TAB Observer Comment Form

1. Submission: ALIAS (Chaski/Croghan/ALIAS Technology LLC)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: Although the submission provides no information about the effectiveness of the assessment of "predatory text," if effective the ALIAS technology may have some potential to be used by large, well-funded service providers for individual, case-by-case assessment of possible "predatory text."

-- Security/Privacy/Practical Considerations: a. If ALIAS is intended to be used to perform analysis of high volumes of text, the submission does not indicate how many "texts" could be analyzed in any given period of time. Given this uncertainty, and given the pricing model, it seems very unlikely that ALIAS could be used to screen in real time all communications over a popular communications service. Although the $100,000 price indicates that an "unlimited" number of screenings can be done, it seems unlikely that $100,000 would cover the screening of millions of texts per day (since the other pricing ranges from $.50 to $100 per screening).

b. Given the pricing structure, ALIAS does not appear to offer any value for free, low cost, or non-profit (but high volume) communications services.

c. There is no indication of whether the ALIAS screening would be done within the network of the communications service provider, or whether all communications by users would be transmitted to the ALIAS company for analysis. If the latter, significant privacy and security concerns are raised by the transmission of all communications to a third party.

d. All of the examples of actual use of ALIAS technology appear to involve, at a minimum, multi-paragraph letters or documents, and there is no indication in the submission of how effective the technology could be to discern the "predatory" or "bullying" intention behind very short messages (such as "LMIRL 2nite" and "4Q" – both of which could easily be benign or in some cases problematic).

e. With regard to threat letters (the only category of document for which the submission provides error rates), it appears that there is a 3-4% false positive rate. If such mis-identified communications are automatically blocked within a given

communications system, it seems likely that users might gravitate away from such a system toward systems that do not block legitimate messages.

-- Policy Considerations: f. A governmental mandate to use this technology to block or screen communications would almost certainly violate the U.S. Constitution. As one particular example, the ALIAS system would "overblock" almost 4 percent of all "angry letters to public officials" – a category of communication that is highly protected under the U.S. First Amendment.

TAB Observer Comment Form

1. Submission: Data Stream Profiling Tool/DSP (Appen Speech and Language Technology Inc.)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: The proposed technology is aimed at law enforcement uses when investigating a specific "person of interest." Based on the submission, the product may be useful in that context.

-- Security/Privacy/Practical Considerations: a. As the submission notes, there would be serious privacy and security concerns if the technology is deployed on a publicly accessible computer such as in an Internet café.

-- Policy Considerations: b. Any use of this technology by a government must be pursuant to court order or other lawful process.

TAB Observer Comment Form

1. Submission: Text Attribution Tool/TAT (Appen Speech and Language Technology Inc.)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: Although the submission provides no information about the effectiveness of the age assessment of text, if effective TAT technology may have some potential to be used by large, well-funded service providers for individual, case-by-case assessment of suspicious text.

-- Security/Privacy/Practical Considerations: a. If TAT is intended to be used to perform analysis of high volumes of text in real time, the submission does not indicate how many "texts" could be analyzed in any given period of time. Given this uncertainty, and given an unclear pricing model, it seems unlikely that TAT could be used to screen in real time all communications over a popular communications service.

b. It appears that TAT requires "training data consisting of documents that are known to represent some factor of interest," but it is not clear where TAT expects to obtain such training data.

c. Given the pricing structure, TAT does not appear to offer any value for free, low cost, or non-profit (but high volume) communications services.

d. All texts to be screened would be transmitted to the Appen Speech and Language Technology company for analysis. Significant privacy and security concerns are raised by the transmission of all communications to a third party.

e. Although no actual use cases are identified, it appears like that TAT technology is intended to analyze text that is, at a minimum, at least a few paragraphs long, and there is no indication in the submission of how effective the technology could be to discern the age of the writer of very short messages (such as "LMIRL 2nite" and "4Q").

f. TAT appears to have potential as a tool to flag suspicious text for later review by humans, and the submission does not suggest that it should be used as an automatic system to block content.

-- Policy Considerations: g. A governmental mandate to use this technology to automatically block or screen communications would almost certainly violate the U.S. Constitution because of the problem of false positives.

TAB Observer Comment Form

1. Submission: Aristotle Integrity (Aristotle International, Inc./Philips)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: The Integrity product may have potential to be used by large, well-funded service providers for voluntary screening of users, as well as by smaller providers that sell products or services and thus can recoup the cost of verification through Aristotle.

-- Security/Privacy/Practical Considerations: a. With the Integrity system, sensitive personal information appears to be transmitted over the Internet without encryption or other protection. Although Aristotle indicates that it does not retain the data it receives, there are few prohibitions on such retention. The transmission of sensitive information to third parties raises significant privacy and security concerns.

b. As the submission notes, the Integrity system does nothing to prevent the sharing of credentials once a verification has been completed. The proposed system appears to be most useful in contexts where all parties want to keep identities secure (such as with gambling where losses are charged to a user's credit card), and less useful in social networking and other mass-market (and often free) services that allow broad communications.

c. As the submission notes, there is no effective way to verify the relationship between two individuals who claim to be a parent and child.

d. As the submission notes, the effectiveness of the system will vary depending on geography, and thus Integrity is less useful for a global service with international users.

e. Given the pricing structure, Integrity does not appear to offer any value for free, low cost, or non-profit communications services.

f. In cases where a user is unable to match information available to Aristotle, the user will often be effectively precluded from using the service (because of a lack of availability of fax capability, lack of time, aversion to faxing copies of identifications, etc.).

g. Users who value the largely anonymous nature of most major social networking services will likely gravitate away from any service that requires authenticated verification.

-- Policy Considerations: h. A governmental mandate to use this technology to block or screen users or communications would almost certainly violate the U.S. Constitution, both by restricting users that Aristotle cannot validate from communicating, and by destroying the constitutional right to communicate anonymously.

i. Broader societal concerns are raised by the ability of private companies to access the diversity of sensitive personal data used by this technology.

TAB Observer Comment Form

1. Submission: AssertID (AssertID/Choi/Trilli)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: By setting out to collect, aggregate, and maintain a comprehensive database of information on all minors in the U.S. (including urging minors to provide personal information online), and by encouraging minors to expose their personal information to online acquaintances for "verification," this proposed system would appear to create far more privacy and security problems than it would solve.

-- Security/Privacy/Practical Considerations: a. With the AssertID system, sensitive personal information is transmitted over the Internet, and the submission does not indicate how that information is protected while in transit over the Internet. The transmission of sensitive information to third parties raises significant privacy and security concerns.

b. AssertID anticipates that a private company would create and maintain a centralized, authoritative database of minors. The privacy and security risks of this approach are significant (and the database would be targeted by hackers, predators, and marketers).

c. The AssertID system appears to do nothing to prevent the sharing of credentials once a verification has been completed. The proposed system is less likely to be effective in contexts in which users have little incentive to maintain tight control of accounts they create – such as social networking and other mass-market (and often free) services that allow broad communications.

d. There is no effective way to verify the relationship between two individuals who claim to be a parent and child (as the submission implicitly acknowledges).

e. Although the pricing structure is not stated, AssertID does not appear to offer any value for free, low cost, or non-profit communications services.

f. Users who value the largely anonymous nature of most major social networking services will likely gravitate away from any service that requires authenticated verification.

g. By requiring minors to disclose information online (and to do so directly to online acquaintances), AssertID appears to run contrary to the accepted advice to minors to NOT disclose information online.

h. The AssertID system seems to be open to a range of attacks from the user base, including for example:

(1) A social norm within a community could arise such that everyone "should" always "verify" ANY fact requested by AssertID to be verified. Such a norm would maximize the ability of users to get online with a minimum of hassle (something that most users would support), and it would greatly undermine the AssertID system.

(2) A group of peers could collaborate to "verify" a completely bogus online identity (by, for example, all agreeing that the fictitious person is over 18-years old and lives in a certain place), and then could share that identity to access services anonymously or services appropriate for other age groups.

(3) A group of peers could easily mount an effective "denial of service" attack on a bullying-target by, as a group, rejecting all of the target's requests for verification. This would seem to offer an opportunity for bullying.

i. By requiring minors (and others) to always use the same e-mail address, AssertID would seem to prevent a common privacy-preserving technique of using different e-mail addresses for different purposes (and protecting the "most real" address for only very well known personal friends or colleagues). This use of a single address would aggravate the problem noted above of an individual becoming a victim of a denial of service attack.

j. As the submission acknowledges, the verification afforded by AssertID would be far from bullet-proof, and thus would not be able to provide strong protection for users.

k. AssertID requires Internet users to validate each others' identities. It is unclear what incentive users will have to do this, and it would seem to be an onerous task for a web of users who already know and trust each other to have to validate every attribute of their friends' identities.

l. It seems likely that users with few friends (or users who prefer to "lurk" without making friends) would have a difficult time getting verified (or getting verified at a "high" level of confidence), thereby making their ability to access online services more difficult.

-- Policy Considerations: m. A governmental mandate to use this technology to block or screen users or communications would almost certainly violate the U.S. Constitution,

both by restricting users who AssertID cannot validate from communicating, and by destroying the constitutional right to communicate anonymously.

TAB Observer Comment Form

1. Submission: ChatSafe (The Carmichael Group, LLC/Carmichael)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: This proposal would make the process of "logging on" to a service so tedious that users would flee to other less onerous services, and it would require all minors to install and use webcams, which in turn would create additional risks for those minors who do not already use webcams to interact with others online.

-- Security/Privacy/Practical Considerations: a. Assuming for the sake of argument that users would use the ChatSafe system and it could discern whether User A on Day 2 was the same person who connected as User A on Day 1, the submission offers no explanation of how the video record of User A is to be connected to any actual real world information (such as the age or identity of User A). The ChatSafe system appears to assume that some company would aggregate sensitive personal information (including videos of minors). The transmission of sensitive information to third parties raises significant privacy and security concerns.

b. The ChatSafe system would create for many users around the world an insurmountable financial and technical hurdle for access to the Internet (the purchase, installation, and maintenance of a webcam), and would make it far less likely that users could access services through Internet cafes, libraries, etc.

c. Child safety experts warn parents AGAINST installing webcams for minors, noting that predators sometimes use webcams to contact minors, and minors sometimes use webcams to post inappropriate videos of themselves online. The ChatSafe proposal would REQUIRE webcams, thereby greatly exacerbating these risks.

d. Users who value the largely anonymous nature of most major social networking services will likely gravitate away from any service that requires authenticated video verification, as would users who appreciate the ease and convenience that online communications offer. It is highly implausible that the millions of social networking users (especially adult users) would put up with ChatSafe (and thus it is likely that both adults and minors would gravitate toward services that do not use ChatSafe).

e. Although the pricing structure is not stated, ChatSafe does not appear to offer any value for free, low cost, or non-profit communications services.

f. The submission appears to advance a range of different technologies that no company has today melded into a functioning product. Even if the abstract proposal were viable, the proposal in its current form does not seem fully baked.

-- Policy Considerations: g. A governmental mandate to use this technology to block or screen users or communications would almost certainly violate the U.S. Constitution, both by restricting users to who are unable to meet the technical requirements of ChatSafe from communicating, and by destroying the constitutional right to communicate anonymously.

TAB Observer Comment Form

1. Submission: Chatsafe (Crystal/Saunders/Crystal Reference Systems)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: The submission advances an interesting theory about how one might identify a conversation between a predator and a minor, but the proposal has not been tested or developed into a working product. If proven and developed, this proposal could be useful to a large, well-funded communications service provider.

-- Security/Privacy/Practical Considerations: a. Although the pricing structure is not stated, Chatsafe appears unlikely to offer value for free, low cost, or non-profit communications services.

-- Policy Considerations: b. A governmental mandate to use this technology to automatically block or screen communications would almost certainly violate the U.S. Constitution, by blocking the ability of Internet users to engage in lawful communications without prior legal process.

TAB Observer Comment Form

1. Submission: Checkmyage (Identity Corp./Gabriel)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: Given the burdens and costs imposed on end users, this proposal seems unlikely to be useful in the large social networking services that attract tens of millions of adults and minors, but the scheme might be useful for niche services that target the most concerned parents.

-- Security/Privacy/Practical Considerations: a. Users who value the largely anonymous nature of most major social networking services will likely gravitate away from any service that requires authenticated in-person verification, as would users who appreciate the ease and convenience of accessing online services without undergoing an external verification process. It is implausible that the millions of social networking users (especially adult users) would utilize Checkmyage (and thus it is likely that both adults and minors would gravitate toward services that do not use Checkmyage).

b. Checkmyage anticipates that it would create and maintain a centralized, authoritative database of minors. The privacy and security risks of this approach are significant (with hackers, predators, and marketers all seeking access to the data). The submission does not address the privacy and security of the database.

c. The proposed system appears to do nothing to prevent the sharing of credentials once a verification has been completed. Thus, the proposed system is less likely to be effective in contexts in which users have little incentive to maintain tight control of accounts they create – such as social networking and other mass-market (and often free) services that allow broad communications.

d. Even with an in-person visit to a notary, there is no reliable way to ensure that an adult who appears with a child is in fact the authorized legal guardian of the child.

e. As the submission acknowledges, the proposal would not be useful for online services that have significant numbers of non-U.S. users.

f. If a parent's access code is compromised, a child would be able to circumvent the system entirely and create additional authorized addresses and IDs (for themselves and for peers).

g. A check for notaries public in 10 zip codes (including major urban and suburban locations) on the checkmyage.com website did not return a single notary that participates in the system.

h. The system does not appear to be in operation, and thus cannot be validated or tested.

-- Policy Considerations: i. A governmental mandate to use this technology to block or screen users or communications would almost certainly violate the U.S. Constitution, both by restricting users who cannot afford Checkmyage from communicating, and by destroying the constitutional right to communicate anonymously.

TAB Observer Comment Form

1. Submission: ChoicePoint Authentication (ChoicePoint)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: Although not completely clear from the submission, this proposal appears to be aimed exclusively at restricting access by minors to "adults-only" products or services (such as alcohol, tobacco, etc.), and it may be useful in those contexts.

-- Security/Privacy/Practical Considerations: a. The submission does not use the term "social network," and it does not appear to be aimed at that context. Although the submission initially indicates that ChoicePoint technology can "prevent minors from accessing particular sites without parental consent," the remainder of the submission is silent on this point, and nothing described in the submission appears to be applicable to determining or enforcing parental consent.

b. The proposal appears to do nothing to prevent the sharing of credentials once a verification has been completed. The proposed system is thus unlikely to be effective in contexts in which users have little incentive to maintain tight control of accounts they create – such as social networking and other mass-market (and often free) services that allow broad communications.

c. Although the pricing structure is not stated, ChoicePoint does not appear to offer any value for free, low cost, or non-profit communications services.

d. Users who value the largely anonymous nature of most major social networking services will likely gravitate away from any service that requires authenticated verification.

-- Policy Considerations: e. A governmental mandate to use this technology to block or screen users or communications would almost certainly violate the U.S. Constitution, both by restricting users who ChoicePoint cannot validate from communicating, and by destroying the constitutional right to communicate anonymously.

f. Significant privacy and security concerns are raised by any large aggregation of personal data such as what ChoicePoint has assembled.

TAB Observer Comment Form

1. Submission: Covenant Eyes Accountability Software AND Covenant Eyes Filter Plus Accountability Software (Covenant Eyes, Inc./DeHaas)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: The submissions describe two related client-side "user empowerment" products that allow parents, employers, and users to monitor or block access to content on a given computer. Based on the assertions in the submissions, these products appear to offer parents and others useful tools for protecting minors online.

-- Security/Privacy/Practical Considerations: a. It is unclear whether the Covenant Eyes company receives and maintains the log information transmitted to the parents/ employers, but if so, significant privacy and security considerations are raised by that transmission and/or retention.

b. The effectiveness of this product can only be determined through hands-on testing. It is unclear whether this product operates only on Web communications or on all kinds of Internet communications.

-- Policy Considerations: c. Although "user empowerment" tools are often effective ways to protecting minors online, a governmental mandate to use this technology to block or screen communications would almost certainly violate the U.S. Constitution, because virtually all filters block access to constitutionally protected material.

TAB Observer Comment Form

1. Submission: DeepNines (DeepNines Technologies/Karimi)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: The proposed technology is aimed at allowing individual institutions (such as a company or a school) to exert significant control over all Internet usage within the institution. Based on the submission, the product may be useful in that context.

-- Security/Privacy/Practical Considerations: a. The product is aimed at a middle area that it not really the focus of the Task Force – it is neither aimed at individual parents seeking to protect children, nor broadly at social networks or online service providers.

b. The focus of the product is to entirely block access to specific sites or categories of services or sites. Thus, for example, the DeepNines Web site touts its ability to block all access to MySpace.com. Although blocking access to all social networking sites is something that individual institutions may choose to do, minors will likely find other ways to access such sites. Alternatively, minors may seek new social sites that have not yet made it to the DeepNines blocking list.

-- Policy Considerations: c. Although this type of "deep packet inspection" may be something an individual company or institution decides to use, a governmental mandate to use this technology to block or screen communications would almost certainly violate the U.S. Constitution, because access to constitutionally protected material would be blocked.

TAB Observer Comment Form

1. Submission: eGuardian (eGuardian, LLC)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: The eGuardian proposal appears to be a combination of login token creation system plus a set of APIs that social networks might build into their services (with an unclear requirement that service providers must create and provide a client-side eGuardian application). This appears to be a possible approach that could be used by niche social networks that seek high levels of security (but which do not aim at a broad, global user base).

-- Security/Privacy/Practical Considerations: a. It is appears that eGuardian may retain a significant amount of data about its users. Significant privacy and security concerns are raised by any aggregation of personal data.

b. The eGuardian system appears to do nothing to prevent the sharing of credentials once a verification has been completed. The proposed system appears unlikely to be effective where users have little incentive to maintain tight security of access.

c. The submission appears to require that social networks create client-side applications to enforce eGuardian verification. If so, this would introduce significant security vulnerabilities into already-fragile home computer contexts, and would significantly change the nature of online access.

d. Users who value the largely anonymous nature of most major social networking services will likely gravitate away from any service that requires the eGuardian system. Moreover, adults and minors will be deterred from any system that requires an installed application in the client computer (making access to a social network much more complicated).

e. The proposal seems highly unlikely to scale to be useful for a mass market communications service that focuses on a global audience.

-- Policy Considerations: f. A governmental mandate to use this technology to block or screen users or communications would almost certainly violate the U.S. Constitution,

both by restricting users who cannot use eGuardian because of a lack of availability from communicating, and by destroying the constitutional right to communicate anonymously.

TAB Observer Comment Form

1. Submission: EthoSafe (EthoSafe, Inc.)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: The EthoSafe product may have potential to be used by large, well-funded service providers for voluntary screening of user-generated content (UGC).

-- Security/Privacy/Practical Considerations: a. The transmission of all UGC to a third party for analysis raises potential privacy and security concerns.

b. As the submission acknowledges, automatic review of non-text content is not yet a robust technology.

c. In light of the pricing structure, EthoSafe does not appear to offer any value for free, low cost, or non-profit communications services.

-- Policy Considerations: d. Although this type of assisted UGC review may be useful for some service providers, a governmental mandate to use this technology to screen communications would raise significant concerns about harm to innovation and technology development, and a mandate to block communications would raise significant constitutional concerns.

TAB Observer Comment Form

1. Submission: Smart Cards (Gemalto, Inc./Pattinson)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: The submission describes a general-purpose technology that might be useful in online child safety applications and services.

-- Policy Considerations: a. A governmental mandate to use this technology would raise serious questions about technology innovation and the ability of other technologies to compete in the marketplace.

TAB Observer Comment Form

1. Submission: CQR-ID (GenMobi Technologies, Inc./Schultz)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: The submission does not disclose how CQR-ID verifies the identity of an adult, and thus this submission should not be further considered by the Task Force. The approach to verifying minors ages and identities could be useful for niche services that target the most concerned parents willing to undertake the school verification process proposed. The submission also does not provide sufficient detail with which to assess the claims made about filtering chat and reviewing images and videos for content concerns.

-- Security/Privacy/Practical Considerations: a. With the CQR-ID system, sensitive personal information is transmitted over the Internet, and the submission does not indicate how that information is protected while in transit over the Internet. The transmission of sensitive information to third parties raises significant privacy and security concerns.

b. CQR-ID would apparently create and maintain a centralized, authoritative database of information on minors and adults. The privacy and security risks of this approach are significant (and the database would be targeted by hackers, predators, and marketers).

c. The CQR-ID system appears to do nothing to prevent the sharing of credentials (including the answers to the PCQ questions) once a verification has been completed. The proposed system appears unlikely to be effective where users have little incentive to maintain tight security of access.

d. The submission provides no information on how an adult's identity is verified. Without this information, the Task Force cannot assess the submission.

e. The low likelihood that schools around the world would, as a practical matter, be able to participate in the CQR-ID system makes it unlikely that CQR-ID would be useful for a global service with international users.

f. The submission is silent on how "false negatives" are handled or whether someone rejected by CQR-ID has any recourse to challenge the determination.

g. Users who value the largely anonymous nature of most major social networking services will likely gravitate away from any service that requires authenticated verification.

h. The submission does not provide sufficient information with which to assess the chat filtering or content screening tools.

-- Policy Considerations: i. A governmental mandate to use this technology to block or screen users or communications would almost certainly violate the U.S. Constitution, both by restricting users who CQR-ID cannot validate from communicating, and by destroying the constitutional right to communicate anonymously. A mandate to use the filtering and screening capabilities also would run afoul of the Constitution.

TAB Observer Comment Form

1. Submission: icouldbe (icouldbe.org)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: The submission describes one example of an individual Web site using technology to limit unauthorized communications using the Web site. It does not appear to describe a single product or family of products available for use by other service providers.

-- Policy Considerations: a. A governmental mandate to use the technology as described in the submission would raise a host of constitutional and policy concerns.

TAB Observer Comment Form

1. Submission: IDology (IDology, Inc./Dancu)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: The IDology product may have potential to be used by large, well-funded service providers for voluntary screening of users to create a "walled garden" for adults, as well as by providers that sell "adult only" products or services and thus can recoup the cost of verification through IDology.

-- Security/Privacy/Practical Considerations: a. The transmission of sensitive information to third parties raises significant privacy and security concerns. It is unclear from the submission whether IDology retains the data it receives from a service provider. It is also unclear whether IDology itself aggregates and retains data from the "billions" of records it accesses. Significant privacy and security concerns are raised by any large aggregation of personal data.

b. The IDology system does nothing to prevent the sharing of credentials once a verification has been completed. The proposed system appears to be most useful in contexts where all parties want to keep identities secure (such as with gambling where losses are charged to a user's credit card), and less useful in social networking and other mass-market (and often free) services that allow broad communications.

c. Although the submission claims to give parents an ability to control their children's online access, there is no effective way to verify the relationship between two individuals who claim to be a parent and child.

d. IDology may not be useful for a global service with international users.

e. Given the pricing structure, IDology does not appear to offer any value for free, low cost, or non-profit communications services.

f. The submission is silent on how "false negatives" are handled or whether someone rejected by IDology has any recourse to challenge the determination.

g. Users who value the largely anonymous nature of most major social networking services will likely gravitate away from any service that requires authenticated verification.

h. The submission does not indicate what kinds of questions are used in the KBA system so that a knowledgeable child would not be able to impersonate his or her parents.

-- Policy Considerations: i. A governmental mandate to use this technology to block or screen users or communications would almost certainly violate the U.S. Constitution, both by restricting users who IDology cannot validate from communicating, and by destroying the constitutional right to communicate anonymously.

j. Broader societal concerns are raised by the ability of private companies to access the diversity of sensitive personal data used by this technology.

TAB Observer Comment Form

1. Submission: InfoGlide (Infoglide Software Corporation/Wood)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: The InfoGlide product may have potential to be used by large, well-funded service providers for voluntary screening of users against sex-offender lists and InfoGlide's proposed database of detailed information gathered from multiple social networks and other service providers.

-- Security/Privacy/Practical Considerations: a. InfoGlide anticipates that it would create and maintain a centralized, authoritative database of social networking users. The privacy and security risks of this approach are significant (and the database would be targeted by hackers, predators, and marketers).

b. The InfoGlide system appears to do nothing to prevent the sharing of credentials once a verification has been completed. Thus, the proposed system is less likely to be effective in contexts in which users have little incentive to maintain tight control of accounts they create – such as social networking and other mass-market (and often free) services that allow broad communications.

c. Users who value the largely anonymous nature of most major social networking services will likely gravitate away from any service that requires authenticated verification.

d. As InfoGlide acknowledges, there would be false-positive matches and people would be incorrectly excluded from online services as sex offenders. The TSA's Secure Flight program, which apparently is based on InfoGlide's services, has had significant false positive problems.

e. InfoGlide offers no explanation as to why online services would agree to turn over sensitive personal information about the services' customers to InfoGlide. The "similarity" searching that InfoGlide touts would require a critical mass of social networking sites as participants, and there is no indication of how InfoGlide expects to assemble such a critical mass.

f. Although the pricing structure is not stated, InfoGlide does not appear to offer any value for free, low cost, or non-profit communications services.

-- Policy Considerations: g. A governmental mandate to use this technology to block or screen users or communications would almost certainly violate the U.S. Constitution, both by restricting users who InfoGlide wrongly excludes from communicating, and by destroying the constitutional right to communicate anonymously.

TAB Observer Comment Form

1. Submission: Keibi Moderation Suite (Keibi Technologies, Inc.)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: The Keibi product may have potential to be used by large, well-funded service providers for voluntary screening of user-generated content (UGC).

-- Security/Privacy/Practical Considerations: a. Keibi appears to collect and retain at least some information about users, raising potential privacy and security concerns. In addition, the transmission of all UGC to a third party for analysis raises similar concerns.

b. The submission does not disclose details about HOW Keibi "automatically" identifies UGC that might violate Terms of Service. For example, Keibi presumably uses image recognition technology to screen images, but the submission does not disclose what types of technologies it uses.

c. In light of the pricing structure, Keibi does not appear to offer any value for free, low cost, or non-profit communications services.

-- Policy Considerations: d. Although this type assisted UGC review may be useful for some service providers, a governmental mandate to use this technology to screen communications would raise significant concerns about harm to innovation and technology development, and a mandate to block communications would raise significant constitutional concerns.

TAB Observer Comment Form

1. Submission: Kidsnet (Kidsnet)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: The submission describes a client-side "user empowerment" tool coupled with an external proxy service that allow parents (and employers and others) to filter a minor's access to the Internet through a Windows computer. Based on the assertions in the submission, this product appears to offer parents and others a useful tool for protecting minors online.

-- Security/Privacy/Practical Considerations: a. The effectiveness of this product can only be determined through hands-on testing. As the submission acknowledges, it only blocks Web traffic on port 80, and thus can likely be circumvented.

-- Policy Considerations: b. Although "user empowerment" tools are often effective ways of protecting minors online, a governmental mandate to use this technology to block or screen communications would almost certainly violate the U.S. Constitution, because virtually all filters block access to constitutionally protected material.

TAB Observer Comment Form

1. Submission: McGruff SafeGuard (McGruff SafeGuard/Spector)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: The submission lacks sufficient information on which to evaluate the proposed technology. Based on the company's Web site, the product is a client-side "user empowerment" tool that allow parents monitor the Internet usage of anyone using a particular computer. Based on the assertions on the Web site, this product appears to offer parents a useful tool for protecting minors online, albeit at an apparent cost of privacy of both the minor and anyone else using a covered computer.

-- Security/Privacy/Practical Considerations: a. It appears that the McGruff company receives and maintains a massive amount of information about all Internet communications to and from the target computer. Significant privacy and security considerations are raised by this data collection.

b. The effectiveness of this product can only be determined through hands-on testing. It is unclear whether this product operates only on Web communications or on all kinds of Internet communications.

c. The McGruff system takes a blacklist report from one McGruff user and applies it to all McGruff users. This appears to create opportunities for an effective denial of service attack in which one or more bullies could sign up for free McGruff accounts and then blacklist a bullying target, which would have the effect of blacklisting the target from all McGruff users.

d. The McGruff website FAQ indicates that the product is unable to monitor chat over the MySpace social networking system.

-- Policy Considerations: e. Although "user empowerment" tools are often effective ways of protecting minors online, a governmental mandate to use this technology to block or screen communications would almost certainly violate the U.S. Constitution, because the system would almost certainly interfere with computer users' rights to engage in constitutionally protected communications.

TAB Observer Comment Form

1. Submission: Information Card (Microsoft)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: The submission describes a general-purpose technology that might be useful in online child safety applications and services.

-- Policy Considerations: a. A governmental mandate to use this technology would raise serious questions about technology innovation and the ability of other technologies to compete in the marketplace.

TAB Observer Comment Form

1. Submission: NetIDme (NetIDme Ltd)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: The submission does not disclose how NetIDme verifies age or identity, and thus this submission should not be further considered by the Task Force. The submission appears to propose a token/passcard identity management system that unifies logins, coupled with a blackbox identity verification system. The submission also proposed a client-side tool, ChatShield, that appears to restrict the ability of users to chat with other users without prior approval.

-- Security/Privacy/Practical Considerations: a. The transmission of sensitive information to third parties raises very significant privacy and security concerns. It is unclear from the submission whether NetIDme retains the data it receives from users. Significant privacy and security concerns are raised by any large aggregation of personal data.

b. The NetIDme system appears to do nothing to prevent the sharing of credentials once a verification has been completed. The proposed system appears unlikely to be effective where users have little incentive to maintain tight security of access.

c. The submission provides no information on how minors' ages are verified. Without this information, the Task Force cannot assess the submission.

d. Without knowing how identification is done, the Task Force is unable to assess whether NetIDme could be useful for a global service with international users.

e. Based on the pricing scheme, it is unlikely that free, low cost, or non-profit communications services would be able to use the NetIDme system.

f. The submission is silent on how "false negatives" are handled or whether someone rejected by NetIDme has any recourse to challenge the determination.

g. Users who value the largely anonymous nature of most major social networking services will likely gravitate away from any service that requires authenticated verification.

-- Policy Considerations: h. A governmental mandate to use this technology to block or screen users or communications would almost certainly violate the U.S. Constitution, both by restricting users who NetIDme cannot validate from communicating, and by destroying the constitutional right to communicate anonymously.

TAB Observer Comment Form

1. Submission: Net Nanny (ContentWatch/Ferioli)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: The submission describes a robust suite of client-side "user empowerment" capabilities that allow parents (and employers and others) to monitor and control a minor's use of a computer and access to the Internet. Based on the assertions in the submission, this product appears to offer parents and others useful tools for protecting minors online.

-- Security/Privacy/Practical Considerations: a. It is unclear from the proposal whether NetNanny/Content Watch would receive and maintain the log and reporting information made available to the parents, which would raise significant privacy and security.

b. The effectiveness of this product can only be determined through hands-on testing.

-- Policy Considerations: c. Although "user empowerment" tools are often effective ways to protecting minors online, a governmental mandate to use this technology to block or screen communications would almost certainly violate the U.S. Constitution, because virtually all filters block access to constitutionally protected material, and this product would prevent other constitutionally protected uses of the Internet.

TAB Observer Comment Form

1. Submission: Portcard (Portcard, Inc.)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: The submission does not disclose anything about how the product verifies identity (including who the "partner" is or what data is used to "verify" identity), and thus this submission should not be further considered by the Task Force. The submission appears to propose a "single login" management system that unifies logins, coupled with a blackbox identity verification system.

-- Security/Privacy/Practical Considerations: a. The transmission of sensitive information to third parties – especially wholly unidentified and unknown third parties – raises very significant privacy and security concerns. It is unclear from the submission whether Portcard or the unidentified identity "partner" retains the data it receives from users. Significant privacy and security concerns are raised by any large aggregation of personal data.

b. The Portcard system does nothing to prevent the sharing of credentials once a verification has been completed. The proposed system appears unlikely to be effective where users have little incentive to maintain tight security of access.

c. Portcard allows an adult to create "verified" identities for minors, but there is no effective way to verify the relationship between two individuals who claim to be a parent and child. According to the Portcard website, "[o]nce a parent is registered, that parent can then register children so that the Portcard.net database will have information as to the age range of someone under 18." Thus, a verified adult could easily create identities for unrelated minors (and could possibly even sell or distribute such identities online).

d. As the submission acknowledges, Portcard may not be useful for a global service with international users because of an inability to verify identity internationally.

e. The submission is unclear on whether a free, low cost, or non-profit communications service would have to pay Portcard for users on the service to be "verified."

f. The submission is silent on how "false negatives" are handled or whether someone rejected by Portcard has any recourse to challenge the determination.

g. Users who value the largely anonymous nature of most major social networking services will likely gravitate away from any service that requires authenticated verification.

h. The submission does not provide sufficient information to suggest that a knowledgeable child would not be able to impersonate his or her parents.

-- Policy Considerations: i. A governmental mandate to use this technology to block or screen users or communications would almost certainly violate the U.S. Constitution, both by restricting users who Portcard cannot validate from communicating, and by destroying the constitutional right to communicate anonymously.

TAB Observer Comment Form

1. Submission: Privo-Parity (Privo/Parity/Tayloe/Trevithick)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: The submission does not disclose how Privo-Parity verifies identity of parents, and this portion of the submission should not be further considered by the Task Force. The bulk of the submission proposes an electronic Cardspace token to identify a minor when accessing a social network.

-- Security/Privacy/Practical Considerations: a. With the Privo-Parity system, sensitive personal information is transmitted over the Internet, and the submission does not indicate how that information is protected while in transit over the Internet. The transmission of sensitive information to third parties raises significant privacy and security concerns.

b. Privo-Parity would create and maintain a centralized, authoritative database of information on minors and adults. The privacy and security risks of this approach are significant (and the database would be targeted by hackers, predators, and marketers).

c. The Privo-Parity system does not prevent the sharing of credentials once a verification has been completed. The proposed system appears unlikely to be effective where users have little incentive to maintain tight security of access.

d. There is no effective way to verify the relationship between two individuals who claim to be a parent and child, opening the system to a range of attacks.

e. Without knowing how identification is done, the Task Force is unable to assess whether Privo-Parity could be useful for a global service with international users.

f. The submission is silent on how "false negatives" are handled or whether someone rejected by Privo-Parity has any recourse to challenge the determination.

g. Users who value the largely anonymous nature of most major social networking services will likely gravitate away from any service that requires authenticated verification.

h. Although the pricing structure is not stated, Privo-Parity does not appear to offer any value for free, low cost, or non-profit communications services. This is especially true because a service using the Privo-Parity system would have to rearchitect the service to work with Privo-Parity.

-- Policy Considerations: i. A governmental mandate to use this technology to block or screen users or communications would almost certainly violate the U.S. Constitution, both by restricting users who Privo-Parity cannot validate from communicating, and by destroying the constitutional right to communicate anonymously.

TAB Observer Comment Form

1. Submission: Protect My Child Registry (Privo/Tayloe)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: The submission does not disclose how PMCR verifies identity or how the registry would interact with service providers, and thus this submission should not be further considered by the Task Force.

-- Security/Privacy/Practical Considerations: a. With the PMCR system, sensitive personal information is transmitted over the Internet, and the submission does not indicate how that information is protected while in transit over the Internet. The transmission of sensitive information to third parties raises significant privacy and security concerns.

b. PMRC/Privo would create and maintain a centralized, authoritative database of information on minors and adults. The privacy and security risks of this approach are significant (and the database would be targeted by hackers, predators, and marketers).

c. The PMCR system appears to do nothing to prevent the sharing of credentials once a verification has been completed. The proposed system appears unlikely to be effective where users have little incentive to maintain tight security of access.

d. There is no effective way to verify the relationship between two individuals who claim to be a parent and child (as the submission implicitly acknowledges).

e. The submission provides conflicting information about how parents' identities are verified before they submit their child's personal information to the PMCR (it says that "verifiable parental identity" is leveraged but also that parental consent may be provided by email or SMS, both of which could easily be used by children posing as their parents).

f. More generally, the submission provides no information on how identity is verified. Without this information, the Task Force cannot assess the submission.

g. Without knowing how identification is done, the Task Force is unable to assess whether PMCR could be useful for a global service with international users.

h. The submission is silent on how "false negatives" are handled or whether someone rejected by PMCR has any recourse to challenge the determination.

i. Users who value the largely anonymous nature of most major social networking services will likely gravitate away from any service that requires authenticated verification.

-- Policy Considerations: j. A governmental mandate to use this technology to block or screen users or communications would almost certainly violate the U.S. Constitution, both by restricting users who PMCR cannot validate from communicating, and by destroying the constitutional right to communicate anonymously.

TAB Observer Comment Form

1. Submission: PureSight (PureSight Technologies Ltd./Azoulay)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: The submission describes a set of "user empowerment" tools that allow parents to block access to content and services on a particular Windows computer. Based on the assertions in the submission, these tools appear to be useful for parents looking to protect their children online.

-- Security/Privacy/Practical Considerations: a. It is unclear whether the PureSight company receives and maintains logs of users' online activities (the submission refers to "monitoring, reporting, and logging systems.") If so, significant privacy and security considerations are raised by the transmission and storage of such information.

b. The effectiveness of this product can only be determined through hands-on testing. The submission does not provide details about false positives (blocking of non-adult content) or the mechanisms in place to prevent minors from circumventing the PureSight software.

-- Policy Considerations: c. Although "user empowerment" tools are often effective ways of protecting minors online, a governmental mandate to use this technology to block or screen communications would almost certainly violate the U.S. Constitution, because virtually all filters block access to constitutionally protected material.

TAB Observer Comment Form

1. Submission: Red Star hs (Maloney)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: The Red Star hs proposal appears to be a combination of a user name/password (UN/PW) creation system plus a set of largely unexplained or articulated functions that social networks might build into their service. The submission lacks sufficient information for the Task Force to consider the second portion of this proposal. Focusing on the UN/PW proposal, this appears to be a possible approach that could be used by niche social networks that seek high levels of security (but which do not aim at a broad, global user base) – albeit an approach with some significant privacy concerns.

-- Security/Privacy/Practical Considerations: a. It appears that the user names that are created by the Red Star hs system contain the birth year and month of all users. This would seem to create dramatic privacy risks in that anytime a user communicated with anyone else, the fact that the user is a minor is exposed.

b. It is unclear from the submission whether Red Star hs retains any data it receives from users, and if so, for what purpose. Significant privacy and security concerns are raised by any aggregation of personal data.

c. The Red Star hs system appears to do nothing to prevent the sharing of credentials once a verification has been completed. The proposed system appears unlikely to be effective where users have little incentive to maintain tight security of access.

d. A major portion of the submission suggests functions that would have to be designed into the social networking service (such as a login time out feature), and the submission does not provide sufficient information about how Red Star hs would propose to inject those functions into existing social networking services.

e. The proposal seems highly unlikely to scale to be useful for a mass market communications service that focuses on a global audience.

f. Users who value the largely anonymous nature of most major social networking services will likely gravitate away from any service that requires the Red Star hs system.

-- Policy Considerations: g. A governmental mandate to use this technology to block or screen users or communications would almost certainly violate the U.S. Constitution, both by restricting users who cannot use Red Star hs because of a lack of availability from communicating, and by destroying the constitutional right to communicate anonymously.

TAB Observer Comment Form

1. Submission: RelyID (RelyID/Mangiacotti)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: The submission appears to propose the "back end" of an identity verification system, and only suggests possible "front end" approaches that online service providers might adopt to use the verification service. The submission lacks sufficient information for the Task Force to evaluate the suggested front end approaches. The "back end" RelyID product may have potential to be used by large, well-funded service providers for voluntary screening of users to create a "walled garden" for adults, as well as by providers that sell "adult only" products or services and thus can recoup the cost of verification through RelyID.

-- Security/Privacy/Practical Considerations: a. The transmission of sensitive information to third parties raises significant privacy and security concerns. It is unclear from the submission whether RelyID retains the data it receives from a service provider. It is also unclear whether RelyID itself aggregates and retains data from the records it accesses. Significant privacy and security concerns are raised by any large aggregation of personal data.

b. The RelyID system does not by itself do anything to prevent the sharing of credentials once a verification has been completed. The proposed system appears to be most useful in contexts where all parties want to keep identities secure (such as with gambling where losses are charged to a user's credit card), and less useful in social networking and other mass-market (and often free) services that allow broad communications.

c. As the submission acknowledges, the use of criminal background checks is less useful for verifying information about minors.

d. RelyID may not be useful for a global service with international users.

e. Given the pricing structure, RelyID does not appear to offer any value for free, low cost, or non-profit communications services.

f. The submission is silent on how "false negatives" are handled or whether someone rejected by RelyID has any recourse to challenge the determination.

g. Users who value the largely anonymous nature of most major social networking services will likely gravitate away from any service that requires authenticated verification.

h. The submission does not indicate what kinds of questions are used in the RelyID system so that a knowledgeable child would not be able to impersonate his or her parents.

-- Policy Considerations: i. A governmental mandate to use this technology to block or screen users or communications would almost certainly violate the U.S. Constitution, both by restricting users who RelyID cannot validate from communicating, and by destroying the constitutional right to communicate anonymously.

j. Broader societal concerns are raised by the ability of private companies to access the diversity of sensitive personal data used by this technology.

TAB Observer Comment Form

1. Submission: Safe Eyes (InternetSafety.com)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: The submission describes a robust suite of client-side "user empowerment" capabilities that allow parents (and employers and others) to monitor and control a minor's use of a computer and access to the Internet. Based on the assertions in the submission, this product appears to offer parents and others useful tools for protecting minors online.

-- Security/Privacy/Practical Considerations: a. It is unclear whether the Safe Eyes company receives and maintains the information transmitted to the parents, but if so, significant privacy and security considerations are raised by that transmission and/or retention.

b. The effectiveness of this product can only be determined through hands-on testing.

-- Policy Considerations: c. Although "user empowerment" tools are often effective ways of protecting minors online, a governmental mandate to use this technology to block or screen communications would almost certainly violate the U.S. Constitution, because virtually all filters block access to constitutionally protected material, and this product would prevent other constitutionally protected uses of the Internet.

TAB Observer Comment Form

1. Submission: SaferSpace (Zemerick Software, Inc.)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: The submission describes client-side "user empowerment" capabilities that allow parents (and employers and others) to configure a Windows computer to block access to specified social networks such as MySpace.com. Based on the assertions in the submission, this product appears to offer parents and others a useful tools for preventing minors from accessing a particular Web site.

-- Security/Privacy/Practical Considerations: a. This system, if effective, would certainly push minors to use lesser known (and perhaps less responsible) social networking sites.

b. The effectiveness of this product, and the ability to withstand circumvention, can only be determined through hands-on testing.

c. By blocking any browser window that contains the text "MySpace" or "myspace.com," this product would lead to significant amount of overblocking (including the blocking of almost all child-safety Web sites, including sites intended to educate minors about online safety).

-- Policy Considerations: d. Although "user empowerment" tools are often effective ways of protecting minors online, a governmental mandate to use this technology would almost certainly violate the U.S. Constitution, because it unavoidably leads to overblocking of lawful content and in any event access to MySpace cannot be constitutionally blocked in its entirety.

TAB Observer Comment Form

1. Submission: Sentinel ADAPT (Sentinel Tech Holding Corp/Hamel)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: The submission describes a forensic technique to "fingerprint" a computer by creating a profile of data obtained from the computer's browser. Although this product may be useful in a law enforcement context, the submission is proposing that the product be used in child safety contexts.

-- Security/Privacy/Practical Considerations: a. The system appears to collect IP addresses (which are often considered "personally identifiable") and other potentially personally identifiable information, and thus raises privacy concerns.

b. The system would seem to undermine a growing security trend within browsers to limit the unrestricted use of Java and other scripts sent from Web sites.

c. Although many minors may not be savvy enough to alter parameters within the browser so as to throw off the ADAPT system, more experienced users seem likely to be able to do so. It further seems likely that if ADAPT is widely deployed on popular social networking services, utilities will become available on the Internet that allow users to spoof ADAPT fingerprints (or at least randomly alter enough of the elements used by ADAPT to defeat the system).

d. Although the pricing structure is not stated, ADAPT does not appear to offer any value for free, low cost, or non-profit communications services.

-- Policy Considerations: e. Any use of this technology by a government must be pursuant to court order or other lawful process, and any government mandate that private entities use this technology raises a host of constitutional and policy concerns.

TAB Observer Comment Form

1. Submission: Sentinel SAFE (Sentinel Tech Holding Corp/Hamel)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: This submission may provide options for large well-funded online services that seek to create child-safe environments.

-- Security/Privacy/Practical Considerations: a. The submission provides no information about the frequency of false positives, nor does it provide sufficient detail of any process to correct false positives.

b. As the submission acknowledges, Sentinel SAFE is claimed to be effective only for sites restricted to U.S. users.

c. Although no pricing information is provided, Sentinel SAFE does not appear to offer any value for free, low cost, or non-profit communications services.

-- Policy Considerations: d. A governmental mandate to use this technology to block or screen users or communications would almost certainly violate the U.S. Constitution, both by restricting the ability of certain users to utilize Internet services and by destroying the constitutional right to communicate anonymously.

TAB Observer Comment Form

1. Submission: Spector/eBlaster (SpectorSoft Corporation/Tate)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: The submission describe a client-side "user empowerment" product that allows parents, employers, and users to monitor access to Internet content on a given computer. Based on the assertions in the submission, this product appears to offer parents and others useful tools for protecting minors online.

-- Security/Privacy/Practical Considerations: a. It is unclear whether the SpectorSoft company receives and maintains the log information transmitted to the parents/ employers, but if so, significant privacy and security considerations are raised by that transmission and/or retention.

b. The effectiveness of this product can only be determined through hands-on testing.

-- Policy Considerations: c. Although "user empowerment" tools are often effective ways of protecting minors online, a governmental mandate to use this technology to block communications would raise serious questions about technology innovation and parents' choices.

TAB Observer Comment Form

1. Submission: Symantec Family Safety (Symantec Corporation)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: The submission describes a robust suite of client-side "user empowerment" capabilities that allow parents (and employers and others) to monitor and control a minor's use of a computer and access to the Internet. Based on the assertions in the submission, this product appears to offer parents and others useful tools for protecting minors online.

-- Security/Privacy/Practical Considerations: a. Under the proposal, Symantec appears to receive and maintain the log information transmitted to the parents, which raises significant privacy and security concerns.

b. The effectiveness of this product can only be determined through hands-on testing.

-- Policy Considerations: c. Although "user empowerment" tools are often effective ways of protecting minors online, a governmental mandate to use this technology to block or screen communications would almost certainly violate the U.S. Constitution, because virtually all filters block access to constitutionally protected material, and this product would prevent other constitutionally protected uses of the Internet.

TAB Observer Comment Form

1. Submission: VerificAge (VerificAge)

2. Commenter: John Morris, General Counsel, Center for Democracy & Technology (CDT), 1634 I Street, NW, Suite 1100, Washington, DC 20006, jmorris@cdt.org

3. Affiliations/Interests: I am a member of the Task Force and a TAB Observer. CDT is a not-for-profit civil liberties organization dedicated to promoting democratic values and constitutional liberties in the digital age. We strongly believe in online child safety and we actively promote voluntary parental empowerment, but we also believe that many child safety proposals raise serious privacy, policy and other concerns.

4. Comments: By requiring the use of a hardware device to do a bone density screening prior to online access, this proposal would radically change how users relate to the Internet, and would certainly drive users – adult and minors – to other services that do not use a bone density scanner.

-- Security/Privacy/Practical Considerations: a. Users who appreciate the ease and convenience that online communications offer will likely gravitate away from any service that requires bone density scanning. It is implausible that the millions of social networking users (especially adult users) would put up with VerificAge (and thus it is likely that both adults and minors would gravitate toward services that do not use VerificAge).

b. The VerificAge system would create for many users around the world a financial and technical hurdle for access to the Internet (the purchase, installation, and maintenance of a bone density scanner), and would make it far less likely that users could access services through Internet cafes, libraries, etc.

c. This product was introduced in 2004 under the name of "i-Mature" but does not appear to have been implemented. The product appears to be useful (assuming it works) only for the creation of "walled gardens" for minors under 14 years old.

-- Policy Considerations: d. A governmental mandate to use this technology to block or screen users or communications would almost certainly violate the U.S. Constitution, by restricting users who are unable to meet the technical requirements of VerificAge from communicating, and because of false positives or negatives.