

Trustworthy Computing

Digital Playgrounds: Creating Safer Online Environments for Children

Microsoft Corporation 2008

When it comes to children's safety online, no technological silver bullet can completely eliminate risk. Indeed, the most important element of online safety for kids is parental supervision and guidance. However, the technology industry can offer better tools for keeping children safer online. Microsoft is proposing an approach whereby online service providers can create safer children-only online communities that use age verification based on digital versions of existing offline identity documents.

Online communities and social interaction are facilitated by innovative technology, including computers and software, Internet servers and open protocols. But ultimately, the nature of online communities is determined in much the same way as in the offline world—by the rules that govern them, how well those rules are enforced and the extent to which those rules are respected. Rules that unduly restrict activity or that are impractical to follow tend to be ignored, while rules that reflect broadly-shared community values require less effort to enforce.

Parental supervision and guidance will always be the most important factor in online safety for kids. Governments, industry and children's advocacy groups offer various kinds of support to parents in this effort. This support includes guidance on how to talk to kids about appropriate online behavior, educational materials for children, and technological tools, including tools that allow parents to limit certain kinds of Internet use or monitor children's online activities. While no technology can completely eliminate risk, Microsoft is proposing an approach that will further improve online safety for children by allowing online service providers to create safer children-only online experiences. The specific rules would be up to the provider, but the approach involves age verification following a reasonably practical and enforceable set of general rules.

We believe that age verification for general-audience Web sites should not be legally imposed—for practical reasons as well as reasons related to privacy, cost and the likely low return in terms of improved safety. However, age verification skeptics might be missing an opportunity to create new choices for consumers. We believe that age verification has potential as one of many optional tools that industry and government can employ to lower online risks because it can help maintain a separation between the interactive online

experiences of children and those of adults. In general, interactive Web sites and services can be categorized as follows:

- Children only (or children and identified adults)
- General audience
- Adults Only

We will focus here on the first category, children-only Web sites and services. Adults-only sites typically have their own technologies for screening out underage users—technologies that, for reasons described below, are impractical for children-only Web sites or general-audience Web sites (which should remain open to all users).¹

To create a children-only service, providers must determine the user's real age and trust the person or entity vouching for that information. Unfortunately, **most experiences on the Web are fairly anonymous and identity attributes are hard to verify**, so it is difficult to determine whether to trust assertions about age or other user attributes. Reputation services on sites such as eBay try to establish the trustworthiness of their users by allowing them to build a reputation over time based on usage. This type of service can be very effective in establishing a level of trust for use in transactions brokered by an auction site. However, to create a deeper level of trust requiring the validation of age claims, we must look to more robust forms of verification.

Adults-only Web sites tend to verify age by collecting personal information and testing it against publicly available databases (such as those containing government ID numbers or credit histories). But in most countries, no online databases can validate with a high degree of confidence a claim about a child's age or about a parent-child relationship. (Even where such databases exist, privacy challenges notwithstanding, only an offline process could verify that the person claiming to have a particular online ID number is indeed that person rather than someone who has appropriated the ID number.) In the absence of these resources, and in light of the privacy and verification issues associated with purely online authentication, we must look to forms of verification from the offline world to manage challenges relating to online identity and trust. In this way, we can enable online service providers to create robust services that afford a higher level of confidence that the users are indeed children.

Offline Claims Applied to the Online World

Offline, we establish trustworthy identity assertions in many ways. Indeed, the identity information we use in sensitive situations—such as name, driver's license number or government ID number—is generally based on previous verification when we were physically present. For example, hospitals issue birth certificates based on eyewitness evidence of a newborn's entry into the world. Later, we might use that birth certificate to get a driver's license or a passport from a government agency. We might then use this other document to open a bank account or register a child for school. These verification procedures in the offline world are often based on both social custom and law.

It turns out that the best way to establish trust online might be to make use of the trust mechanisms that already exist offline. To establish a high level of assurance for online interactions or transactions, we should

¹ As a policy matter, we believe that the choice of target audience for a Web site or service should be left to the service provider, not imposed by law.

create digital versions of existing trusted identity documents and allow people to use them when proof of identity is needed online.

The use of such documents will make it possible to create safer children-only Web sites and online services. Children (and perhaps certain adults) who have a digital identity document with a trusted age claim could use it to access children-only digital playgrounds, class forums, social networking sites or other types of online interaction. People without such appropriate digital identities would be barred.

In many countries, children don't carry the kinds of offline identity documents found in the typical adult's wallet. So how would these documents be issued, and who would be authorized to make identity claims for children? Again, we can take advantage of existing offline processes where secure in-person identity verification already occurs—for example, at the time a national identity card or passport is issued, or when a child is being registered for school.

In countries where children are issued robust national identity documents from birth (such as some countries in Europe), corresponding digital versions would be the obvious choice for online verification. In other countries (such as the U.S.), schools would be well-positioned to issue identity documents because they have an existing process to determine a child's age and identity at the time of school registration. Alternatively, government offices could issue these digital identities in the same way that they issue non-driver IDs or passports. In some countries, the post office would be another good option. Private-sector entities could even be used to issue claims, given some assurance of accreditation and security protections.

We recommend that the decision about whether a child should be issued a digital identity card be left up to the parents. Parental demand for the creation and issuance of these digital identities would, in turn, drive Web site operators to create children-only Web sites and services where such identities would be used.

To protect privacy, the data on these digital identities could be limited to age and proof of authenticity. No personal data would need to be embedded in the card, and no personal data known to the school (or other identity provider) would need to be released onto the Internet. If a country does issue digital identity cards that include personal information, online service providers should set their systems to request only a verified confirmation of age (rather than the full set of information on a given card). Decisions regarding what data to include in a digital identity would ultimately be policy decisions made collaboratively by government, privacy advocates, industry, and child development experts.

Digital environments restricted to age-verified children **would not be without risks**. Indeed, the overall approach described here focuses on risk reduction and mitigation, not on risk elimination. Any community is safe only to the extent that rules are in place and are respected by the participants. Individual behavior, such as cyberbullying, would still need to be addressed, education would still be needed to promote online etiquette, and enforcement by online community hosts would still be crucial.

As noted earlier, technology cannot provide a silver bullet for online safety, and a solution based on such identity documents would of course not be foolproof. Identity providers would have to take steps to limit who could obtain a digital identity. As in the offline world, credentials might be issued based on clever misrepresentations to the provider. To minimize such risks, identity providers would have to be properly trained and accredited.

Another challenge is managing issues related to lost, stolen or borrowed identity cards. From time to time, identity cards might be lost, stolen, sold or borrowed—much like in the offline world. Each individual would ultimately bear the responsibility to safeguard his or her own digital identity, and children would need to be taught to secure their identities. However, if a digital identity card were to fall into the wrong hands, the relevant and properly authorized authorities would need to have processes in place (with appropriate restrictions) to swiftly obtain information about both the card’s improper use and the identity of the original card holder. This would allow law enforcement to narrow the suspect pool and quickly commence more effective investigations. Additional steps should also be taken to minimize the risk that digital identities could be easily used if they fall into the wrong hands. Such steps should recognize that digital identities need far more security protections than a simple username and password, which are easily compromised. Digital identity documents should include PIN numbers and should be cryptographically secure, auditable and revocable in the event of compromise. The specific devices or IP addresses that a given identity could be used from could also be restricted. Digital identity documents should work with existing identity systems and be interoperable between providers.

These realities suggest that the objective should be to bring online and offline safety into parity so parents and children can expect a similar level of safety and privacy protection in both environments—not to seek perfect enforcement in the online world (which is unachievable) or create false expectations of security. Indeed, we still teach children not to talk to strangers in the offline world; even in a safer online world, children would still need to be educated about the risks to their privacy and safety.

An Approach Based on Information Card Technology

Much of the basic technology required for the creation of digital “identity cards”—technology known as an Information Card² system—already exists. It represents a significant improvement in authentication security and interoperability across all types of government, enterprise and consumer networks.

Information Cards are not physical cards—they are digital identities analogous to tangible cards in a person’s wallet. In much the same way that a person might use a student ID card to get free admission to a museum or demonstrate eligibility to purchase discounted train tickets, a digital Information Card issued by one entity can be used to verify the card owner’s identity or identity attribute (such as age) with another entity, as long as the card includes the necessary data.

The creation and use of Information Cards involves three parties. The first party is the entity that issues the card. In the case of a card for use in sensitive interactions, the issuer might be a government, business or nonprofit organization. For less sensitive uses, individuals might issue themselves a card. The second party, or relying party, is whoever needs to accept the card during a transaction. The third party is the cardholder, who decides which card to present in a given transaction. In some cases, there might also be an additional

² Microsoft is a provider of Information Card technology; our implementation is called [Windows CardSpace™](#). All of the protocols for Information Cards are under the Microsoft [Open Specification Promise](#), so anyone is free to build software that uses or issues Information Cards. Others have already begun to do so for the Mac, Linux and Windows® platforms. (Examples include [DigitalMe](#) and [Higgins](#).)

To further advance the interoperability and adoption of this technology, Microsoft and other prominent companies recently formed the nonprofit [Information Card Foundation](#). The 35 members of this foundation—including Equifax, Google, Novell, Oracle and PayPal—share Microsoft’s commitment to fostering a simpler, more secure and more open digital identity system on the Internet, increasing users’ control over their personal information and enabling mutually beneficial digital relationships between people and businesses.

entity providing the secure in-person proofing element of the card issuance process so that the card issuer can issue cards with the requisite degree of confidence.

Information Card technology removes the need to rely on usernames and passwords to access Web sites, and it supports a range of robust encryption methods that help prevent tampering with the card's data or intercepting it in transit. Information Cards also allow relying parties to request the minimum amount of personal information needed to authenticate an identity for a given transaction. For example, an Information Card issued by a civic organization might have six fields—for name, address, birth date, member number and so on—but if a relying party, such as an e-commerce Web site offering discounts to members of the organization, needs only two fields of information to complete a transaction (such as “Does the card certify that the holder is a member of the organization?” and “Is the digital identity itself valid?”), that party will receive only those two fields of information.

From an infrastructure perspective, this system will require a number of investments. First, identity providers (such as government agencies or schools) will need the resources to issue the digital identities. Relying parties (such as children-only Web sites) must modify their systems to accept these kinds of digital identities. Finally, children must be taught how to use digital identity cards and must be given incentives to do so.

Incentives

As with many aspects of the online world, the availability of a particular technology or service does not necessarily mean that the market will embrace it. Some of the calls for age verification have focused on general-audience social networking services because they are perceived to be the most popular among both teens and adults. Some attempts at creating children-only online experiences have proven less attractive to the marketplace. The .kids.us domain, for example, has not gained a critical mass of users.

But there are reasons to believe that age-limited online services could be appealing. While some teens may be interested in notoriety (in current parlance, becoming “Internet famous”), many other teens are far more concerned about their immediate social network, classmates and close group of friends, and they are indifferent to whether they can engage the world at large in their online lives. More broadly, dating and matchmaking sites have proven to be a reasonably stable Internet business model in a variety of countries, and an obvious feature of these sites is interaction with a discrete set of other users and separation of the potentially desirable from those less so. Many general-audience social networking sites also feature tools to find individuals already known to the user (such as classmates and former work colleagues).

These examples illustrate that online experiences with an additional level of trust in the identity of other community members could prove attractive to consumers, particularly to children or teens who are just starting to engage in online socializing and whose parents do not feel they are ready for a general-audience Web site.

Conclusion

We have outlined a framework for a largely technical approach to the age verification challenge. The nontechnical aspects of the problem will be as difficult to solve as the technical ones, if not more so. To make

this vision a reality, child development experts, governments and industry must work together to address a variety of additional challenges, including:

- Determining whether a system such as the one described in this document strikes the right balance between risk and usefulness
- Designing the necessary criteria for in-person proofing events as well as the subsequent issuing, auditing and revoking of digital identity cards
- Providing the institutional resources for securely issuing and managing digital identity cards
- Determining what market and regulatory environments are needed to support, or at least not hinder, the creation of both digital identities and the children-only Web sites that will accept the identities
- Determining incentives for children to use such Web sites
- Determining how to teach children about the importance of keeping their digital identity safe
- Resolving questions of indemnity if a digital identity falls into the wrong hands
- Determining what kind of moderating is appropriate on these Web sites, and who should be allowed to be a moderator

Creating safer children-only online experiences will no doubt be a difficult undertaking, and Microsoft's proposal is by no means the only possible approach. However, we believe that a model based on in-person proofing, the use of Information Cards and collaboration between government, industry and child development experts offers the most fruitful area of investigation. We therefore recommend a collaborative effort between government, industry and children's development experts to pilot such a system.

The information contained in this document represents the current view of Microsoft Corp. on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise), or for any purpose, without the express written permission of Microsoft.

Microsoft may have patents, patent applications, trademarks, copyrights or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights or other intellectual property.

© 2008 Microsoft Corp. All rights reserved.

Microsoft, Windows and Windows CardSpace are either registered trademarks or trademarks of Microsoft Corp. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Microsoft Corp. • One Microsoft Way • Redmond, WA 98052-6399 • USA