Protecting Our Children In a Cyber Society

The internet is growing at an ever increasing rate. Whilst an invaluable source of information, much of the content is inappropriate for children.

Current filters and blacklists are ineffective, require downloading on individual devices and can be bypassed.

Most of the solutions available today rely on combinations of blacklists and filters to restrict content. These methods are only accurate to a certain point. Filtering can often return false positives when blocking content that may be of actual significance to the user. More seriously, children can inadvertently stumble across inappropriate sites due to the many flaws in filtering. A report released by the Australian Government shows that filtering only blocks about 80% of unwanted content. The report went on to say that between 2.4% and 3.4% of content was over blocked by filtering.[1]

Several solutions in the market also employ a whitelist as part of their defence. These are usually limited with the lists only containing a few thousand sites.

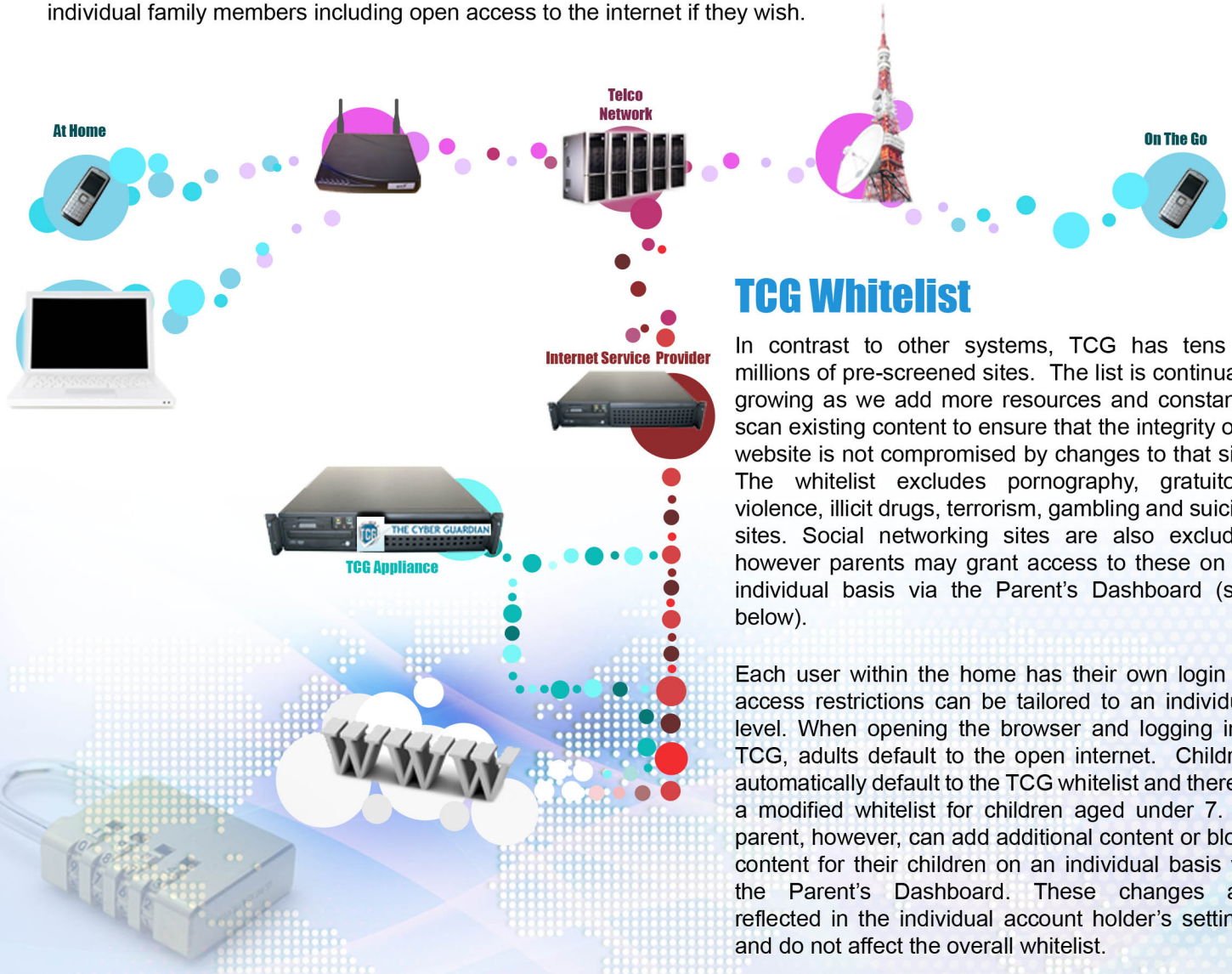
Products currently used by families are client based software solutions loaded onto the home PC. This in itself can be daunting, confusing and frustrating for parents.

In addition, children can be technically more adept than their parents and current solutions can be bypassed by various means that are widely promoted on the internet. A further limitation of the current solutions is that they only protect the machine they are loaded onto.

[1] Page 13, Internet Service Provider (ISP), Content Filtering Pilot Report, Enex Testlab, 15/12/09

The Cyber Guardian (TCG) has developed a new & unique solution incorporating a number of functions which, together, provide a user friendly, protected environment across all devices & operating systems.

Deployed at ISP level, no client-side download is required for any device. A whitelist of 10's of millions of pre-screened sites are automatically available via the TCG custom built search engine and parents have control over content for individual family members including open access to the internet if they wish.



TCG Whitelist

In contrast to other systems, TCG has tens of millions of pre-screened sites. The list is continually growing as we add more resources and constantly scan existing content to ensure that the integrity of a website is not compromised by changes to that site. The whitelist excludes pornography, gratuitous violence, illicit drugs, terrorism, gambling and suicide sites. Social networking sites are also excluded however parents may grant access to these on an individual basis via the Parent's Dashboard (see below).

Each user within the home has their own login so access restrictions can be tailored to an individual level. When opening the browser and logging into TCG, adults default to the open internet. Children automatically default to the TCG whitelist and there is a modified whitelist for children aged under 7. A parent, however, can add additional content or block content for their children on an individual basis via the Parent's Dashboard. These changes are reflected in the individual account holder's settings and do not affect the overall whitelist.

System Deployed at ISP Level

Our device sits at the Internet Service Provider (ISP) level and cannot be bypassed by even the smartest of kids. After subscribing to our service via the ISP, account holders using any device, including any 3G enabled mobile device, will have access and content validated by TCG's system, wherever they are. All requests from subscribers, after identification by the ISP, are routed through our appliances and validated based on a combination of our extensive whitelist and user defined parameters.

The Cyber Guardian's system outperforms other systems due to the minimal touch approach to resource validation. No 'on-the-fly' scanning of resources is necessary, a check is simply performed to confirm the user privileges and is served immediately back to the end user. Our solution can easily be deployed in a high availability configuration (N+1) and can be scaled out indefinitely to meet even the busiest ISP networks without impacting the user experience. All user and session data is synchronised continuously across each of the devices deployed within the network and regular updates of our whitelist are automatically updated on each appliance as they are made available. These appliances are 'set and forget'. TCG takes care of the rest.

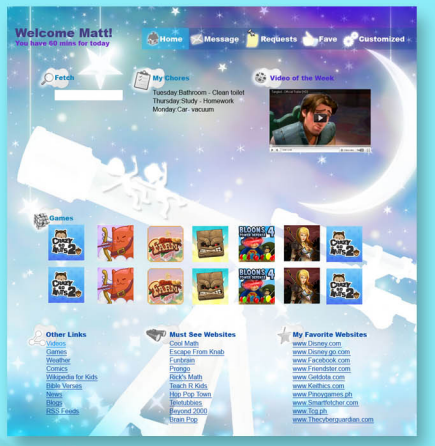
TCG Search Engine

We have utilised leading search technology to develop our own search engine that allows a ‘safe’ search within the extensive TCG database of approved sites.

User Experience

TCG has developed home page themes for our key user groups. These groups are Under 7’s, 7 to 12 year olds and 13 years plus. The home page is highly configurable and designed to be user friendly, fun and educational.

Under 7’s home page



7-12 years home page

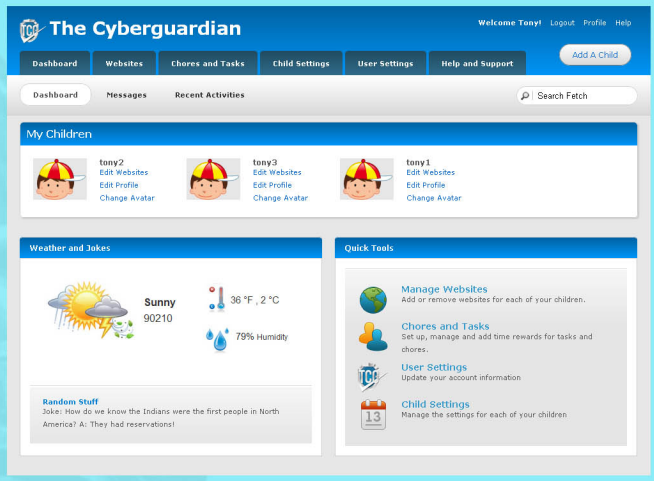
13 years + home page

Parent’s Dashboard

Parents are presented with a console that allows configuration of a number of settings for their individual children.

They can add or remove specific sites and can also control access around specific days/times or length of access. Social networking sites, for example, can be added as an option with a parent only allowing access at particular times rather than after lights out or during homework period.

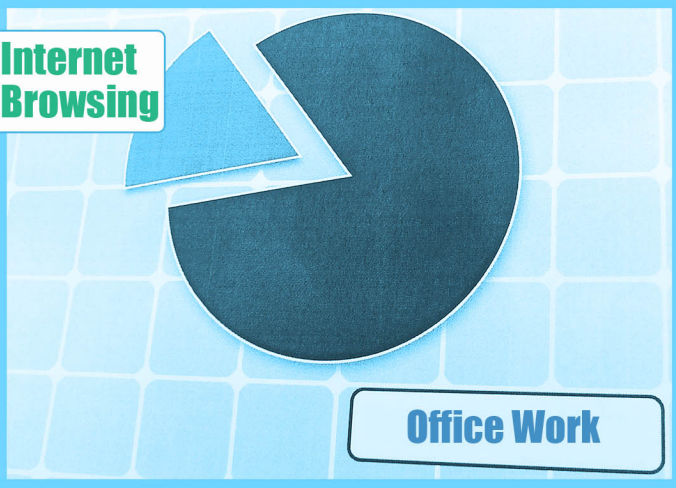
A parent may even reward a child with additional time or remove time if so desired. The Parent’s Dashboard is accessed via a login and can be accessed remotely.



The Negative Effect of Internet Use in the Workplace

Research conducted around the world continues to highlight the problems relating to the misuse of the internet during work hours.

The risk is not confined to the loss of productivity and the cost's associated to the employer but also the risk of downloading harmful or inappropriate content, how that information is shared in the workplace or externally and the impact on other employees. Organizations have a duty of care and a social responsibility in regards to this issue.



Loss of Productivity

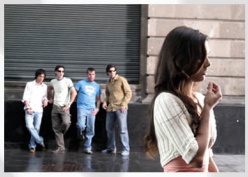
According to many reports, employees spend up to 2 hours per day accessing websites that are not associated with their employment. In some work environments' it can be as high as 50%. Social networking sites such as Facebook, blogging sites and news and sport are just some of the sites frequently visited by employees during work hours.

Whilst it is accepted that the use of the Internet is a necessary part of the working day for the many employees, visiting non work related content should be restricted to the employees own time such as lunch break. This will increase productivity, provide a safer work environment and educate the employees on acceptable use of the internet.

Consider an hourly rate paid to an employee and the amount of productivity that is lost due to inappropriate use of the internet during work hours. The resulting loss of revenue is significant. Based on 2 hours per day at an hourly rate of $15 per hour and allowing for annual leave etc, the cost for one employee would be around $7200 per annum. In a workplace of 2000 staff, the potential loss of revenue or extra cost would be $14.5 million per year. A workforce of 200,000 is losing $ 144 million per year.

(Values used are in US dollars and for demonstration purposes only).

Risk to the Organisation



Sexual harassment – An employee viewing pornography at work puts the company at risk if another employee sees something offensive. The employer has a duty of care to ensure that the workplace is safe environment in all respects for all employees.

Employee morale – The distribution of inappropriate or negative information obtained from the internet can have a detrimental effect on staff morale. Not all employees's exposed to inappropriate content in the workplace take action but simply and quietly build a resentment for their colleagues and employee which can ultimately prove costly to the company.

Illegal activity – All countries have different standards and laws and the downloading of certain material in some countries may be breaking the law. Organisations can be held responsible if an employee accesses, distributes illegal information or uses that information to commit a crime.

Downloading of malicious files - The indiscriminate downloading of files from the internet can introduce a whole host of potential security issues for the company. Viruses, phishing and malicious files can be inadvertently downloaded by employees intentionally or accidentally.

TCG Corporate/Government Solution

TCG, along with providing protection in a domestic situation, is also an ideal solution for the workplace. The principles that apply to the home user version are applied to suit the corporate or government environment. The standard whitelist can be utilised along with the addition or deletion of sites the company deems suitable or unsuitable, all managed by the company administrator. Particular sites can be available to targeted employees, for example: . Senior management may require access to the open internet, the marketing department may require access to social networking sites and blogs, or the accounting department may require access to banking sites. TCG offers a range of customised solutions, easily managed by the company administrator including:

- Adding or deleting sites from the whitelist for overall company use or targeted to certain employees or departments.
- Blocking access to the whitelist for all employees not requiring internet access during their work day.
- Allowing employers that do not need internet access, to access the whitelist for a set amount of time per day to check the news, perform personal banking etc. This could either be, for example, 45 minutes that can be used throughout the whole day or restricted to a certain time period, say between 12 noon and 1pm during the lunch break.

Schools

Existing filter systems currently used in schools can be bypassed by savvy students via proxy servers. The TCG system provides a robust and safer environment for public and private schools which can be managed by the school administrator. The whitelist can be easily modified to provide access to all curriculum based research and study sites while restricting access to non-school related internet surfing and proxy servers.

Other uses of the TCG System

With adaptation, the TCG systems can also be used to exclude websites that are deemed to be inappropriate or illegal in any particular country or jurisdiction. By restricting access to approved URL's, TCG's system is able to build a healthy internet environment without slowing down the user experience in the process.

Patent Applied For (Application # 2011901108)