TAB Observer Comment Form

1. Please clearly identify the Submission you are commenting upon (Company Name and Key Product/Technology Information)

   Company Name: Crystal Reference Systems
   Key Product: ChatSafe (Text Analysis of Pedophile Activity)

2. Your Name/Address/Email/Official Title and Affiliations

   Dr. Teresa Piliouras (email: piliouras@west.poly.edu)
   Adjunct Professor of Management Information Systems
   Center for Emerging Technologies - Hawthorne Graduate Center
   Polytechnic University of NYU
   40 Saw Mill River Road
   Hawthorne, NY 10532

3. Please provide and describe any and all affiliations or interests you may have related to the work of the Task Force and the TAB. This includes professional, financial, and legal affiliations that might potentially influence your thought and opinion about child safety online.

   Dr. Teresa Piliouras – Other Affiliations
   Teresa Piliouras is an Adjunct Professor in Computer and Information Science/Technology Management at Polytechnic University, where she has taught since 1994. Dr. Piliouras is working on ways to protect children on the Internet and to promote public health. She is involved in a number of broad-based community outreach programs to bring seniors and "at-risk" youth together to address problems of health and wellness. This involves creating community wiki-webs designed to create a sense of support and community, especially among those who may have been marginalized in the past. She is founder and President of Albright Associates, a company dedicated to protecting the privacy and safety of children in digital environments.

4. Please provide any commentary you would like the TAB and Task Force to review, keeping in mind that this document is public information and will be made publicly available.

1. SCOPE AND AIM OF COMMENTS

The scope of these comments is limited strictly to a review of information contained in the completed "Internet Safety Technical Task Force Technology Submission Template" which vendors submitted to the TAB, including referenced company websites and literature, and company profiles obtained from Hoover's. As a result, some of these

observations may be based on incomplete, in accurate, or outdated information, and should not be viewed as definitive. Although a best effort has been put forth to provide reliable information, we do not make any guarantee of its accuracy and do not assume responsibility for the consequences of its use. No direct testing or performance evaluation was conducted on the product submissions.

The aim of these observations is to provide a context for comparing vendor submissions with respect to each other and relative to the stated goals of the TAB.

2. SUMMARY OF FINDINGS

ChatSafe by Crystal Reference Systems was one of seven (7) text analysis technology solutions received by the TAB. This type of solution represented 18% of all forty (40) vendor submissions.

The product submissions relating to text analysis used one of three (3) basic approaches:

1. *Linguistic analysis of online conversations over time for inappropriate content and exchanges*.
    - ChatSafe's approach falls into this category. ChatSafe does not appear to have tools to collect transcripts of chats and conversations, and this implies some other mechanism must be used to capture this input before it can be analyzed. This solution appears to be best suited for forensic investigations. DeepNines itrust platform examines applications that look "dangerous", and provides tools to capture data traffic and user information. It is possible that itrust might be used to automate the capture and delivery of suspicious data feeds to ChatSafe for further analysis.

    - ALIAS is in this category, and of all the submissions appears to be the most similar to ChatSafe.

    - Credint's TeenSafe solution is in this category. Unlike ChatSafe and Alias, it provides a mechanism for capturing online conversations so they can be analyzed. It also provides parental alerts. TeenSafe was designed for use on a specific personal computer or smart phone, or alternatively, can be implemented by ISPs, Instant Messenger (IM) vendors, and within the Internet cloud.

2. *Monitoring of online conversations for suspicious behaviors and exchanges with known predators*. This differs from the previous category in that is examines an online exchange at a particular point in time and attempts to determine if it involves an individual on a registered black list.

    - Mc Gruff SafeGuards' approach falls into this category. The vendor's submission to TAB did not explicitly describe the mechanism for

monitoring and identifying suspicious conversations. SafeGuard capabilities include parental alert and reporting features which can also be used by law enforcement.

3. *Profiling of user or content based on pre-defined criteria*:

    - Keibi's approach falls into this category. It examines text to determine if it contains obscenity, violence, abuse of Terms Of Service (bullying or illegal activity) and spam. This solution does not look at conversations per se but rather the overall appropriateness and source of content. If it is discovered that a member has posted objectionable content, their content can be removed and they can be blocked from making future postings. Although this tool offers text analysis, because of these capabilities, it is considered primarily a filtering and blocking tool. This service operates on a subscriber website or ISP, and does not require installation of client software.

    - EthoSafes' approach falls into this category. EthoSafe assign tags to content using a combination of automated and manual methods. These tags provide qualitative assessments of the content which are used to match against a website's terms of use policies. For example, EthoSafe has a standard set of tags in the categories of language, nudity, violence, sex, potential harm (e.g. drug references), and spam. In addition to the standard tags, clients have the option of specifying custom tags. This solution operates as a Software as a Service for social media publishers.

    - TAT's approach falls into this category. TAT (Text Attribution Tool) creates profiles of user age, demographics, and psychometric traits for the purpose of assisting law enforcement and forensic investigations. The vendor submission to TAB did not explicitly mention a mechanism for capturing suspicious conversations, and this implies some other mechanism must be used to capture input before it can be analyzed by TAT.

All of the companies submitting text analysis solutions had 20 or fewer employees. They may thus be considered small businesses. None are dominant in their industry.

3. COMPANY SIZE (NUMBER OF EMPLOYEES)

Based on data collected from Hoovers on the number of employees working for vendors making submissions relating to text analysis technologies:

- All of the companies had 20 or fewer employees.

In the chart below, companies are presented alphabetically within the same employee size group.

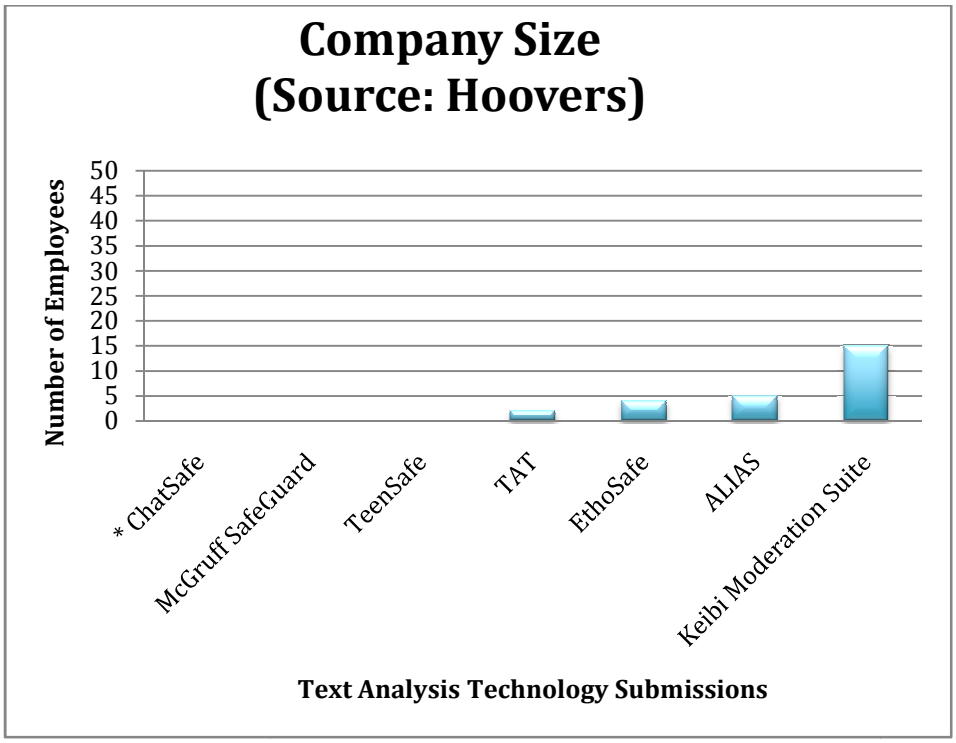

Figure 1: "Text Analysis" Submissions By Company Size

TAB Observer Comment Form

1. Please clearly identify the Submission you are commenting upon (Company Name and Key Product/Technology Information)

   Company Name: IDology, Inc.
   Key Product: IdV (Identity Verification)

2. Your Name/Address/Email/Official Title and Affiliations

   Dr. Teresa Piliouras (email: piliouras@west.poly.edu)
   Adjunct Professor of Management Information Systems
   Center for Emerging Technologies - Hawthorne Graduate Center
   Polytechnic University of NYU
   40 Saw Mill River Road
   Hawthorne, NY 10532

3. Please provide and describe any and all affiliations or interests you may have related to the work of the Task Force and the TAB. This includes professional, financial, and legal affiliations that might potentially influence your thought and opinion about child safety online.

   Dr. Teresa Piliouras – Other Affiliations
   Teresa Piliouras is an Adjunct Professor in Computer and Information Science/Technology Management at Polytechnic University, where she has taught since 1994. Dr. Piliouras is working on ways to protect children on the Internet and to promote public health. She is involved in a number of broad-based community outreach programs to bring seniors and "at-risk" youth together to address problems of health and wellness. This involves creating community wiki-webs designed to create a sense of support and community, especially among those who may have been marginalized in the past. She is founder and President of Albright Associates, a company dedicated to protecting the privacy and safety of children in digital environments.

4. Please provide any commentary you would like the TAB and Task Force to review, keeping in mind that this document is public information and will be made publicly available.

1. SCOPE AND AIM OF COMMENTS

The scope of these comments is limited strictly to a review of information contained in the completed "Internet Safety Technical Task Force Technology Submission Template" which vendors submitted to the TAB, including referenced company websites and literature, and company profiles obtained from Hoover's. As a result, some of these

observations may be based on incomplete, in accurate, or outdated information, and should not be viewed as definitive. Although a best effort has been put forth to provide reliable information, we do not make any guarantee of its accuracy and do not assume responsibility for the consequences of its use. No direct testing or performance evaluation was conducted on the product submissions.

The aim of these observations is to provide a context for comparing vendor submissions with respect to each other and relative to the stated goals of the TAB.

2. SUMMARY OF FINDINGS

In a previous analysis performed for the TAB by the author, a number of age verification tools were identified, including: Bharosa's Authenticator, Trufina's Personal Identification Management, Zvetco Biometrics' Verifi "One-Touch" System, Veratad, RSA Identity Verification, Verified Person, Geotrust's Identity Verification, and Intelius. These tools were not included in the vendor submissions suggesting the spectrum of available solutions is not fully represented. The TAB may need to make additional solicitations to encourage greater response and better overall representation of available internet safety solutions.

IDology was one of seventeen (17) age verification technology solutions received by the TAB. This type of solution class represented 43% of all vendor submissions.

Six (6) basic variations to age verification were represented in the vendor submissions. IDology's approach to age verification is based on public records.

In general, the verification solutions relied upon: 1) user or parent asserted identity and age information, which is possibly matched against previously created databases of user characteristics, 2) or a computer specially configured to check a biometric or log-in source.

The safety protection afforded in the first case is largely dependent upon the user's veracity and is most effective for adults (and can be defeated if a person knows information about another person which they use to impersonate them). This approach may be used to prequalify and verify the identity characteristics of a parent registering their child for a protection service; however, generally a child's identity and association with a parent cannot be established without some sort of direct personal verification (for example, at a school or medical facility). Even in these cases, it may be difficult, if not impossible, to establish a definitive relationship between a parent in child because of a variety of guardianship, custody, adoption, and other legal considerations.

In the second case, identity controls may be circumvented if the child uses a machine that does not have them installed.

Most (88%) of the companies submitting age verification solutions had 100 or fewer employees and are not dominant in their industry, and may thus be considered small businesses.

3. AGE VERIFICATION APPROACH

"On-line age/identity providers" are important from two perspectives. First, a secure enrollment process for children which includes age information would support automated monitoring and filtering based on age. Second, a safe process would not allow an adult to register as a child.

Six (6) different approaches to age verification were represented in the seven-teen (17) TAB submissions, including:

- Biometrics - fingerprint, voice, or face recognition analysis used to estimate user age;
- Notary Publics - who review government issued identity document and assert that document bearer is rightful owner so an identity credential can be issued;
- Peer-based - using online social reputation scores to give evidence of a person's age and identity characteristics;
- Public Records Data – which is matched against user-asserted data when the person attempts to enter an age or identity controlled website;
- Schools - which vouch for and register current students in identity verification program;
- Token – which involves installing hardware and/or software devices on a personal computer to limit user access to websites and/or content based on previously established user, parental, or website policies.

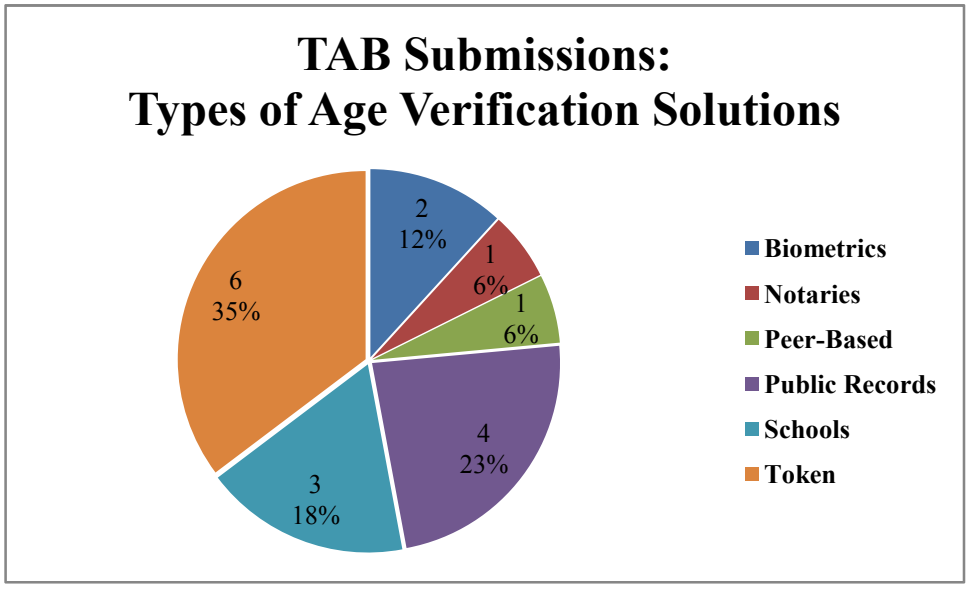

Figure 1: Types of Age Verification Solutions Submitted to TAB

IDology's approach to age and identity verification is based on compilations of publically available records on private citizens. When a person attempts to enter an age-controlled website using its services, they are asked questions such as their full name, telephone number, and Social-Security-Number. Answers are then checked against previously stored information. If they match, the person is deemed verified. Because this information is public and readily available to close friends and family, it does not establish a person's identity so much as the fact that a person with such a name and phone number exists. This approach to age/identity verification does not work well for children because this type of personal data generally is not available from public databases.

4. IDENTITY SERVICE VERSUS IDENTITY INFRASTRUCTURE

Another way to view the TAB submissions is by the type of identity service(s) they provide:

- *Identity provider services* – which establish and issue credentials for an end-user's on-line identity;
- *Identity infrastructure services* - which link an end- user, relying party, and an identity provider to facilitate the granting of rights by the relying party (which uses the on-line identity in some online context, such as an online transaction).

As defined above, IDology provides an identity provider service. It does this by verifying a user's age and identity, and issuing credentials which are used by a website to qualify visitors.

An issue underlying the functionality and effectiveness of the products examined in this report is the notion of on-line identity. In the on-line world, we must understand the difference between an individual's "true identity" (TID) and their potentially pseudonymous on-line identity (OLID), how both are used, and the relationship between them. In many cases, people use OLIDs that have no obvious link to their TID. Even in cases where a real name is used for the OLID, ambiguities and duplicate names make it difficult to reliably map an OLID to a TID.

In the case of on-line child safety, it is not necessary (or even desirable in some cases) for the TID to be available to others on-line. But it may be important to have attributes of the TID available to the protection software for that software to operate effectively. For example, in various kinds of online communications the age of the user is often important, and potentially their criminal record of a user (e. g., in the case of a registered sex offender). In other cases, such as the investigation of inappropriate on-line behavior, or discovering who a "bad actor" is and with whom s/he has been communicating, a reliable link between the OLID and TID is critical.

With this in mind, examination of the way these products handle identity issues is a key part of the evaluation process. To foster that examination, we discuss some of the relevant basic concepts of identity in the on-line environment.

Identity is always used in some context, be it real world or on-line. The on-line context may be shopping, participation in discussion groups, blogging, and participation in a social networking web site.

In the simple case of, for example, setting up a free email account with a "user name" of the user's choice, the mail server is the relying party. The rights granted are the right to read, send, and manipulate email for that user name. The identity provider is the user, who creates the user name and password when creating the account. The "identity infrastructure" is internal to the mail server.

Another simple example is purchasing a book form an on-line bookstore with a credit card. In this case, the relying party is the bookstore, and the rights granted are essentially the right to use the credit card to purchase books. Here, the identity provider is the credit card company—they give the user the credit card (credentials) to use along with his name. The "identity infrastructure" is an Internet connection from the bookstore server to the credit card server, with the transaction information sent to the credit card server, which in turn can authorize the charge or not. In this case, the credit card company is an identity provider for multiple users and to multiple relying parties. Note, very significantly, that the identity provider performs some kind of investigation (credit check, etc.) before issuing the credentials. In this case, the identity provider essentially authenticates the user (from their knowledge of the card number, security code, and possibly name and/or mailing address), and only grants rights to charge a purchase for a certain amount of money.

There is growing momentum building towards the use of broader identity infrastructures that use a common framework to link multiple identity providers, multiple users, and multiple relying parties. These frameworks allow users to authenticate themselves to the identity infrastructure or identity provider. The identity provider may then provide only relevant assertions about the user (which possibly may not include their name) to the relying party. Examples of recent projects that fall broadly into the concept of identity infrastructures include Microsoft CardSpace, the Liberty Alliance (originating in the financial community), the open source Higgins Project (backed by IBM, Novel, and others), and the open source OpenID program. Child safety products evaluated in this study use some of these infrastructures.

Several questions about the identity providers need to be considered:

- How is a person's identity created?
- Is there an OLID linked to a TID? If so, how is that TID verified by the identity provider?

- How secure is the identity provider's systems? Can they be broken into easily to create fake identities, or steal credentials for valid identities?

In short, how trustworthy is any identity from the identity provider? In practice, there is a great range of trustworthiness in identity providers.

Banks and financial institutions are identity providers when they issue credit and debit cards. They do provide some degree of true identity verification before issuing credentials via credit checks, etc. In general (but not always), they are a reliable issuer of identity credentials based on TID verification, but in the hands of users and relying parties these credentials can sometimes be "stolen." In some cases, stronger credentials such as one time use credit card numbers, cryptographic identity tokens, or biometrics, which are more difficult to "steal," are used.

Many on line services allow the user to create their own identity (e. g., screen name, or email address) and credentials (password); in other words the user is essentially the identity provider. This "user centric identity" is common on social networking sites, discussion sites, email providers, etc. In some cases of user centric identity, these are paid services (e. g., some email providers), so there is a (possibly hidden) link of the OLID to a TID via credit card number and cardholder name. In other cases, a user may be asked to associate their TID (name, address) with their OLID, but the information is not verified, and is therefore unreliable. In many cases, no name is requested when the OLID is created.

All the identity infrastructures mentioned above can, in principal, be used with different types of identity providers. However, Liberty Alliance, for example, is focused more on financial institutions and similar entities; while OpenID, for example, is focused on user centric identity.

The common philosophy of user centric identity is that a single OLID is created and used in multiple on-line activities, and the on-line community develops trust in the OLID over time based on on-line actions. The user also has control when to use the identity, and what information about that OLID to share in any on-line exchange.

For child on-line safety products, the use of identity should be reviewed with the above observations in mind, and questions such as these should be asked:

- If an OLID is used without any linkage to a TLD, can any information about that TLD (such as age, criminal record) be trusted?
- If there is a link to a TLD, how reliable is that linkage? Is the linkage made through a reliable third party (e. g. a financial institution, a verified parent, etc.)
- If a TLD is provided by the user, but not verified, can that be trusted?
- If a TLD is provided (verified or not), and used to determine information about the TLD (such as age, criminal record) from other sources, how reliable

is the use of the TLD in locating records about that TLD? Will similar names/addresses lead to using information about another individual? Will alternate spellings, use of middle names, etc. lead to not finding important records?

If the verification process does not identify a child conclusively, the identity infrastructure and associated identity provider services may be compromised. Even if these functions perform well, if they are not active when a child uses a computer, the child is at risk. There is a need for comprehensive tool interaction to provide significantly stronger child safeguards than currently exist or which can be provided by these tools working in isolation.

In summary, the use of identity on-line is often a difficult problem, and any proposed solutions require very careful analysis.

5. COMPANY SIZE (NUMBER OF EMPLOYEES)

Based on data collected from Hoovers on the number of employees working for vendors making submissions to the TAB relating to age verification technologies:

- 88% of the companies had 100 or fewer employees.
- Microsoft dominated all others by several orders of magnitude.

IDology, as a small business, is representative of the companies offering age-verification submissions to the TAB.

In the chart below, companies are presented alphabetically within the same employee size group.

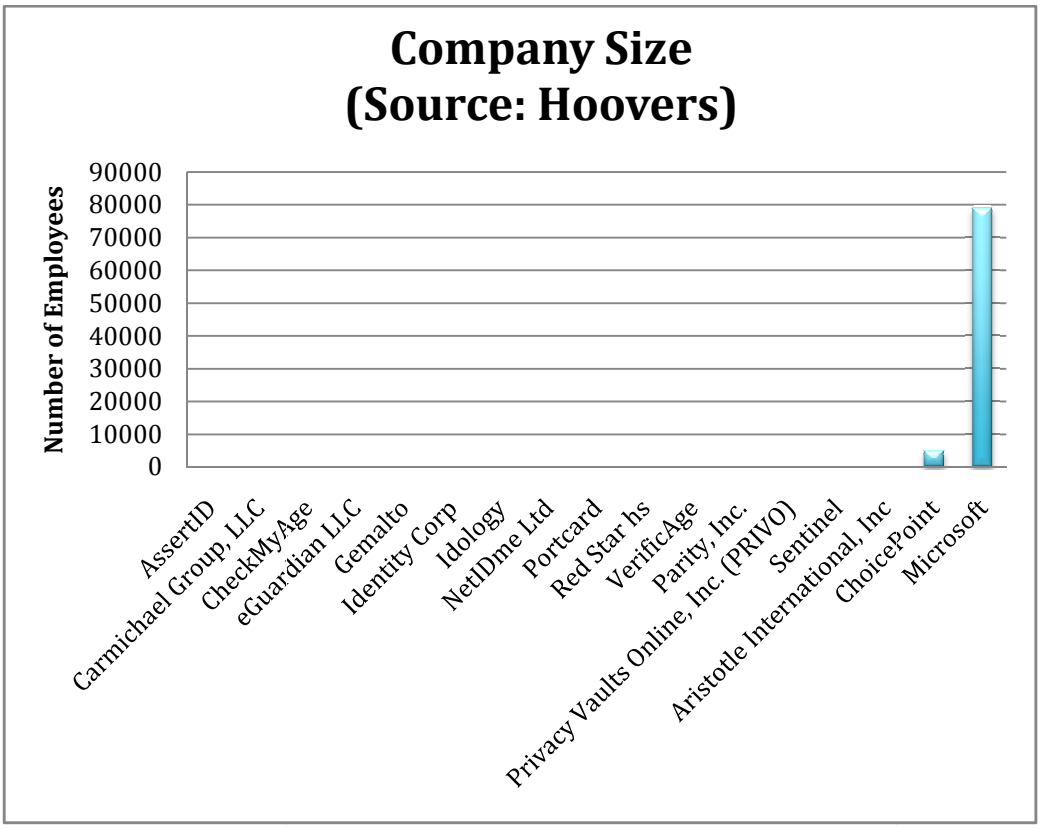

Figure 2: Age Verification Submissions By Company Size

TAB Observer Comment Form

1. Please clearly identify the Submission you are commenting upon (Company Name and Key Product/Technology Information)

   Company Name: Symantec
   Key Product: Symantec Family Safety (Filtering)

2. Your Name/Address/Email/Official Title and Affiliations

   Dr. Teresa Piliouras (email: piliouras@west.poly.edu)
   Adjunct Professor of Management Information Systems
   Center for Emerging Technologies - Hawthorne Graduate Center
   Polytechnic University of NYU
   40 Saw Mill River Road
   Hawthorne, NY 10532

3. Please provide and describe any and all affiliations or interests you may have related to the work of the Task Force and the TAB. This includes professional, financial, and legal affiliations that might potentially influence your thought and opinion about child safety online.

   Dr. Teresa Piliouras – Other Affiliations
   Teresa Piliouras is an Adjunct Professor in Computer and Information Science/Technology Management at Polytechnic University, where she has taught since 1994. Dr. Piliouras is working on ways to protect children on the Internet and to promote public health. She is involved in a number of broad-based community outreach programs to bring seniors and "at-risk" youth together to address problems of health and wellness. This involves creating community wiki-webs designed to create a sense of support and community, especially among those who may have been marginalized in the past. She is founder and President of Albright Associates, a company dedicated to protecting the privacy and safety of children in digital environments.

4. Please provide any commentary you would like the TAB and Task Force to review, keeping in mind that this document is public information and will be made publicly available.

1. SCOPE AND AIM OF COMMENTS

The scope of these comments is limited strictly to a review of information contained in the completed "Internet Safety Technical Task Force Technology Submission Template" which vendors submitted to the TAB, including referenced company websites and

literature, and company profiles obtained from Hoover's. As a result, some of these observations may be based on incomplete, inaccurate, or outdated information, and should not be viewed as definitive. Although a best effort has been put forth to provide reliable information, we do not make any guarantee of its accuracy and do not assume responsibility for the consequences of its use. No direct testing or performance evaluation was conducted on the product submissions.

The aim of these observations is to provide a context for comparing vendor submissions with respect to each other and relative to the stated goals of the TAB.

2. SUMMARY OF FINDINGS

In a previous analysis performed for the TAB by the author, a number of filtering and auditing tools were identified, including: Blue Coat Systems' K9 Web Protection, McAfee Security Suite, and Online Chaperone. These tools were not included in the vendor submissions suggesting the spectrum of available solutions is not fully represented. The TAB may need to make additional solicitations to encourage greater response and better overall representation of available internet safety solutions.

The Symantec Family Safety submission was one of fourteen (14) filtering and auditing solutions received by the TAB. Of the submissions, Symantec and Gemalto are clearly major industry players. This type of child safety solution represented 35% of all vendor submissions, second in size behind the class of age verification submissions (43%).

Three (3) basic approaches to filtering are represented in the TAB submissions: client based solutions implemented on a home computer; service provider solutions implemented by a website or content provider; and a combination of both. Symantec's approach to filtering uses a client based software implementation on a home computer.

In general, in the case of the *filtering and blocking solutions*, if a child uses a computer outside their home and away from their parent's watchful eyes, the child will not be protected if the machine is not similarly configured with filtering controls. Some solutions attempt to address this problem by requiring the website to prequalify visitors with respect to age. However these solutions are not implemented on a significant commercial scale, especially on sites catering to youth.

Predator blocking solutions can be circumvented if the predator chooses to create a fake persona using an email address that is not logged in central predator registries. These solutions are effective if the predator is honest about their online identity, but they can be defeated if they are not.

Content blocking may be effective in preventing illegal or inappropriate content from being displayed on websites, but broad based protection for children requires that these solutions be widely implemented on many websites.

3. FILTERING APPROACH

The three (3) approaches to filtering and auditing represented in the TAB submissions include:

- *Client-based approaches* which involve installing software on a home computer for the purposes of limiting a child's access to the Internet or to specific types of content, and/or monitoring and reporting the child's activities to parents. The vendor submissions in this category included: Symantec; Covenant Eyes products; Kidsnet; McGruff SafeGuard; NetNanny; PureSight; SafeEyes; SaferSpace; and Spectorsoft.
- *Service provider approaches* which involve use of software on websites for the purpose of limiting the content which users may access or view. The vendor submissions in this category included: DeepNine, GMT, and Keibi.
- *Combination approaches* which involve the use of client and website based interventions working in concert to limit access and inappropriate content. The vendor submission in this category was Gemalto's smart card/USB solution which operates in conjunction with a service provider to block visitors from entering if s/he does not have the necessary smart card or USB configuration installed on their machine.

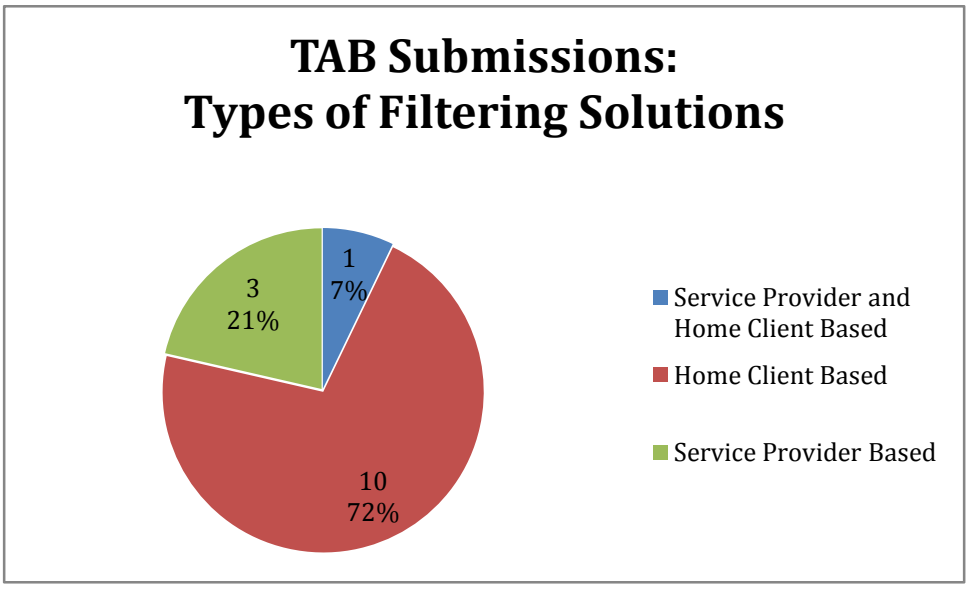

Figure 1: Types of Filtering Solutions Submitted to TAB

4. COMPANY SIZE (NUMBER OF EMPLOYEES)

Based on data collected from Hoovers on the number of employees working for vendors making submissions relating to filtering technologies:

- All but two (85%) of the companies had 100 or fewer employees.
- With respect to company size, Symantec and Gemalto dominated other submissions by several orders of magnitude, and are clearly leaders in their respective markets.

In the chart below, companies are presented alphabetically within the same employee size group.

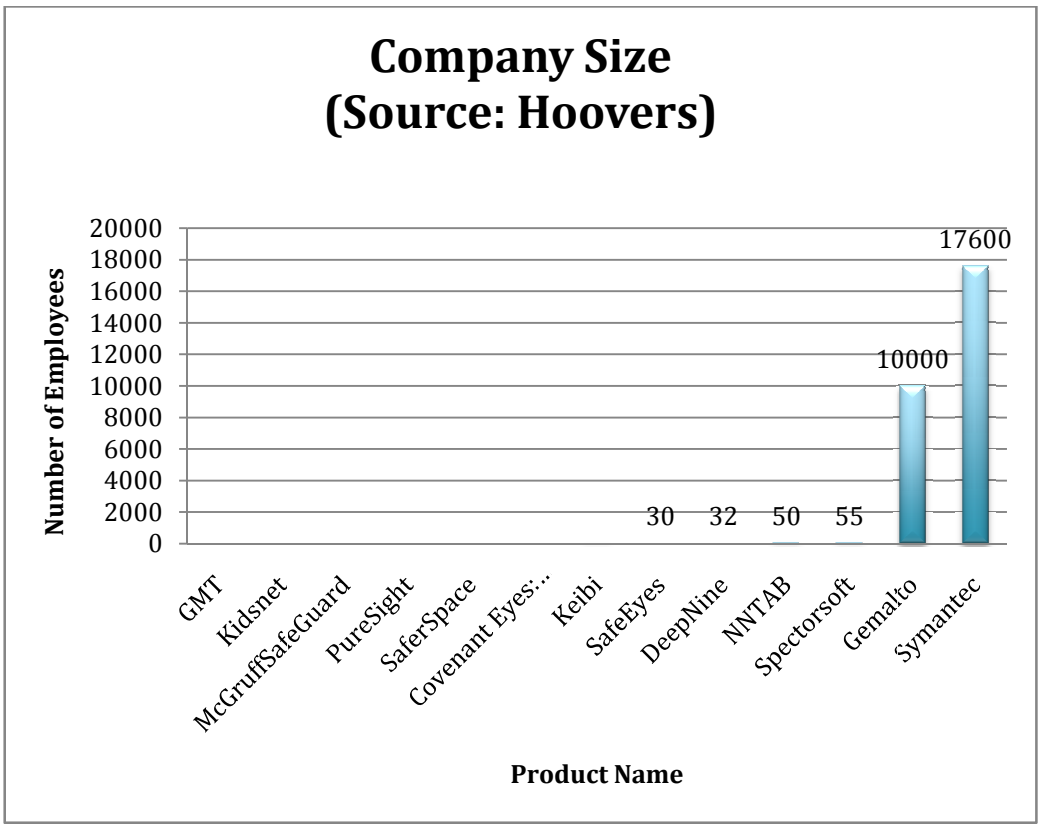

Figure 2: Filtering Submissions By Company Size