Internet Safety Technical Task Force
Technology Submission

InternetSafety.com, Inc.
http://www.internetsafety.com

ABSTRACT
The Internet is useful tool that can both enrich our lives and make them simpler in many ways. However, along with the usefulness of the Internet also comes the responsibility for parents to protect children from inappropriate content that is also available. For this reason InternetSafety.com has created Safe Eyes – a parental control suite for both Windows and Macintosh computer system. With Safe Eyes, parents have the toolset they need to help protect their family while on the Internet.

Functional Goals
☒ Limit harmful contact between adults and minors
☒ Limit harmful contact between minors
☒ Limit/prevent minors from accessing inappropriate content on the Internet
☒ Limit/prevent minors from creating inappropriate content on the Internet
☐ Limit the availability of illegal content on the Internet
☒ Prevent minors from accessing particular sites without parental consent
☒ Prevent harassment, unwanted solicitation, and bullying of minors on the Internet
☒ Other
- Limit/Prevent minors from using Instant Messenger applications.
- Limit a minor's time spent on the Internet and the time-of-day when Internet can be used.
- Limit/Prevent minors from send or receiving email except from pre-approved contacts.
- Track posting of personal data to Internet websites such as social networks, blogs, or message boards.
- Limit/Prevent minors from using Internet-enabled programs such as file sharing and media players.
- Provide usage reports that allow parents to know what websites were visited, the Internet-enabled programs used, personal data that was posted online, and Instant Messenger conversations held.
- Provide parents with an instant alert in the event that a minor violates their Internet safety policy.

PROBLEM INTRODUCTION
The goal of Safe Eyes is to provide a toolset for protecting minors from activity or content on the Internet that is not suitable given their age. This suite of tools helps protect minors from multiple Internet threats with a single product. These tools include:

1. Web Filter: To address the problems of minors accessing inappropriate content and preventing access to particular sites without parental consent, Safe Eyes offers the ability to block websites based on 35 selectable categories. Mechanisms also exist to block search results on certain search terms and to build a customized block/allow list.

2. Instant Messaging: To address the problems of: harmful contact between adults and minors; harmful contact between minors; and to prevent harassment, unwanted solicitation, and bullying of minors Safe Eyes has the ability to block Instant Messengers or record the Instant Messenger conversations held.

3. Time Limits: To address the problem of excessive Internet usage by a minor, Safe Eyes allows for time limits to be placed on Internet usage as well as limiting the times of day the Internet can be used.

4. Email: To address the problems of: harmful contact between adults and minors; harmful contact between minors; and to prevent harassment, unwanted solicitation, and bullying of minors, Safe Eyes can allow email to only be sent to and received from pre-approved email addresses.

5. Social Networking: To address the problems of: harmful contact between adults and minors; harmful contact between minors; to prevent harassment, unwanted solicitation, and bullying of minors; and limiting a minors ability to create inappropriate content online, Safe Eyes can track and report when personal data, sexually suggestive content, or profane content is posted on the Internet.

6. Program Blocking: To address the problem of minors accessing the Internet through Internet-enabled software programs, Safe Eyes can block access to any software program that attempts to connect to the Internet.

7. Usage Reporting: To address the problems of parents being able to communicate what is and is not acceptable online behavior, and the preventing of minors from creating inappropriate content on the Internet Safe Eyes can produce detailed Internet usage reports for later review.

8. Instant Alerts: To address the problems of minors accessing inappropriate content and preventing access to particular sites without parental consent, Safe Eyes can immediately alert a parent by email, text message, or a phone call when inappropriate activity is attempted.

PROPOSED SOLUTION

Safe Eyes is a client/server application that is installed on the end-user's computer and can be configured to protect against multiple Internet threats. The software can be either downloaded directly from our website or can be ordered on CD-ROM and shipped to the customer's home. Once installed the main functions of the software are:

1. Web Filter: Safe Eyes uses a category database that classifies websites into one or more of 35 categories. The category database resides on the server rather than the client to ensure that each customer benefits from the latest database update automatically. The category database is updated daily. The Safe Eyes application is connected real-time to this server infrastructure when it is active and logged in. When the user requests a website a small request is sent to the Safe Eyes server which returns the categories for the site. If the current Safe Eyes user is allowed to visit a website with these categories the site is loaded. If the user is not allowed to access the site a "website blocked" page will be returned instead. Safe Eyes also has the ability to block searches on specific key words and phrases. These keywords can either be entered by the user or a pre-defined list of sexually suggestive terms and profanity can be selected. Safe Eyes allows for the administrative user to override websites by blocking or allowing specific sites that the user specifies. Additionally, Safe Eyes can be configured to block access to all websites and only allow the user to visit pre-approved websites for which the administrator has given their consent to access.

2. Instant Messaging: With Safe Eyes a user can be blocked from using AIM, ICQ, MSN or Yahoo messengers. If blocking is not the desired outcome, Safe Eyes can be configured to simply record both sides of an instant messenger conversation and make that available for review at a later time. To accomplish both of these functions Safe Eyes looks at the Internet traffic and searches for protocol-specific patterns that match AIM, ICQ, MSN, or Yahoo. This means that blocking or recording of instant messenger traffic will work regardless of the client the end-user has installed.

3. Time Limits: Time limits allow the Safe Eyes administrative user to specify when and for how long the Internet can be used by a specific user. There can be limit on the times of day that the user is allowed to access the Internet. In addition there can be a simple limit on the total amount of time the Internet can be used in a day. These two options work hand-in-hand with each other and can allow a user a specific amount of time that can only be used during a certain time of the day. Time of day access can be set the same for each day of the week or each day can have an individual setting. When Safe Eyes is logged in for a user that has Time Limits the time and heartbeat functions to update the time come from the server so that the user cannot tamper with the system clock to extend their Internet usage times. Additionally, if a user moves to another computer in the house and logs in with their username the Time Limits will follow them as well as any accrued time already used for the day.

4. Email: Safe Eyes can be configured to only allow a specified user to send and receive email with a pre-approved list of contacts. Using a POP3 and SMTP proxy Safe Eyes intercepts all email being received or sent by a specified email address and determines if the email address is on the list of approved contacts. If it is not, the email is deleted and never delivered anywhere. If it is, the email is either delivered or sent on to the recipient. The email feature of Safe Eyes works with all of the major email clients but does not work with web-based email accounts. However, Safe Eyes gives the administrative user the option to block access to web-based email sites so that all email access for a specific user can be controlled.

5. Social Networking: Safe Eyes allows the administrative user to specify items of personal information that they do not wish the users on their account to post online. Examples of the types of data would be street, address, home phone, cell phone, or school name. The user can also specify any other type of information they want to monitor for. Once this information has been entered, Safe Eyes monitors all data posted to the Internet and records the date, time, website, Safe Eyes user, and the information that was posted if any item of personal data is posted. Safe Eyes does not prohibit the posting of data, it only adds an entry to the user's usage report for viewing by the administrator. Additionally, the administrative user can also monitor for any sexually suggestive terms or profanity that is posted by a Safe Eyes user. These are the same pre-defined dictionaries that are used in the keyword filtering portion of the Web Filter feature above.

6. Program Blocking: With Safe Eyes, an administrative user can specify whether specific programs that access the Internet can be used. Examples would be Instant messengers, media players, P2P file sharing, games, etc. Safe Eyes comes with a pre-built list of applications it can block but the user can always specify any application on their computer they would like to block access to. Safe Eyes only blocks the Intent portion of these applications. This means that, for example, if you blocked iTunes, the Safe Eyes user would be able to

play and listen to music but would not be able to access the iTunes store. Programs are blocked using a combination of filename, application footprint, and TCP/IP protocol patterns.

7. Usage Reporting: Safe Eyes can be configured to report all Internet usage to either the local computer or the Safe Eyes secure servers. By reporting the data only to the local computer the usage logs will only be available on the computer that the access occurred on. This means that if a user used multiple computers in the house their usage data would be spread over multiple computers and in order to view the data the administrator would need to visit each computer. Alternatively, if the data is stored on the secure servers all of a user's usage history is reported to a single place and can be viewed by the administrator from any web-enabled computer.

8. Instant Alerts: The Safe Eyes administrator can opt to receive an instant alert when a Safe Eyes user attempts to access a website that has been banned in the Web Filter section. The alerts can be received by email, text message, or phone call. These alerts are sent from the server to avoid tampering by the user.

Safe Eyes is a versatile tool that is currently in use in homes, schools, business, religious organizations, and libraries in over 125 countries around the world. In order to use Safe Eyes the user's computer must meet the following requirements:

Microsoft Windows: Windows 2000/XP/Vista, Pentium II 233 MHz or faster, 5MB of hard disk space, 128MB of RAM.

Apple Macintosh: OSX 10.4 or higher, PowerPC or Intel processor, 10MB of hard disk space, 128MB of RAM.

EXPERTISE
InternetSafety.com has been developing Internet Safety products since 1999. Our first product, SafeBrowse, was a dialup Internet service that had a web content filter built into the connection that could not be bypassed or disabled. It was the first content filter of its type that allowed each customer to specify the level of filtering enforced when they used the Internet. With the decline of dialup service in 2002, the Company decided to build a stand-alone product, Safe Eyes, which could be installed on any Internet connection. Safe Eyes has consistently rated highly in independent reviews. Notable reviews have included: rated as the #1 product in 2005 by Consumer Reports, two-time winner of PC Magazine's Editor's Choice award, and LAPTOP Magazine Editor's Choice award.

COMPANY OVERVIEW
InternetSafety.com was founded in 1999 by two brothers, Shane & Aaron Kenny. The company was initially funded by a round of "friends and family" investment as well as the cash flow generated from ongoing operations. In January 2007, a round of venture investment gave the company the capital required to fund its growth plans. At the same time Forrest Collier was hired to serve as CEO. Shane Kenny currently serves as COO & President while Aaron Kenny serves as CTO.

In July of 2007 InternetSafety.com successfully won a global bid with the federal government of Australian to provide free Internet filters to its citizens. With its PC and Mac compatible products Safe Eyes currently represents two of the four products available through this government program.

BUSINESS MODEL OVERVIEW
A 12 month subscription of Safe Eyes can be downloaded for $49.95 or purchased on CD-ROM for $54.95. Both the download and CD-ROM versions allow for Safe Eyes to be installed on up to 3 computers – with any mix of Windows or Macintosh.

Distribution to non-profits, start-up sites, and other organizations is handled on a case-by-case basis. This allows us to ensure that we recommend the best InternetSafety.com product to meet the needs of the customer. Non-profits, religious organizations, and schools typically receive a standard discount off of list prices. In addition to the consumer version of Safe Eyes, InternetSafety.com also distributes small business filtering solutions on both a software (Safe Eyes Business) and hardware (EtherShield) basis.

MORE INFORMATION
Company website: www.internetsafety.com

Product websites: www.safeeyes.com
www.ethershield.com

Product User Manual: www.internetsafety.com/safe-eyes/download/SafeEyesUserManual.pdf

Product Screenshots: www.internetsafety.com/computer-monitoring-screenshots.php

CONTACT INFORMATION
Shane Kenny
3979 S. Main Street, Suite 230
Acworth, GA 30101

Email: shane.kenny@internetsafety.com
Phone: 678.384.5302

CERTIFICATION
"I certify that I have read and agree to the terms of the Internet Safety Technical Task Force Intellectual Property Policy."