Internet Safety Technical Task Force
Technology Submission

Symantec Corporation
http://www.symantec.com

JULY 21, 2008

ABSTRACT
Over the past two years, Symantec has researched the issues facing children online – and worked to understand the low adoption rate of parental control products. As a result of this research, we have developed a new approach to keeping kids safe online – Norton Family Safety. This product stays away from the over-bearing "big brother" approach of most parental control products – and utilizes cutting-edge technologies in a family friendly and collaborative environment. Our goal is to provide caregivers with the tools they need to help children safely navigate the internet, while facilitating critical engagement between adults and children regarding online activity.

Keywords
Parental controls, web content filtering, web usage reports, instant messaging controls, computer time limits, social network monitoring

Functional Goals
Please indicate the functional goals of the submitted technology by checking the relevant box(es):
- ☑ 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 – provide parent insight to child online activities

PROBLEM INTRODUCTION
The need for an effective approach to child safety software is clear. The Internet provides children with unprecedented exposure to unfiltered material, as well as an opportunity to put information about themselves out for others to see without understanding the related consequences. Most parents simply do not have the time to monitor all of their children's online activities. Without proper guidance, the Internet can be an unsafe place for children to grow up – kids wanting to appear older can easily present themselves with fabricated identity or age on a social networking site, kids wanting to be noticed can post inappropriate photos of themselves or their Personally Identifiable Information (PII) online, and kids working through serious issues can take risky behavior to new levels by joining unmonitored social groups focused on encouraging destructive behavior such as anorexia or bulimia. Thus, through the Internet, common childhood curiosity or youthful experimentation can lead to long-lasting and serious consequences.

The problem of parental controls is not new by any means – early forms of software have been around for over 20 years. These rudimentary solutions were often "brute force" techniques which simply blocked any internet traffic on the network level with no intelligence. Parental controls have now evolved to try to provide the parent some more level of granularity (blocking web sites by category for example). Many solutions were technically based – how to use the best technology available to restrict activities by children.

Symantec wanted to understand why the market was so fragmented. Before delivering a technical solution, we wanted to first understand the problem. Our internal research took into account the available information on children's online behavior, and actively engaged with industry and child domain experts, along with parents, children and other caregivers.

With the results from this research, we decided to take a new philosophical approach to online family safety – and to address each of the following three areas where current parental controls fail in a new way:

1) The software includes explicit biases in its configuration that forces a particular parenting style by limiting parents with inflexible settings. Symantec avoided this by providing flexible and configurable settings for caregivers to apply their own styles. For example, web content filtering can range from the very strict access – in which a caregiver must pre-approve each and every visited site - to total freedom to surf the Web without any filtering.

2) Children are left out of the process. The children are the most affected by any type of parental controls, as it is their actions that will be blocked or monitored. Our research found that using such software can create a hostile environment in which the child feels helpless – leading many kids to try and subvert the controls and hide their behavior. To address this issue – we took steps to include the child as an active stakeholder in the software. By being actively involved, we believe that children are less likely to want to subvert the technology, and more likely to learn

from the process. Children are provided with access to the portal web site, have the ability to send interactive requests to their parents asking for real-time expansion of restrictions, and can help develop "House Rules," agreeing to comply with certain behaviors online.

3) The software is used as spyware, which creates an aura of distrust, often alienating the parents from the children they are seeking to protect. Contrary to this approach, we wanted to create an environment of trust and collaboration and took specific measures to ensure the child is a part of the process – and always aware of what the software is doing. Messages (via system tray toasters) always alert the child of the software's activity, and the software will never take an action without notifying the child that it was taken.

With this philosophy in hand, we have integrated several of our core technologies to create a new family safety solution that involves the entire family. The goal was to educate the parents to their children's activities online – not to create a restrictive environment of "do this, not that". Symantec reports provide the parent with what we believe is the right level of information, careful to respect the child's right to privacy, to spark talking points between parent and child – while providing a reliable and effective method for parents to guide and manage their children's online behavior.

The software is not a substitute for real interactive parenting, but simply a tool to help out. To do this, Symantec provides the parent with the ability to supervise and monitor their children's online web, instant messaging, search term and social networking activities.

PROPOSED SOLUTION

Architecture

Symantec Family Safety consists of two components: a client-side agent and a server-side agent.

The client-side agent must be installed on the child's computer or laptop. If the agent is not installed, there will be no monitoring or supervision that takes place. Thus, if the child uses a different computer at school or a friend's house, Symantec and the parent will have no knowledge of their activities. The agent is independent of all Symantec products and it can be installed as a stand-alone product or in addition to Symantec products. The agent is also independent of other independent software vendors' anti-virus products. However, due to potential conflicts, it is not designed to work in conjunction with other forms of parental controls.

The purpose of the agent is to provide the monitoring and supervision functionality of the product. The agent monitors outgoing communications on the network level, regardless of the point of origin. So it detects Internet traffic from a browser or a different application (such as iTunes).

The agent can potentially block Internet traffic depending on the policy for the child. The agent also collects information about the child's usage (if enabled by the parent) in log files. The log files are sent up to Symantec servers intermittingly throughout the day. The files are encrypted on the machine, as well as when it is sent to Symantec.

The second component is the Symantec datacenter which houses parent portal. The portal web site is the parent's primary form of contact with the product. Upon log in, the parent will be able to supervise, monitor, and change the settings for their children. The web site is accessible from any Internet browser, regardless of the parent's location. The datacenter houses all the log files in a proprietary partitioned and encrypted database.

Flexibility

The software settings are flexible enough to provide each caregivers the capabilities to enforce their own style. For example, web content filtering can range from the very strict access – in which a caregiver must pre-approve each and every visited site - to total freedom to surf the Web without any filtering.

Child Involvement

The child is an active stakeholder in the process. Parents are encouraged to walk through the set-up with their child, so that the child is aware of what the different settings are. This also helps underscore the point that the software is for the protection of the child, not to create restrictions. The last step of the setup includes development of "House Rules," which compile the agreement between parent and child with regard to computer usage.

The child is also actively involved in the evolution of the product. As the child matures, the software can change and become less (or more) restrictive. If configured to do so, the child can request rule changes to any of the settings – which will be sent to the parent for discussion. For example, the child can request access to a web site or category they were previously blocked from.

Full-Disclosure

Privacy concerns for the child were a key element in the design. Symantec did not want to be considered spyware. In addition to a distinct system tray icon that is present at all times, Symantec does a few other things to notify the child. On every new login, the child is alerted that Symantec software is running. In addition, if there are any rule changes that occur, the child is notified of the rule change and provided a link to the new "House Rules". Finally, Symantec does not take any action that the child is not aware of. If Symantec blocks access to a web site, an appropriate message is displayed. Similarly, if IM monitoring is taking place, the child is notified.

Web Content
Web content filtering is a core feature of Symantec's family safety product. The parent can choose to allow or block web sites based on a specific domain, or category. The category is provided via a third-party URL list. Parents can choose to configure the block to either prohibit the site, or just to warn the child that the site may not be appropriate, giving the child the final say – with notification to the parent if the site is accessed.

Reports and usage stats are generated for each child. The reports only keep the top level domain and reports that to the parent (for example "mail.google.com" is reported as "google.com"). Part of this is to let to child have some sense of privacy while provide the parent some insight into the child's activities. While it is easier to simply report the entire URL, Symantec took an extra step to simplify the reports for the parents. Reports are available for the previous 30 days of data.

Instant Messaging
Symantec allows the parent to manage the child's buddy list, and can detect IM conversations with any of the following protocols: AOL, MSN, ICQ, Yahoo, Google Chat. Buddies can be classified as: "Friends" with no restrictions or monitoring, "Unsure" buddies, which are monitored at the level set by the parent, and "Blocked" buddies, which are completely blocked. IM Message logs are available for the previous 30 days of data.

Search Terms
Search terms provide parents with insight on the intent of the child in surfing the Web. It's one thing if a child comes across a porn site on accident, or against their will via a popup. However, it's another thing if the child is actively searching for mature content. Symantec can monitor search terms for the major search engines: Ask, Google, Yahoo, and provide those terms back to the parent to help stimulate useful conversations about safe online behavior. The search terms are reported for the previous 30 days. In addition, the parent can mandate a "safe search" filtered result from each search engine.

Social Networks
Development of a profile on a social networking site has become extremely common with teens online – and often, this is done without parental guidance or consent. This feature provides parents with information regarding their child's accounts on social networking sites – allowing parents to receive a report on each account that is logged into on the computer. Certain attributes, such as a screen name and age, are captured and reported to the parent. At no time does Symantec capture the child's password.

The report lists the child's screen name and age (if specified in the account) and links to the public profile page of the child. If the social network has "private" pages, the parent is notified that they need to create an account and have the child add them as a friend.

Time Limits
Symantec allows parents to configure standard time and internet restrictions periods. The parent can restrict the time allowance or time period of computer usage. Similarly, the parent can restrict time periods for Internet usage, but still allow computer usage.

Internationalization
We anticipate this product will initially be available in the United States. Internationalization efforts are underway to localize the product for compliance with various laws and cultural-driven online behaviors. We are very conscious of the specific privacy laws in many countries, including the European Union – and are actively working to address these in this product.

EXPERTISE
This product was developed through a collaborative effort between Symantec's research and development teams, primarily driven by the Advanced Concepts division of Symantec Research Labs, under the office of the CTO. Advanced Concepts has a charter to find promising ideas, assemble small development teams and build innovative new products. Norton Family Safety has been in development for the past two years, and recently transferred from the Advanced Concepts team to Symantec's Consumer Business Unit for further development and formal release.

COMPANY OVERVIEW
Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world. The company helps customers protect their infrastructure, information and interactions by delivering software and services that address risks to security, availability, compliance and performance. Headquartered in Cupertino, CA, Symantec has operations in more than 40 countries.

BUSINESS MODEL OVERVIEW
As per the Advanced Concepts charter, the product is currently under a private and limited release pilot period. A public beta will be available in late 2008, and general availability in early 2009.

CONTACT INFORMATION
David Lee, Product Manager
david_lee@symantec.com
424-750-7518

Laura Garcia-Manrique, VP Product Management
laura_garcia-manrique@symantec.com
424-750-7276

900 Corporate Pointe

Culver, City, CA 90230

CERTIFICATION

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

LEGAL NOTICE

The Berkman Center, the Task Force and Task Force members, and the Technical Advisory Board, including its members and affiliates, are under no obligation to maintain the confidentiality of the submitted abstracts or other materials you provide. Please do not submit any information in your technical abstract that is confidential, proprietary or not for public dissemination. Please submit only information that you are willing to have made public. All submissions are subject to the Task Force Intellectual Property Policy: http://cyber.law.harvard.edu/research/isttf/ippolicy. By submitting your abstract or proposal, you certify that you have read and agree to the terms of that Policy.