, LinkedIn does not appear to have significant objectionable material so it was not included in this evaluation.

Of themselves, most of these social media sites are not wrong. It is the content and the way they are used that creates the problems. Without further investigation, MTAC decided that these social media sites should be allowed for the purpose of this evaluation (with exception of 4chan which appears to contain absolutely no appropriate material). This decision was partly based on the fact that Caylix allowed Facebook, Twitter, and Pinterest. The combined (*dange'* x *likelihood*) score for these sites varied between 2 and 4 depending on the popularity.

Along with the search engine component, this is the one segment of the test that penalizes the filters for overblocking. (For example if the filter blocks facebook.com it is not given the points assigned to facebook.com). To balance this, a number of inappropriate sites for each of these social media sites were included in the evaluation. Thus if the filter allows twitter.com and successfully blocks the inappropriate pages it obtains a high score. If it blocks twitter.com entirely it is penalized for blocking the site but gains points for blocking the inappropriate sites.

It should be noted that this method of evaluation does not in any way constitute an endorsement of these social media sites by MTAC.

4. Filter Test Results

For this filter evaluation, MTAC included 9 commercially available filters:

- Bsecure/Cloudcare
- CleanInternet
- CovenantEyes
- CyberSitter
- Hedgebuilders
- iGateWeb
- Integard
- KidsWatch
- NetNanny

In addition, the test was also done on the newer **Kliksafe/Smoothwall** filter (which is not currently commercially available in North America), and **NetProtector**, a product developed by Cordys B.V. (a Dutch software company), which is used by EO and Solcon in the Netherlands but does not appear to be commercially available in North America. And finally, the test was also done on the filter that was provided by **Caylix Internet Inc.** to obtain a relative benchmark whereby other filters could be compared. Thus a total of 12 filters were included in this evaluation.

Many of the commercially available filters have different levels of filtering, usually defined by age. For the filters with the highest success rates, the test was done at a more restrictive (child) level of filtering and a less restrictive (adult) level to determine the difference in performance.

Table 1 provides a list of the filters evaluated and their respective success rates. Where more than one level was evaluated, the level is included in parenthesis behind the name. It should be noted that due to the nature of this evaluation the resulting Success Rate score should not be taken as a highly precise indicator. But rather, this value should be used as a statistical indication of the probability of the filters' quality with a certain degree of uncertainty.

From these results, it quickly becomes apparent that none of the filters were perfect or even came close to an excellent score[4]. In no wise does MTAC want this evaluation to be construed as a criticism against Caylix (and the Kliksafe engine behind it), however it is disappointing that this filter only achieved about 55%.

From these results it becomes clear that iGateWeb and NetNanny are the highest performing filters. These two products are quite different from each other which results in the unexpected benefit of being able to satisfy the needs of a more diverse group of internet users. These two filters will be discussed in greater detail in a subsequent section of this report.

This report will not discuss each of the other filters in detail. However, some comments for Bsecure/Cloudcare and Hedgebuilders are warranted because these appear to be popular alternatives in our community.

Table 1: Filter scores[4].

Filter[5]	Success Rate
IGateWeb - (level - i70)	67%
Net Nanny - (Child)	62%
Kliksafe/Smoothwall	60%
Bsecure Cloudcare - (youth, 9-12)	57%
IGateWeb - (level - i10)	55%
Caylix Inc.	55%[6]
KidsWatch - (adolescent)	44%
Net Nanny - (adult)	43%
Netprotector	43%
CyberSitter - (most strict)	41%
CleanInternet	39%
Bsecure Cloudcare - (adult, 18+)	38%
Integard - (child - level 2)	38%
Hedgebuilders	33%
Covenant Eyes (teen)	28%

4.1 Bsecure Cloudcare

Bsecure Cloudcare (formerly known as Bsafe Online) is a software filter quite similar to the NetNanny internet filter. At the more restrictive levels, this filter performs reasonably well. However, at less restrictive levels the score drops significantly and is below the median Success Rate of 43%. Perhaps this is because the dynamic content filter employed by Bsecure is not as powerful as that employed by NetNanny.

4.2 Hedgebuilders

Hedgebuilders is also a software filter developed by a company with a Christian background. It does not provide any of the additional features provided by NetNanny or Bsecure. The user is not able to change any of the filter settings directly. This can only be done by contacting Hedgebuilders and asking them to make the desired changes. In terms of implementation and bypassability this method has advantages especially for users with lesser computer skills. However, Hedgebuilders performed very poorly in evaluation of the actual filter.

This poor performance is caused in part by a serious flaw in the Hedgebuilder filter: Some sites are correctly identified as inappropriate and the message pops up that the site is blocked, sometimes repeatedly, but the site continues to load and appear anyways.

[4] A low score may not necessarily indicate the filter allowed excessive inappropriate sites (underblocking) overblocking or lack of locking search engines to safesearch could contribute to a low score.

[5] The software industry is a rapidly changing world. Software available today may no longer be available tomorrow, or could be radically changed. Hence the quality and score of any of the filters listed here could change with an update. For the benefit of future reference, the NetNanny software used in this evaluation was version 6.5.13.2. Version numbers are not known for the iGateWeb filter used in this evaluation.

[6] In a previously issued letter, the Caylix Inc. score was slightly lower. However, further refinement of the data analysis increased the success rate to 55%.

5. Filter Recommendations

Based on these test results, MTAC recommends the following two filters: **iGateWeb**[7] and **NetNanny**[8]. The following sections will outline some of the difference together with the advantages and disadvantages of these two filters and some scenarios when one filter may be more suitable than the other. It is important to note that MTAC has only evaluated the iGateWeb filter using a direct connection to iGateWeb's proxy server where the filtering is done. MTAC was not able to evaluate the performance and implementation of the actual eGate router provided by iGateWeb. Thus the characteristics ascribed to iGateWeb have been determined from their website and from email correspondence with Mr. Arjan Jansen, a founding partner of iGateWeb.

5.1 Similarities

iGateWeb and NetNanny have several similarities: Aside from the obvious that they are both internet filters, both filter web content by routing all the web traffic through their proxy server where the actual filtering is done. Both filters use Dynamic Content Filtering which means the content is evaluated everytime it is accessed since it could have changed (for example online news sites).

Accountability reporting or log showing all the internet activity, is provided by both filters, although the frequency and granularity or level of detail differs.

One important similarity is that both filters can be disabled or overridden by the administrator.

5.2 Differences

The differences between the two recommended filters are more significant.

5.2.1 Corporate

iGateWeb is owned by people from the NRC in Alberta and Ontario thus it was developed from a Christian perspective similar to our own. On the other hand, NetNanny was originally developed in 1995 and purchased by ContentWatch Inc in 2007. ContentWatch Inc. appears to be a secular company without any indication of Christian origins. This difference could perhaps become more apparent in how some of the 'gray' websites (not clearly appropriate or inappropriate) are filtered. However for any of the clearly inappropriate content (pornography, gambling, violence, etc) there is significant difference.

The two corporations also differ in size and quantity of services provided. iGateWeb appears to be a relatively small company that only provides internet filtering for computers with the eGate router. ContentWatch Inc. is considerably larger and provides a variety of internet protection products for personal and business use. ContentWatch Inc. also provides a mobile filter for Android phones and is currently working on developing a mobile filter for iOS, which is the operating system used by iPhones and iPads.

5.2.2 Filter structure and implementation

NetNanny is a software based filter. This means the user needs to install the filter on each computer which can be done by downloading the software from the NetNanny website. The software can then be configured with different filtering levels and permissions for different user profiles. Each user account on the computer can be assigned a different NetNanny profile. For example, a 'child' NetNanny profile can be created. This 'child' filter

[7] iGateWeb website is www.igateweb.com
[8] NetNanny website is www.netnanny.com

profile can then easily be assigned to one or more user login accounts on that computer. NetNanny can be modified by the administrator (person who has control of the program). Thus the administrator can un-install, disable NetNanny, or override any block at any time. It should be noted that these options (uninstalling, disabling, or overriding) are not available to any of the other users. So children that do not have the admin password cannot turnoff NetNanny or override blocked sites.

iGateWeb is a hardware based internet filter. The eGate router, a physical box, is placed in the home network between the computer and the modem (the internet source). The router is connected to the modem with a network cable and to the computers with similar cables or via a wireless connection. No software needs to be installed on the computers. So all computers in the house that are connected to the internet via the eGate router will have filtered internet. This eGate can be physically unplugged or removed from the network and the computers can connect directly to the modem or to another cheap router (available at prices starting from $20) thereby having access to unfiltered internet. iGateWeb has told MTAC the report will show when the router was unplugged from the network. However, damage could have been done by that time obviously.

This difference gives rise to significant advantages and disadvantages. Since iGateweb is a physical device in the home, any computers or even smartphones connecting to the internet by WiFi will be filtered. This includes any hidden boot partitions or virtual computers (computers hidden within a computer). Also any new laptops or visitors' devices are also filtered. The disadvantage of this arrangement is that if any WiFi is available (for example from neighbours) then any computer can connect to the internet through the neighbours' wireless connection and have access to unfiltered internet. In addition, if a laptop is taken out of the home and connected to the internet by one of the many free WiFi connections (available at Starbucks, MacDonalds, Safeway, etc) it will have access to unfiltered internet.

On the other hand, NetNanny will protect computers on which it has been installed from other available and free WiFi sources such as neighbours, Starbucks etc. However since NetNanny must be installed on each computer any smartphones, new computers, and visitors' laptops will have access to unfiltered internet.

For families living in rural areas that do not have access to neighbours WiFi or do not use a Laptop outside the home, iGateWeb may be a good option because it effectively filters all devices in the home. For people living in more densely populated areas where free WiFi is more readily available, NetNanny may be a better choice because it effectively filters regardless of which connection is used to access the internet.

5.2.3 Features and Options

Other significant differences between the two filters are the quantity of features and other tools available.

iGateWeb is very simple: the user selects a filtering level between i-10 and i-90. Once selected, this filtering level can only be modified by iGateWeb. iGateWeb users do not have the ability to customize filtering, have different filtering profiles for different users, or override blocked sites.

NetNanny, while simple to use and setup, has numerous other features and options. This allows the administrator to create custom profiles for different users. Other tools include remote administrator of user profiles on the computer, time restrictions on accessing the internet. Other NetNanny features include the ability to create custom black and white lists allowing the administrator to further refine what is available for

different profiles. Thus for little children everything can be blocked except what is on the custom whitelist, or for other profiles the administrator can choose to block sites like Facebook etc. NetNanny also allows the admin to create custom keyword lists that are blocked. For example, adding keywords like 'satanic' and 'satanic bible' are effective at dynamically blocking sites that contain those keywords. NetNanny also has more advanced reporting tools including chat logs and the ability to send email alerts for various triggers (such as when a child attempts to access a specific site or attempts to enter personal information). This is valuable in combating dangers like identity theft and sexual predators.

For parents who are not very proficient with computers, iGateWeb may be a good option because of its simplicity and lack of options. On the other hand, parents with some basic computer skills and who want different filtering profiles or access to the other good features, NetNanny may be the better option. It should be noted that although NetNanny has many different options and features, the default filtering profile does not need any configuring and is quite effective. The installation is done by following a series of simple prompts (clicking 'next' or 'yes' and providing some information such as names and passwords) and can be completed within 10 minutes.

5.2.4 Accountability Reporting

NetNanny and iGateWeb also differ in the way they provide accountability reports. Currently iGateWeb emails a report once per month. Since iGateWeb does not have different user profiles, all the data would likely be included in a single summary. NetNanny provides a log on the computer meaning the administrator can view the logs for each of different user profiles at any time. In addition, NetNanny also allows the profile to be setup to allow online viewing of the reports[9]. This means the administrator of the NetNanny account can log into their account at the NetNanny site from any computer in the world and view the logs for the different user profiles. These online tools also allow the administrator to modify profiles and change settings.

For parents who do not desire different filtering profiles for different users, iGateWeb may be the better option. For parents that travel or want to monitor internet use from children who use laptops that can connect to other WiFi networks, or would like separate logs for each of the users/children NetNanny may be the better option.

Considering these differences it quickly becomes apparent that NetNanny and iGateWeb complement each other – The strengths of the one fill in the weaknesses of the other. Since each member and family have different circumstances it is impossible to recommend only a single filter that everyone should use.

[9] To view reports online, the administrator needs to select this option in the settings.

6. Conclusion and Sobering Reflections

After having identified iGateWeb and NetNanny as the two recommended filters for our community it is important to address a few related issues and add a few concluding remarks.

6.1 Filter Circumvention

Filter circumvention is any situation where the user could have access to unfiltered internet even though attempts have been made to implement a secure filter.

Ideally there would be complete control over all internet connection sources and all internet traffic could be safely filtered. Unfortunately this is not the reality of today, even with either of the two recommended filters. As identified in the previous section, even these filters can be either unplugged or modified/overridden.

In a simplistic form this problem is constrained in scope to a computer savvy user (child or parent) who can manipulate the home computer and network to access the unfiltered internet by either unplugging the eGate router or disabling or circumventing NetNanny with a virtual computer. An ISP filter model such as Kliksafe, or previously Caylix, solves this problem. However, in reality the problem is much larger than this single example. To demonstrate the extent of this issue two aspects need to be explained: devices to access the internet, and methods to connect to the internet.

Devices to access the internet include:

- Desktop computers
- Laptops/Netbooks
- Tablets
- Smartphones (iPhones, BlackBerry, Android phones)

The cost to acquire one of these devices start at close to free for a smartphone on a multiyear voice/data plan or less than $200 for a used laptop or netbook which is a more basic laptop computer.

Methods to connect to the internet include:

- Paid subscription with an ISP for a home connection (cable, satellite, ADSL, or dialup)
- Paid subscription for a data package for a smartphone or tablet (this is known as a 3G connection)
- Free wireless internet (WiFi)
    - from an individual with an unsecured wireless router
    - made available in many public places (Starbucks, MacDonalds, Safeway, BC Ferries, Colleges/Universities, libraries, airports)
- Municipal WiFi or Google WiFi is the concept of turning an entire city into wireless access zone[10].
- Many smartphones (iphones) and tablets can be turned into wireless access points. I.e. A computer can connect to the smartphone either with a cable or wirelessly and connect to the internet using that smartphone's 3G data connection.

[10] Municipal WiFi may or may not be entirely free. For example, Google WiFi is a free city wide wireless network in Mountain View, California. Wikipedia lists 18 cities in Canada that currently have some form of Municipal WiFi. (http://en.wikipedia.org/wiki/Municipal_wireless_network)

With a little imagination and with minimal computer skills, most of the devices can be connected to any of the internet connections.

One example: For less than $200 someone could purchase a second laptop (assuming that NetNanny was installed on their other computer) and connect to any of the numerous free WiFi locations thereby obtaining access to unfiltered internet.

Many people have a smartphone or tablet which has direct access to unfiltered internet using the 3G wireless technology. On some of these smartphones, especially the popular iPhone it is very difficult to install a filter because Apple, the company that develops and sells the iPhones, tightly controls the software that operates on the iPhone.

This is an enormous problem and MTAC has struggled with this single issue for countless hours. After much discussion, MTAC has been forced to conclude that there is currently no single filter solution to the problem of circumvention.

6.2 Concluding remarks

From the information provided in this report and from personal experience it is apparent that the internet is impossible to ignore. The degree to which the internet in its various forms has pervaded our communities, and from the numerous benefits and completely acceptable uses, it is clear that the internet as a technology can no longer be kept outside of our community as was done previously with television. Although sacrifices could be made in terms of the benefits and convenience of tools and services powered by the internet, MTAC cannot envision how this would be possible without extremely radical changes in lifestyle, business and education.

MTAC recommends the use of iGateWeb or NetNanny since these achieved the highest 'success rates'. However it also important to recognize that the top score was only 67%. This low top score coupled with the circumvention problem and other dangers described previously clearly shows that having an internet filter is not the final solution. It is critical to recognize that either of these filters is only a single weapon in the arsenal that must be used to fight the ever increasing dangers of the internet. Another weapon would be to maintain constant vigilance in monitoring the internet activity of others in the home.

A different weapon is **awareness**. We must be aware of the current internet situation and of the defenses available today. Aware of incredibly rapid changes and developments in the technological and digital world of today and the potential dangers these might bring. We must be aware so strategies can be developed and positions established to combat these dangers before they can gain a foothold in our community.

Finally, no human power or wisdom will prevail against the evils of the human heart and the devil's efforts to destroy what is left of God's church in these dark and perishing times. It is our duty to be vigilant, to watch (Mark 13), also regarding forms of media and technological developments that endanger our way of life, but above all to pray for God's saving and preserving grace for our communities and for ourselves. Without which all efforts are vain.