Internet Safety Technical Task Force
Technology Submission

eGuardian, LLC
http://www.eguardian.com

ABSTRACT
eGuardian was founded on the realization that children are not sufficiently protected on the Internet from predators, inappropriate content and cyberbullying. We believe age verification for minors is the single most effective way to mitigate these threats, while allowing children to safely explore the Internet. We use a unique offline verification process coupled with an online service delivery platform to provide accurate and secure age verification services. Our offline verification leverages school employees and existing processes at the child's school to perform the age verification. Our partners integrate their technology with our web service solution to provide them with age information.

Keywords
identification, age verification, parental controls, filtering

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

PROBLEM INTRODUCTION
Problem: allowing anonymous online communication leads to harmful contact between adults and minors, including sexual solicitation and exposure to age inappropriate content.
Solution: our age verification services allow our partners to protect eGuardian enrolled children from anonymous communication. In contrast to restricting the activities they can perform, we encourage and enable a broader range of activities thereby enhancing the online experience (such as freeform chat, as opposed to select phrase chatting on child websites and exploring social networking profiles of other verified minors in their age range).

Problem: allowing anonymous communication often leads to harmful contact between minors due to circumstances created by anonymity. There is also a vast maturity difference between minors themselves, and thus not all content and communication is appropriate for each user. [1]
Solution: by negating perceived anonymity minors are less likely to engage in inappropriate activities such as cyberbullying. When inappropriate activity does occur, we have a clear path back to the child's parent/guardian to report misconduct. Furthermore, with verified age information our website partners can provide a layer of content and communication separation based on age. This further enhances the experience for each minor.

Problem: 1 in 7 minors received sexual advances on the Internet, and 1 in 3 was exposed to adult content. Exposure to unwanted adult content increased, despite an increase in the use of filters and site blockers [2] .
Solution: working with partners we enable safe online communities and destination sites for eGuardian children. We are more site enablers than site blockers.
Search engines are the predominant method of exposure to websites with inappropriate content [3]. For partners in the search engine space we have established a protocol which immediately communicates to our partner the age of a minor. Search engines can immediately enable filtering of advertising and search results so they are age appropriate. Additionally, adult content websites receive simple communication that the visitor is a minor. This enables the site to immediately block access to any questionable content or imagery even prior to the visitor having to authenticate.

Problem: the creation of inappropriate content on the Internet can come in many forms, including social networking posts, blogs, and text messages. Many occurrences of inappropriate content creation, and cyber-bullying, can be attributed to, or at least exasperated by, the anonymous nature of the Web [4] .
Solution: Although eGuardian does not directly limit/prevent the creation of inappropriate content, this material is inherently restricted while using an identity verified account on a partner website. This helps to

eliminate peer-to-peer cyberbullying activities such as spreading rumors or posting embarrassing content. If this activity does occur, it is now feasible to report this to the minor's parents and have the situation rectified.

Problem: minors will often attempt to find ways to access content and interact with others without parental consent. The desire for this type of activity largely depends on the age of the child. In general, children want the ability to explore and interact with their peers using various avenues of technology. Parents typically want to allow this type of communication, but are hesitant due to the risks and exposure that accompany this exploration.
Solution: we work with site blocking partners to "eGuardian enable" their software. As a result, many partner sites and services that were previously considered unsafe are now safe and thus may not require explicit parental consent. It is typically not the activity itself (such as posting comments on social network sites) that concerns us as parents, it is the content and anonymous relationships that pose a potential problem. eGuardian gives partners the ability to monitor content and make sure the experience is appropriate for the age of the minor, and eliminates anonymous contact without parental consent.

Problem: cyberbullying, harassment and unwanted solicitation of minors are prevalent on the Internet in today's landscape. This leads to unhealthy experiences and interaction for the children.
Solution: A number of factors contribute to cyberbullying. One key issue is the reluctance of children to report the abuse to authority figures [5]. Other factors include fear of losing access to technology, and a belief that cyber bullies cannot be stopped. This type of activity can be effectively controlled within eGuardian partner sites. An eGuardian child who misbehaves can be properly penalized by the partner, parent — or eGuardian as a whole — thus giving children an effective way to report and counteract cyberbullying.

PROPOSED SOLUTION

eGuardian provides a unique and secure solution for verifying the age and identity of minors. Our technology allows us to integrate with partners and provide them with reliable identity verification information.

The key to our enrollment process is that we work directly with schools to verify the age and identity of each minor. We are capable of enrolling children at any public school throughout the United States and Canada. Completing a registration at a new school typically takes between 2-4 days. Our process includes an application submitted by parents to the schools, and a web portal that allows each school to electronically review and approve each child's application. Once the application has passed the verification screening we provide the eGuardian activation account credentials to the verified address on file. These credentials can be used to activate eGuardian protection for any eGuardian partner service, whether that be a website, chat client, email account or other such service.

Our solution consists of two key technology components. The first component is called our "Web Login API". This solution is designed for partners with an online environment, such as a website or web based chat solution, that require their members to authenticate in a browser based environment. Each partner receives API access to verify that the activation credentials provided are indeed active and valid. Once this is determined, they can allow the minor to interact with other eGuardian verified minors within their respective service offering. This API is based on OpenID (http://www.openid.net), and eGuardian is an OpenID provider. We've made key enhancements to our OpenID offering to help improve the integrity of our service. One such improvement was an algorithm developed to detect anomalies in access patterns. For example, if an account authenticates from two IP addresses that are geographically diverse within a specified time frame, we can immediately disable the account. Or, if the account is accessed at non-standard times relevant to the minor's age and typical login patterns, the fraud probability rating on the account is increased. We have also implemented visual queue technology to help mitigate phishing attempts. Once the partner has submitted the OpenID URI to the eGuardian OpenID server, we display our own web page that contains a unique visual experience that the parent and child will recognize upon login. This helps prevent sites attempting to pose as the eGuardian OpenID server and collect activation account passwords. A use case example for our Web Login API would be the registration process on a child-based social interaction site. If the child going through the website's registration process already has an eGuardian account, they can enter the activation account username and password to immediately enable eGuardian protection. If they do not have an eGuardian account they can still be granted access to the site at the discretion of the partner, but the parent must also complete the eGuardian enrollment form. Once they have successfully enabled eGuardian protection for their account, they are then granted full access and/or additional features that may be available on that site only to age verified minors.

The second component is our "Identity Verification API", which is a web service solution. We are not a replacement or competitor of client applications such as site blockers or parental control software. We augment and enhance these applications by providing age verification on top of their existing service. This integration effort is facilitated through our Identity Verification API. The web service is consumed by our partners within their applications. Each partner application will utilize the API features differently based upon the type of service they offer. A specific use case example would be site blocker software. To activate eGuardian protection for the software, the user enters their eGuardian activation credentials. The site blocker software

sends these credentials to the Identity Verification API to validate the account. The client application would also be required to transmit the eGuardian "identity string" (an arbitrary rotating string used by eGuardian as a token to identify the visitor) to approved eGuardian partner websites through a custom HTTP header variable. This identity string is what the website partners in turn transmit to the Identity Verification API to check for account validity and receive the age, gender and zip code of the minor (we never release any personally identifying information, such as name or address).

Our technology effectively provides tools for delivery of age verification information to our partners in a secure manner. Our technology does not by itself protect children, we instead enable our partners to protect the children in their respective environments by virtue of knowing they are working with an identity-verified minor. Our strength lies in our ability to securely and accurately obtain and maintain the identity information database, as well as the simplicity of integration with the technology. The key weaknesses with our technology are a) many of the website partners that use our web login solution rely on username/password combinations in the hands of children; b) due to our offline verification process there is a delay from initial registration to the time in which their account is verified (typically 1-4 days), but at most this is an inconvenience that is offset by the partners allowing immediate restricted access; c) our presence at the personal computer level relies on the existence of an eGuardian enabled client application, which is provided by our partner software, and the quality of our partners' client application solutions. The website and client application partners that integrate eGuardian dictate the effectiveness of the protection. For example, with site blocking software that is transmitting our identity string to website partners, if it is easily disabled or bypassed, then the eGuardian communication is removed as well. We have inherent exposure in this model, but it is also counteracted by lack of motivation by minors to bypass it. If they can still reach the sites and resources they want to find, their motivation for going around the protection is significantly reduced.

The success of our product does not rely on law or policy, although these factors would likely help speed the adoption. We rely on the adoption of the technology with key partners. Our solution does not require ubiquity, it only requires the cooperation of a few key partners to create a safe online community for our children to be effective. Furthermore our technology and business model scales very easily into the international marketplace with any country that maintains an organized school system similar to the US and UK.

The eGuardian solution has been very effective to date in its key area of value, building the identity verification process and garnering participation of schools. We have a multi-incentive based system that tightly integrates eGuardian into the schools and has a very positive fiscal impact for them as well as tremendous benefit for the parents. We have overcome the limitations in getting this process efficient, scalable and financially sustainable.

EXPERTISE

The founders of the company, Ron Zayas and Robert Patrick, have extensive backgrounds in marketing and technology, respectively. Ron brings a world class marketing and strategic background to the company. His expertise has been vital in growing the company and tackling the strategic impediments that have previously slowed acceptance of identity verification on the Internet. Robert brings over 10 years experience as a respected technology consultant for some of the largest firms in the world. Specializing in software system analysis and development, Robert was a perfect match to design the technology infrastructure for eGuardian. We have added industry leaders to our management team that not only complement the founders' skill sets, but also maintain expertise in the entertainment and child product space. Our team is seasoned in the key aspects of the market in which eGuardian operates.

COMPANY OVERVIEW

Ron Zayas (Co-founder and CEO). Ron is the founder and former CEO of 360 Business Consulting, a leading-edge marketing, technology and sales consulting company that operates seven offices in eight states. Started in 2003, 360 Business Consulting's clientele grew to include many of the fastest growing small businesses on the West coast, and a select number of Fortune 500 companies.

Ron co-founded 360 after spending 10 years as the senior vice president and chief marketing officer for the world's largest franchisor of printing and small business services, Franchise Services, Inc. Ron brings expertise in marketing, advertising and ecommerce strategies. While at FSI, Ron oversaw the development of the company's national advertising campaigns, marketing implementation and industry-leading websites and ecommerce infrastructure. His ability to utilize leading-edge technology to accomplish solid marketing objectives helped grow the company and allowed it to venture into new products and service offerings.

Robert Patrick (Co-founder and CTO). As the founder and president of one of Southern California's premier web development companies, PhD Computing, Robert's technical expertise was essential to the design and development of the eGuardian technology for protecting children online. After founding his first software development firm at the age of 18, Robert's leadership established the company as a leader in web based technology. Working with several Fortune 500 companies, his team developed various patented technology that has now become industry standard.

Other key members of the eGuardian team include:

Carolyn Petty (CFO). Carolyn has more than 20 years experience at the startup and corporate finance level. In her executive positions with such major corporations as CBS Television Distribution, Chase Manhattan Bank and Coca-Cola, she has played a key role in technology assessment, budgeting, financial strategy and reporting and operational support.

Jay Elliot (Board of Directors). Jay has more than 30 years operations' experience with such corporate giants as IBM, Intel, and Apple Computer. He served as the Executive Vice President of Apple Computer where he was responsible for all corporate operations plus overall corporate business planning, reporting directly to the CEO. Additionally, Jay reported directly to Steven Jobs, chairman of the board and co-founder of Apple. Jay joined IBM and managed the company's 16,000-employee software division. Jay left IBM to join Intel as the director of the California operations reporting to Intel's CEO, Andy Grove.

Sally Coon (Vice President of Operations). An innovative executive, Sally comes to eGuardian from Franchise Services, Inc. where as a company vice-president she managed a $2 million departmental budget and developed and implemented revised support processes and training programs that improved the company's efficiency and customer service. She has extensive expertise in franchise operations and support, leadership, training, team building, project management, marketing and financial analysis.

eGuardian is funded by private investors and investment groups within Southern California, with a customer base reaching throughout the United States, Canada and the UK. We are consistently adding new partners to leverage and expand the eGuardian protected community of children.

BUSINESS MODEL OVERVIEW

Parents enroll their children in eGuardian for a one-time $29 fee, of which a significant portion of the proceeds go directly back to the school. We also have subsidized programs that can eliminate this cost for families in need.

Our revenues come primarily from technology partners that utilize the eGuardian protection system for commercial purposes. Our goal is to enhance our partners' product offerings, thereby allowing them to charge more for this value added service, and we share in this additional incremental revenue. We collect a monthly fee between 25¢-50¢ per month per identity verified member, based on volume. Alternately, for partners that do not charge access fees and/or rely on advertising, we also offer revenue sharing models derived for this targeted advertising revenue. Our ability to provide identity verified information allows for better targeted, and more appropriate, advertising to eGuardian protected children which has been positively received by the parents. Partners are able to charge more for the directed ads.

Given that our model is based on volume, performance and incremental profit sharing, it is very accessible to start-up sites and services. We offer reduced pricing programs to non-profit organizations that not only allow them to utilize the service, but they can potentially generate additional revenue for themselves through enrollments.

MORE INFORMATION

For additional information on eGuardian visit our website at http://www.eguardian.com/isttf. Here you will find more specific information such as:

How We Protect Children:
http://eguardian.com/howitprotects.php

Our Process:
http://eguardian.com/ourprocess.php

Frequently Asked Questions:
http://eguardian.com/faq.php

CONTACT INFORMATION

Robert Patrick (CTO)
robert.patrick@eguardian.com
direct: (909) 740-3161
office: (949) 279.4680

3281 East Guasti Road
Suite 320
Ontario, California
91761

CERTIFICATION

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

REFERENCES

1. US Computer Emergency Readiness Team (http://www.us-cert.gov/cas/tips/ST06-005.html)

2. The National Center for Mission and Exploited Children (http://www.missingkids.com/en_US/publications/NC132.pdf)

3. Georgia Tech survey on web use (http://www.gvu.gatech.edu/user_surveys/survey-1997-10/graphs/use/How_Users_Find_out_About_WWW_Pages.html)

4. Patchin, J. W. & Hinduja, S. (2006). Bullies move beyond the schoolyard: A preliminary look at cyberbullying Youth Violence and Juvenile Justice, 4(2), 148-169)

5. National Children's Home Charity and Tesco Mobile 2005 Survey)

(http://www.nch.org.uk/uploads/documents/Mobile_bullying_%20report.pdf)