Internet Safety Technical Task Force
Technology Submission

Privacy Vaults Online, Inc. d/b/a Privo
Denise Tayloe, President & CEO
http://www.privo.com

ABSTRACT
User generated content, social networks and anonymity without accountability pose significant challenges to protect minors online. Privo currently delivers to industry its leading identity and permission management solutions via its PrivoLock™ platform, using the MyPrivo™ customizable web-based interface and the PrivoDirect™ web services to access the Privo platform. Today, parents manage their children's online access with PrivoLock. The PrivoCard™ iCard technology and the Protect My Child Registry™ (PMCR) are two additional tools for parents, children and businesses to use to operate safely online. Building on Privo's experience, we use the same security, encryption, and scalability designs used in our other services for the PMCR. This proposal focuses on the PMCR.

Keywords
youth and adult identity verification and management, parental controls, COPPA, risk mitigation, auditable third party

Functional Goals
The functional goals of the submitted technology are:
- ☑ Limit harmful contact between adults and minors
- ☐ Limit harmful contact between minors
- ☑ Limit/prevent minors from accessing inappropriate content on the Internet
- ☐ Limit/prevent minors from creating inappropriate content on the Internet
- ☐ Limit the availability of illegal content on the Internet
- ☑ Prevent minors from accessing particular sites without parental consent
- ☐ Prevent harassment, unwanted solicitation, and bullying of minors on the Internet
- ☑ Other – Provide educational outreach to parents and minors who use the PMCR.

PROBLEM INTRODUCTION
In July 2006, the Federal Trade Commission (FTC) shared with Congress its concern about potential danger to children who visit social networking Web sites. In testimony before the House Committee on Energy and Commerce Subcommittee on Oversight and Investigation, FTC Commissioner Pamela Jones Harbour said there is a "need for social networking Web sites -- individually, collectively, and, most importantly, expeditiously -- to develop and implement safety features to protect children who visit their sites and empower parents to protect their children when they do so." "Because the information that children post on their online journals, web logs or 'blogs' can be accessed by other Internet users, social networking Web sites raise heightened privacy and security concerns. In particular, sexual predators may use the information that children provide on social networking sites to identify, contact, and exploit them, unless these sites are constructed to reduce access to this information, or users themselves take steps to limit unwanted access." "The social networking industry has a clear incentive to create a safe online community," Harbour said.

There are a variety of reasons a business might need to restrict children from certain web content, advertising and outbound marketing communication: company-imposed restrictions based on terms of use; parent restricted by overriding a company's terms of use; or imposed through regulatory requirements.

While there is no absolute solution to these problems, it is possible to give parents powerful new tools to protect their children online. There will always be a few children who manage to defeat age restrictions. Likewise, those who mean to harm children may find ways to defeat those same protections. However, the Protect My Child Registry will provide significant protection for a broad age range of children, by giving parents a mechanism to provide age information to web sites that may be inappropriate for children. Businesses have the social and legal, in the case of Children's Online Privacy Protection Act (COPPA), obligation to acknowledge and use access to this information responsibly. Accordingly there should be an ongoing vigilance by businesses and parents to provide tools to filter out adult and minor attempts to circumvent protective barriers.

In order to provide a safe social networking environment for kids, boundaries between adults and minors are necessary. Therefore, age verification seems to be the obvious answer to the problem. However, this approach is technically difficult, if not impossible, to implement effectively, is cost-prohibitive, and places an unrealistic burden on consumers and businesses.

PROPOSED SOLUTION
As a neutral third-party, Privo, which has been granted Safe Harbor status under COPPA, and its industry leading partner propose to offer an interoperable Protect My Child

Registry that would allow parents to have a voice in whether their children can participate in online environments that pose a perceived potential risk.

The PMCR has been designed to address the industry-wide privacy issue of controlling access to personal information and content for multiple age groups, including the U13 segment that is specifically addressed by COPPA. In its simplest form, the PMCR will provide a secure, scalable, and cost sensitive solution which allows a parent or guardian to put organizations (subscribing or non-subscribing) on notice of the need to protect or turn away from registration PII associated with a minor child.

The PMCR is designed to allow parents to manage their children's access to age restricted products and services whether the age restriction is company imposed through terms of use, parent restricted by overriding a company's terms of use, or imposed through regulatory requirements. The PMCR will act as an agent on behalf of the parent and child subscriber to notify companies of the age associated with, at minimum, the child's registered email address(es). Notice will take place for non-subscribing companies through paper or secure electronic means. Subscribing members could potentially have at least three ways to use the service: 1) ping real time subscriber registrations against the PMCR on an as needed basis, 2) batch process (past or ongoing registrants), or 3) with a push method to be processed by the subscribing client within their own operating environment. Given the sensitivity of the information being stored, the PMCR will take extreme precautions in protecting the integrity of the data, leveraging partners as needed to create a world-class secure environment.

The registration process will be executed in such as a way as to minimize someone fraudulently registering an adult without their consent. The person creating the registration will have to demonstrate control of the email address being registered as belonging to a child. Combative child and conflicting parent approval situations will require parents to participate in the verification process to override and mitigate the need for U18 opt in. The PMCR will retain its integrity through a sliding scale approach for the need to verify data.

To establish the PMCR as a flexible and evolving infrastructure for the benefit of all constituents will require: governance structure for direction; definition of the terms of use; rules of conduct; enforcement protocols; arbitration policies, procedures and support; verification methodology; service level agreements; data security and integrity design and maintenance; customer service infrastructure; quality assurance; monitoring, metrics, billing and general operational support. Building on our combined experience, we will use the same security, encryption, and scalability designs used in our other services.

Privo already delivers identity and permission management solutions to companies, parents and children under COPPA. The unique suite of solutions enables client companies to reasonably verify and authenticate the digital identity of their consumers. Companies can use Privo's proprietary solutions to enable them to build legally compliant and socially responsible online relationships with young consumers. Parents can use Privo to manage their children's personal information, so that they understand, permit and agree to the online relationships which are appropriate for their children. Children can safely interact online with other kids and the brands they love with a Privo approved identity.

Many of these PrivoLock™ features will be leveraged to maximize the effectiveness of the PMCR, including:

- Full service registration and permissioning infrastructure
- Verifiable parental identity and consent credentials
- Audit trail maintained
- Security and integrity of data
- Delivery of parental notice and privacy practices
- Parental account management to view, edit and delete data collected and establish premissions
- Customer service and support of parent inquires

Current consent methods include:

- Online: email, SMS, driver's license, partial SSN, credit card
- Offline: print and fax or outbound mail to address with PIN, toll-free phone number

The PMCR solution proposed proposed in this document is fully responsive to the recent "Joint Statement on Key Principles of Networking Sites Safety" which requires the establishment of a children's email registry.

In Addition to the Above Description, Please Address Each of the Following:

- Describe the solution's technical attributes, e.g. features and functionality.

  The PMCR would work as follows:

  - Parents create their own personal parental account which allows them to provide the PMCR with their children's personally identifiable information (which could include the child's full name, home address, birth date, email address, instant message handle, SMS cell phone contact, school name, personal website URL, etc.). This data is stored on secure servers and is not accessible to the outside world.

- Participating age restricted websites and social networks (in a self-regulating mode) would agree to "ping" each registration attempt against the PMCR. The registry analyzes in real time each attempted registration and cross-references for matches against the various fields in the database. When an "at risk registration" is identified by the registry, the registry returns to the participating site the associated age attribute, and if applicable the requested parental override. The participating site would use that information to invoke its terms of use and its regulatory requirements (e.g. COPPA requires parental consent for U13 participation). If necessary the site would temporarily suspend the registration and notify the PMCR. The PMCR would then alert the parent and provide at least two choices:
  - The parent can agree to the registration and provide parental consent through the PrivoLock™ system.
  - The parent can block the attempted registration and the participating site denies the registrant access.

- Provide use cases.

  Privo currently provides services to: an international family oriented film studio; an international restaurant chain; an international game publisher; an international entertainment standards board; a professional sports franchise; not for profit organizations; a virtual worlds provider; an international dress up doll site; tween/teen girl's blogging site; youth only social network; and general audience sports social network. These are representative of our customer base.

- Specify what the technology successfully solves and what it does not. Describe how the technology's effectiveness is evaluated, measured, and tested.

  The PMCR can only protect the information provided. It enables parents to monitor and maintain reasonable control of their child's personal information. It allows the parent to provide actual knowledge of their child's age so that subscribing and non-subscribing companies can be held accountable and mitigate the risk associated with rampant age falsification.

  It enables advertising networks to deliver age appropriate ads within the confines of social pressure and applicable regulations and laws.

  It enables a scrubbing mechanism to age restricted companies, thereby reducing inappropriate delivery of content and marketing materials.

- Provide a strengths-weaknesses analysis.

  This societal issue is not solved by Privo or any other child protection company. There is no one solution that will solve all issues associated with the need for online child protection. The PMCR is only one of many needed solutions. But, it requires participation by busy parents, vulnerable children, and ROI driven businesses. There already exists U.S. and international legislation that mandates compliance and innovation to create safer online environments.

  Some of the most beneficial features of the PMCR are the information dissemination and education capabilities which provide a vehicle to engage in public service announcements and distribute free parental monitoring software.

- Detail the implementation requirements and technical standards used.

  For the end consumer a standard computer with internet access via a web browser and an email account will be the only necessary tool to participate in the PMCR. Also, cell phone with SMS capabilities may be needed. A payment method may be required.

  For businesses there should be minimal implementation requirements for additional hardware or software licensing. The PMCR is comprised of several integrated, web-based components that are designed to operate in concert to deliver a secure, scalable and service-oriented architecture that satisfies the most rigorous requirements of businesses, consumers and the regulatory authorities. The technology platform leverages industry standard, component-based models and application design patterns. The PMCR architecture is based on industry standards, eliminating vendor or technology "lock-in".

  The current implementation methods and design details for the PMCR are not available for disclosure in this document since the Task Force includes direct competitors. Further disclosure of technical details may be presented to the appropriate non-competing Task Force members and advisers.

- Discuss the technology's reliance and use of law and policy for success.

  Companies are required to comply with COPPA if they are directed to children or general audience sites that receive actual knowledge that they are dealing with children under the age of 13. The PMCR will provide, on behalf of the parent, actual knowledge to those companies which need to protect a U13's PII.

Currently COPPA limits its protection to U13 minors. Discussions are ongoing to consider raising the protected age as it relates to sharing and public disclosure of data.

- Discuss the viability of the technology in both the US and international context.

  Privo and its partners have developed a set of capabilities that are not encumbered by its technology implementation or by focusing only on a subset of markets. We view the available markets as segments of age gated online content with a set of configurable services to validate identity and credentials. The systems have been designed to these criteria. Therefore, as the market drivers and opportunities demand the provision of services beyond the U.S. environment and its requirements, the underlying technology is flexible to address those needs. Privo's customer base is already requiring support for international markets.

EXPERTISE

Privo has been consulting on children's privacy and online best practices, providing Safe Harbor certification, designing, implementing and delivering identity and permission management in the children's space for over five years. We have been a pioneer in the industry and have expertise, relationships and a knowledge base that makes us the leading company in this market space. We have technology partners in development, security and operations that enable Privo to maintain its leading edge status. As we have expanded into new markets and technologies Privo has developed new partnerships and alliances that enable us to continue to grow faster and smarter.

COMPANY OVERVIEW

Privo, founded in 2001, is a privately held corporation based in Northern Virginia servicing Fortune 1000 companies and nonprofits in their efforts to comply with existing federal children's privacy legislation and social or legal pressure to obtain parental consent. Denise Tayloe is a founder and the CEO of Privo. The company was established to enable websites to comply with the Children's Online Privacy Protection Act (COPPA) when websites interact with and market to children online (including mobile communications) under the age of 13 ("U13"). Privo's proprietary digital identity and permission management software, PrivoLock™, includes a suite of software and service tools designed to enable companies to efficiently and inexpensively meet the COPPA requirements by in part managing the COPPA-required "verifiable parental permission" process for client companies. Privo intends to leverage its software to enable client companies to verify the digital identity of a broader range of consumers making online decisions concerning access to products and services.

BUSINESS MODEL OVERVIEW

In order to drive adoption and help address the broader social imperatives, the PMCR will offer basic free services for both consumers and businesses. However, both consumers and businesses would be asked to pay for premium services. For businesses the pricing structure envisions a minimum entry fee and a minimum annual subscription fee based on anticipated and actual volume. A transaction model is also comtemplated.

The pricing approach tries to ensure that the ongoing cost for the enhanced services to constituents is not prohibitive. The need for a third party infrastructure play sets the stage for a network effect, which produces economies of scale and widespread adoption. The basic business services are targeted to be cost liquidating; the profit model will be driven mainly by the value added services. Opportunities for sponsors are also contemplated.

CONTACT INFORMATION

Denise Tayloe –President & CEO
Privo
8229 Boone Boulevard
Suite 410
Vienna, VA 22182
Phone: (703.932.4979)
Email: dtayloe@privo.com
http://www.privo.com

CERTIFICATION

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