Washington Journal of Law, Technology & Arts

Volume 5 | Issue 2 Article 1

10-1-2008

Age Verification as a Shield for Minors on the Internet: A Quixotic Search?

Francoise Gilbert

AGE VERIFICATION AS A SHIELD FOR MINORS ON THE INTERNET: A QUIXOTIC SEARCH?

Francoise Gilbert[1]

Abstract

This article examines the issues raised by the use of the Internet by minors and children. In addition to being an outstanding source of information and a tool for connecting people in numerous affinity networks, the Internet has a dark side. Its resources may be abused for many bad deeds, including cyber bullying or facilitating encounters with child predators. One way to protect minors is to ensure that their age and identity is verified. However, this is not technically feasible without infringing on the privacy of these children as well as that of the adults who might have to be screened as well, if only to prove that there are not minors. After looking at the current problems, the existing laws, and comparing with developments in other countries, the article identifies some of legal and technical hurdles before stressing the important role of parents, guardians and education. While legislators are playing whack-a-mole, chasing child pornography, child predators, and cyber bullying, parents cannot let their children venture on the Internet unprepared and unsupervised. Despite its friendly face and its very approachable demeanor, the Internet is not a nanny. Rather, it is a reflection of the world, a combination of the good, the bad and the ugly.

Table of Contents

INTRODUCTION

<1>On the Internet, no one knows you are a dog.[2] In many instances, the freedom and anonymity of the Internet allows anyone to easily register on a website using any name or identity. Generally, one only needs an email address. Gmail, Hotmail, and Yahoo, for example, provide easy access to free email accounts. A savvy 12-year-old child can easily use an alternate identity obtained from a free email account, misrepresent her age, and obtain the user ID and passwords necessary to register on a social

networking site or online liquor store. Conversely, it is also easy for an adult to portray himself as a teenager, and obtain the user ID and password needed to register with a site used by children or minors.

<2>While the existence of child predators, pedophiles and other criminals is not a recent phenomenon, the ease of access to social networking or other websites that offer interaction between members has provided an additional venue for unsupervised encounters between adults and minors. The freedom and anonymity that these sites provide allows adults to meet minors online, move the relationship offline, and initiate sexual activities prohibited by law.

<3>In response, legislators and Internet companies are looking at procedures, such as age verification, to protect minors from inappropriate material or contacts and prevent minors from accessing websites aimed at adults. Is it possible to achieve this goal? Are there more reliable and less intrusive methods? This article explores some of the issues raised by age verification and looks at the status of laws and government enforcement actions that focus on preventing minors from accessing websites intended for adults.

Background

<4>The case *Doe v. SexSearch.com* provides a typical example of the controversy regarding social networking sites where there is no verification of the age or personal information provided by a registrant.[3] SexSearch.com is a website offering an online adult dating service that encourages its members to meet and engage in sexual encounters. Members provide information for a profile by responding to specific questions posed by the website. They may also upload photographs and video content to their profile. John Doe became a member of SexSearch.com, and shortly thereafter located Jane Roe's profile. Jane Roe's profile included her birth date, her age (eighteen), and an authentic image of Jane Roe at her then-current age. After chatting online through SexSearch.com, the two decided to schedule an encounter to take place at Jane Roe's home. During the encounter, the two engaged in consensual sexual relations; however, it later turned out that Jane Roe was actually fourteen years of age, in spite of her online registration. A few weeks later, John Doe was arrested and charged with engaging in unlawful sexual conduct with a minor, which exposed him to a penalty of fifteen years in prison and a classification that might include lifetime registration as a sex offender.[4] Mr. Doe then sued the social networking site for having failed to adequately screen the minor during the registration.[5]

<5>Concurrently, families are looking for ways to protect their children.[6] Victims of child predators have had trouble finding relief when attempting to hold the social network site responsible for having failed to prevent minors from lying in order to register on their sites. For example, in May 2008, the U.S. Court of Appeals for the Fifth Circuit ruled in favor of MySpace in a suit filed by a minor who had been assaulted by an adult whom she had met through MySpace.[7] The plaintiff, Julie Doe, despite being thirteen, had registered on MySpace, representing that she was eighteen years old. She met a sexual predator online, and was assaulted after arranging a face-to-face encounter. Julie Doe sued MySpace, arguing that the social networking site was negligent for not having implemented technological safeguards that would have prevented her registration and the subsequent meeting. The court ruled that the Communications Decency Act immunizes the social networking site from liability on claims that it was negligent in not protecting underage users from online child predators.[8]

FEDERAL LEGISLATIVE ACTIVITY

<6>In the past few months, Congress has passed several bills aimed at increasing the protection for minors in response to the risks to which minors are exposed when using the Internet. The KIDS Act[9] and the PROTECT Our Children Act[10] increase federal oversight of the online activities of registered sexual predators and other online sexual activities that include minors.

KIDS Act

<7>The KIDS Act (or Keeping the Internet Devoid of Sexual Predators Act of 2008) requires sex offenders to register with the National Sex Offender Registry the email address and other Internet identifiers that they use.[11] The new law mandates that Internet identifier information be kept current,[12] but exempts the information from public disclosure.[13] Additionally, the law requires the U.S. Attorney General to maintain a secure system to allow social networking websites to use this system in order to compare their records against the database.[14] The KIDS Act also grants the Attorney General the power to deny, suspend, or terminate use of the system by a social networking website for misuse.[15]

PROTECT Our Children Act

<8>The PROTECT Our Children Act (Providing Resources, Officers and Technology to Eradicate Cyber Threats to Our Children Act of 2008) requires the Department of Justice to develop and implement a National Strategy for Child Exploitation Prevention and Interdiction.[16] The Act creates reporting requirements for electronic communication service providers and remote computing service providers that obtain actual knowledge of the sexual exploitation of minors.[17] To the extent that the service provider has information about the involved individual, it must provide the identity, email address, IP address, URL, and other identifying information of the individual who appears to have violated the law.[18] Failure to abide by this obligation exposes the service provider to a fine of up to $150,000 for an initial violation, and up to $300,000 for subsequent violations.[19]

STATE LEGISLATIVE ACTIVITIES

<9>Numerous state legislatures have been active in this area of the law, as well. Several bills requiring age verification measures on websites have been proposed, including in the following states: Connecticut,[20] Georgia,[21] Illinois,[22] Iowa,[23] Mississippi,[24] and North Carolina.[25] In addition, bills mandating that convicted sex offenders register their e-mail addresses with the state were introduced in the Arizona,[26] Kentucky,[27] and Virginia legislatures.[28]

FOREIGN REGULATORY ACTIVITIES

<10>In addition to the United States, several other countries have issued recommendations regarding the protection of minors using online social networking and adult websites.

United Kingdom

<11>In April 2008, the United Kingdom government issued the country's first social networking guidance for the industry, parents and children, aimed at helping teens and tweens interact safely on the Internet[29] and recommending that social networking websites offer strong privacy protection procedures and use identity authentication measures. This guidance comes at the time when the U.K.'s Office of Telecommunications released a report showing that more than 25% of the country's eight and eleven-year-old children have set up a profile on social networking sites even though age restrictions may be in place to prevent pre-teens from accessing such sites.[30]

<12>The recommendations of the Taskforce on Online Child Protection aimed at online social networking sites include:

- Making safety information for users, parents and caretakers prominent, easily accessible and clear;
- Making safety information available during the registration process more prominent on the homepage, and accessible from appropriate places within the service, such as in a welcome message;
- Addressing individual responsibilities to respect and protect the online community, such as how to behave responsibly when posting images and comments;
- Providing instructions for tools that can help users protect their privacy and prevent unwanted contact or communication through the use of (1) the "ignore" function; (2) removing other users from a contact list; and (3) reviewing and removing unwanted comments on their site;
- Requesting and validating, where possible and appropriate, personal information from users;
- Capturing IP addresses or unique identifiers (for mobile devices) with a date and time stamp at registration, regularly refreshing the information after each log-in;
- Screening user profile photos, especially for users under 18, and removing inappropriate or sexually provocative images or videos posted by users; and
- Creating reporting mechanisms that automatically capture essential information and relevant evidence, such as a "screen capture" mechanism that records abusive or inappropriate content, the online ID of the abuser, and the time and date of the incident.[31]

Spain

<13>In 2008, the Spanish Data Protection Agency published a privacy handbook for children and parents with recommendations on using appropriate safeguards while online.[32] For example, parental consent is

required for processing of data for children under the age of 14.[33] The handbook also addresses the privacy risks to which minors are exposed, and provides recommendations, including the following:

- Minors should be taught how to use the Internet in a suitable manner in order to avoid any potential privacy risks;
- Parents should provide guidance to their children regarding the use of Internet, cautioning them on ancillary risks and making sure they do not post or share personal data or personal photos with strangers;
- Parents should raise their children's awareness and caution them on the benefits and drawbacks of the information society;
- Parents should closely supervise their children when using the Internet, ensuring access to adequately protected sites and refusing to provide personal data when there are not sufficient safeguards in place;
- Parents should advise their children on the risks of online social environments and instruct them to be cautious when online; and,
- Personal data should always be provided under parental supervision.[34]

<14>The handbook also addresses the important need to balance monitoring the children's activities in order to protect them from evils and ensuring that the children's privacy rights be protected. Thus, the monitoring of their personal computers should be done only when absolutely required and by way of special user accounts with certain restrictions.

NEW RULES AFFECTING SOCIAL NETWORKING SITES

<15>State Attorneys General have also initiated child protection actions against major social networking sites in connection with the use of these sites for the sale of sex or pornographic material. These investigations culminated with settlements between MySpace, Facebook, and a coalition of State Attorneys General.[35] These settlements provide useful guidelines for social networking and online sites (such as virtual world or multi-player game sites) that provide for social interaction amongst users.

MySpace

<16>In its January 2008 settlement with forty-nine State Attorneys General,[36] MySpace agreed to implement design and functionality changes to its site and to develop education and tools for parents, educators, and children. MySpace will cooperate with law enforcement to deter and prosecute criminals misusing the Internet, in addition to developing a new set of privacy protection standards.[37] MySpace will hire a third party to compile a registry of email addresses provided by parents who want to restrict their children's access to the website[38] and will bar anyone using an email address listed in the registry from signing up or creating a user page profile. MySpace will also improve the algorithm used to check for underage users.[39]

<17>In order to protect members under eighteen, MySpace will automatically change the default setting from "public" to "private" for profiles of users under eighteen, and restrict requests from others to be their "friends". MySpace will keep closed a section of its site for users under eighteen, so that they can block all users over eighteen from viewing their profile or contacting them. Users over eighteen will only be able to search this blocked section for students who are graduating in the current or upcoming year. Further, users over eighteen will not be able to add users under sixteen as friends unless they know the younger user's last name or email address.[40]

<18>Furthermore, MySpace will include new privacy protections for all users, allowing them to establish a "private" setting for their profile, and block others from contacting them.[41] MySpace also committed to devote more resources to online privacy and safety efforts and to better respond to user complaints.[42] MySpace will implement a twenty-four-hour hotline to respond to inquiries from law enforcement officials, remove sex offenders from the site, and hire a third party to identify and expunge inappropriate images and disable any links to pornographic websites.[43] In addition to the above measures, MySpace will organize an industry-wide Internet Safety Technical Task Force devoted to finding and developing online safety tools, authentication tools, and to establish specific objective criteria that will be used to evaluate emerging safety solutions.[44]

Facebook

<19>In May 2008, Facebook entered into a similar settlement[45] in which it agreed to add more than forty safeguards to protect young users from sexual predators and cyber bullies.[46] Facebook will ban convicted sex offenders from the site and will limit older users' ability to search online for subscribers

under eighteen. Like MySpace, Facebook has agreed to build a taskforce seeking ways to better verify users' age and identity.

<20>Facebook will ensure that companies offering services on the site comply with the new safety and privacy guidelines. In particular, Facebook will keep tobacco and alcohol advertisements from users too young to purchase the products and will remove groups whose comments or images suggest that they involve incest, pedophilia, or other inappropriate content. Moreover, the company will send warning messages when a child is in danger of giving personal information to an adult. Facebook will also review user's profiles when they ask to change their age, ensuring that the update is legitimate, and not intended to let adults masquerade as children.[47]

ADDITIONAL DOMESTIC LEGAL MODELS

<21>In the United States, additional laws and regulations have been in place for several years attempting to protect children from the dangers of venturing into the adults' world. One of the most important laws in this area is the Children Online Privacy Protection Act ("COPPA"). COPPA is limited to the protection of minors under thirteen.

Children's Online Privacy Protection Act

<22>COPPA applies to websites that are directed to children under thirteen or have actual knowledge that children under thirteen use the site.[48] The law regulates the collection of personal information about a child online including full name, home address, email address and hobbies.[49] The protected information also includes information collected through cookies and other tracking mechanisms when they are tied to individually identifiable information. The law requires websites to identify users under thirteen. When a user is identified as younger than thirteen, the interaction with the children and the collection, use, or retention of the child's data must be conducted as specified in the law and its related regulations.

<23>While the law and its regulations do not suggest specific mechanisms or technologies, the Federal Trade Commission (FTC) has provided specific guidance. In general, websites must use a screening mechanism that asks users to provide age in a way that does not invite falsification (neutral age-screening). For example, a drop down menu for users to enter the year of birth would be one possibility, but a drop down menu that allows users to enter birth years only making them thirteen or older would not be considered neutral because it would invite younger user to lie about their data of birth. A check box stating, "I am twelve years-old," would not be considered neutral, for the same reason. On the other hand, a temporary or permanent cookie might be used to prevent users from back buttoning and entering a new age to circumvent the screening mechanisms.[50]

Verifiable Consent Under COPPA

<24>COPPA also requires that, before collecting, using, or disclosing personal information from a child, an operator obtain verifiable consent from the child's parent.[51] The operator must make reasonable efforts, taking into consideration available technology, to provide a parent of the child with notice of its information practices and the parent must have consented to those practices.[52] The FTC uses a "sliding scale" approach to parental consent.[53] The required method of consent varies based on how the operator uses the child's personal information. Generally, if the operator discloses the information to others, a more rigorous method of consent is required than if it uses information for internal purposes. If the operator wants to disclose a child's personal information to third parties, the methods of consent required include (a) written consent: obtaining a signed form from the parent via postal mail or fax; (b) phone call: taking calls from parents through a toll-free telephone number staffed by trained personnel; (c) credit card: accepting and verifying a credit card number in connection with a transaction; and (d) email accompanied by digital signature.[54] Unfortunately, this provision fails to recognize that payment cards can be issued to minors and that merchants have little ability to verify that the card was issued to a minor, or simply choose not to incur the costs necessary to obtain the needed information.

Additional COPPA Requirements

<25>In addition to the above, COPPA requires two types of notices for users and their parents. One notice is to be addressed to the children, and the other type of notice is to be addressed to their parents or guardian. The notice of information practices that is addressed to children must be readable by children,[55] it must be clear and easy to understand, and it must state what information is collected on the site and the required participation of the child's parent or guardian. The notice of information practices that is intended for the parents must explain that parents have the right to access and control over their children's information. Of course, the company must concurrently provide the parents with this access and control.[56]

Enforcement of COPPA by the Federal Trade Commission

<26>The FTC has aggressively prosecuted websites used primarily by children when these sites had questionable data collection practices. The FTC has several avenues for prosecuting companies for their data collection, use, and sharing practices that affect the privacy of young children. The FTC may bring both enforcement actions under COPPA and under 15 U.S.C. § 45.[57] Since the late 1990's, the FTC has conducted numerous enforcement actions against sites that collect information from children under thirteen.

United States v. Sony BMG Music Entertainment

<27>The FTC's most recent enforcement action was conducted against Sony BMG Music Entertainment ("Sony") under charges that Sony had violated COPPA and 15 U.S.C. § 45.[58] According to the FTC complaints, users were required to submit a broad range of personal information, including date of birth, in order to register on the websites that Sony operated for its artists and labels. On 196 of these sites, Sony collected personal information from thousands of underage fans without first obtaining their parents' consent.[59] Many of these sites also enabled children to engage in private messaging, which allowed them to interact with others, including adults.

<28>The FTC alleged that Sony violated COPPA by failing to provide sufficient notice of the type of information the company collects from children, how it uses this information, and what information it shares with others. Sony also allegedly failed to provide parents with notices of its information practices, to obtain their verifiable consent, and to provide them with means to review the personal information collected from their children or to refuse to permit further use or maintenance of this information.[60] Additionally, the FTC charged Sony with violating 15 U.S.C. § 45 by falsely stating in its privacy policy that users who indicate that they are under thirteen will be restricted from participating in Sony activities.[61] Actually, Sony accepted registrations from users who entered a date of birth indicating that they were under thirteen, and allowed them to use the site.[62]

<29>The December 2008 Consent Decree calls for Sony to pay a $1 million fine, and to delete all personal information collected and maintained in violation of the law since April 21, 2000.[63] The Consent Decree also has a significant education component in addition to numerous reporting and recording keeping requirements.[64] Sony must educate children who use its sites and their parents, about children's privacy in general, and social networking in particular.[65] For five years from the date of entry of the Consent Decree, the company must place clear and conspicuous notices throughout its sites to invite parents and children to visit the FTC materials related to children's privacy and social networking.[66] There are additional compliance, reporting, and record keeping provisions. For example, for three years from the date of the consent decree, Sony must maintain and make available to the FTC, all documents demonstrating compliance with the Consent Decree.[67] Moreover, each document must be retained for at least two years after its creation.[68]

State Action Under COPPA

<30>The Texas State Attorney General, the only state Attorney General who elected not to participate in the nationwide consent decrees with MySpace and Facebook described above in this article, has taken other initiatives in connection with the protection of children online. In April 2008, the Texas State Attorney General completed an action under COPPA, in the case *Texas v. Doll Palace Corp.*[69] In this case, among other things, the site required users, as part of the sign-up registration process, to provide their age. They were then presented with a screen stating "The site requires that you have permission from a parent if you are under thirteen. Do you have a parent with you now?" Following the statement, the user was required to click a "yes" or "no" box in order to continue.[70] The Texas Assistant Attorney General found this practice questionable, and commented that: "Companies cannot take on a veil of innocence by hinting to underage users ways to bypass age verification requirements."[71]

Child Registry Laws

<31>In addition to the Federal laws aimed at protecting children, States have taken numerous initiatives, as well. Utah and Michigan have addressed the protection of minors from solicitations for the purchase of illegal products or substances, such as alcohol, by enacting their Child Registry Laws in 2005.[72] Both of these statutes permit individuals to register "contact points" of minors younger than eighteen. These contact points include email address, phone number, and fax number. The laws prohibit sending a communication to a contact point that is registered in the State Registry if the communication advertises

a product or service that a minor is prohibited by law from purchasing, or that is harmful to minors as defined in the state law: gambling, pornography, alcohol, tobacco, and illegal and prescription drugs.[73] The prohibition applies even if the communication is otherwise solicited. Violations of these laws are subject to stiff penalties including prison and fines.[74] The Registries that maintain the lists of "contact points" are kept under the authority of the State of Utah and State of Michigan. Marketers who wish to advertise products or services that are covered by the law must compare their list against the registry list before sending their emails.[75]

ELECTRONIC AUTHENTICATION

<32>To date, the legislators have stayed away from looking at how to implement a reliable age verification process. Instead, they have opted to address the issue of child predators and dangers of social networking through measures that would prevent sex offenders from accessing the sites. Powerful protective tools, such as electronic authentication, are currently available in commerce. The mechanisms have been marketed, for example, to websites that sell alcohol online, so that a site has a means to verify that the purchaser of alcohol meets the drinking age requirements.[76]

<33>The use of these technical means for age verification poses serious technical and legal problems.[77] In order to be able to verify the age of a person, an organization is likely to need access to additional personal information about the person. Once a person's identity is determined, it is necessary to use the proper tools to authenticate the person upon her return to the site. These two phases are known as the "identification" and "authentication process."[78]

<34>During the *Identification* phase, an organization will need to determine who a specific person is. This is done through associating attributes, such as name, address, social security number, gender, date of birth, with a real person. Once the identification process has determined enough about a person that the company is willing to do business with the individual, an *Authentication* process is used when someone purporting to be that person seeks remote access to the website. Authentication involves verifying that the person trying to access the system is really the person who was previously identified.[79] In most cases, the identification process will require the participation of one or more third parties (identity providers) who can provide the required identity information.[80] In the case of a social networking site, it could be a school, a parent, or a third party.

<35>Identity verification through electronic authentication raises numerous legal issues. For example, the identification process requires the collection of personal information by the identity provider, and the disclosure of this information to the social networking site (relying party). What information does the identity provider collect? How much of this information may it disclose to the relying party?

<36>The nature of the assertion made about a person will also have to be defined precisely. The collection process and the use of the collected information will be subject to information privacy and information security laws. There may be data retention requirements or prohibitions. If information is transferred across borders, foreign laws restricting the transfer of information outside a country may apply. There are also liability concerns. What happens if there is a faulty authentication and the applicant is granted access to the site or to the system when he should have been excluded? Who will bear the risk associated with a faulty authentication? The concepts of federated identity management, user authentication, and age verification are still in their infancy. They will require further legal analysis and scrutiny.

OTHER COMPLEX ISSUES

<37>There are many unresolved issues surrounding the concept of age verification.[81] Verifying a person's age is likely to require access to more information than just age so that the person is authenticated. When the disclosure of a person's identity is required, numerous privacy and security concerns arise. Concerns also remain regarding errors, the consequences for these errors (data spills, people being wrongfully accused, identity theft) and the liability for these errors. There are, as well, broader questions about human rights and society in general, and others that remain outside the scope of this article.

Privacy Issues

<38>Age verification requires the collection of personal information by the identity provider, and the disclosure of some of this information to the social networking site (or other relying party), which are likely to intrude on a person's right of privacy. In order to protect children, it might be necessary to obtain information from everyone, so that a classification can be made. It is only after having gathered this information and organized it in logical categories that we can differentiate children or minors from adults. How much and what information does the identity provider need in order to identify a person? How much of this information may it disclose to the relying party? The data collection practices associated with identity management should be evaluated in view of the Fair Information Practice

Principles[82] in order to ensure that privacy rights are respected.

Data Security and Data Control

<38>Collecting personal information also requires that security measures be used for the protection of the information. What happens if there is a faulty authentication and the applicant is granted access to the site or to the system when he should have been excluded? Who will bear the risk associated with a faulty authentication?

<40>Recent rulings are requiring website owners to scrub their databases against public exclusion lists in order to identify which of their users must be removed or denied entry. Mechanisms will have to be created to enable businesses to be able to verify that an individual is not part of an excluded category. The creation of these exclusion lists creates as well substantial security issues. Who should be responsible for managing these databases? Which security measures would have to be used to protect this information? How would errors be identified and corrected? These are some questions that have yet to be addressed.

How to Ensure Adequate Authentication and Identification

<41>To be effective and efficient, age verification systems require the collection of some type of personal information. Which information? To protect children, should only adults be "tagged," so that an individual would be deemed a child if he or she is not listed on the databases? What would be the content of such a database, and how much information would be required to authenticate a person and label that person an "adult"?

<42>Moreover, when applied to children, information such as social security numbers might not be available to authenticate age. Children do not necessarily have social security numbers. Nor do they have credit reports or bank accounts against which to verify information. If none of this information is available, or if there were a concern that collecting this information would open the door to more identity theft or other risks, how could children be identified? Would the involvement of their parents be required? Would the schools also be an appropriate vehicle to provide identity? Is this feasible? Is this desirable?

Duration of the Authorization

<43>Age verification may work at the time of the initial registration, but how about the other uses of the site? Once a user has been authenticated and provided a user name and password, how do we know with some certainty that the individual who logs in on a site with a certain username and password is the same as the one who initially signed on and provided personal details? Can a site with reasonable access control procedures know that the person who logs on under Juliana's user name is still Juliana after the site has validated once that there is in fact a twenty-five-year-old named Juliana? Individuals, especially children, are notorious for sharing passwords and user ID. In many households, the entire family shares one computer. Different users might not have different accounts. Could Juliana's little brother who uses the family computer after his older sister Juliana benefit from the settings of the older sister's account?

Anonymity

<44>Even if all websites were classified or labeled "PG 13" or "R" like movies or video games are, and if it were possible to create a technical solution that would be easy to implement, there would remain the problem of balancing the legitimate individual rights and freedoms against the need to protect children from predators or from content that might not be suited to them. Identification requires knowledge of and access to personal data. Would it be possible to have robust age verification, but still protect the right to use the Internet anonymously? Would Internet users, regardless of age, be required to register and login wherever they go? Would an adult who wants to check Club Penguin before registering his children to the service have to provide detailed identification so that Club Penguin verifies that this father is not otherwise a child predator or a pedophile? If this were the case, where would the boundaries be set?

Constitutional Law or Human Rights Issues

<45>The Constitutions of many countries provide the citizens and residents of these countries with extensive rights. Would excluding minors from social networking sites, virtual worlds, multiplayer gaming sites, and the like violate the children's constitutional rights to free speech (in the US) or similar rights? Would age verification aimed at minors, but necessarily required of all users, pass constitutional scrutiny if it burdens the free expression of adults?

<46>In the United States, the Communication Decency Act of 1996,[83] which attempted to regulate pornographic material (when available to children) on the Internet has been partially overturned. The indecency provisions were held to be an unconstitutional abridgement of the First Amendment Right to Free Speech because they did not permit parents to decide for themselves what material was acceptable for their children.

<47>Similarly, the "Children Online Protection Act" or "COPA" (not to be confused with the Children Online Privacy Protection Act or COPPA)[84] was adopted to restrict access by minors to any material defined as harmful to minors on the Internet. Courts have repeatedly struck down COPA on the grounds that the law violates the constitutional right to free speech under the First Amendment to the Constitution of the United States.

What Limits to the Proposed Silo System?

<48>Most age verification schemes currently contemplated might end-up establishing silos to separate children from adults, in order to prevent adults from entering a world dedicated to children, and children from accessing adult only content. Is this a good thing? How does this compare with daily life where children, teens, young adults, adults and seniors constantly interact with each other?

GLOBAL ISSUES

<49>Other issues stem from the global reach of the Internet. Given that the Internet can be accessed from anywhere in the world, would barriers created in one country prove to be useless or inefficient in a global economy? There are indeed major hurdles.

Worldwide Cooperation Needed

<50>First, age verification legal regimes are likely to be poorly adapted to the global reach of the Internet. A country-centric age verification regime would fail when minors can access foreign-based websites located in more permissive legal regimes. Unless all countries cooperate in creating a global age verification regime, teens and others trying to avoid age verification will seek access to foreign sites that are subject to less restrictive laws.

Which Definition of "Majority"?

<51>Furthermore, even if all countries agreed to create an age verification regime to bar minors from accessing certain sites – or certain areas of a site –, the countries would have to agree on thorny definitions, such as the definition of "minor." In general, "majority" is defined as the age of consent and legal responsibility. There is no consensus globally about the age of majority. Most countries have adopted eighteen as the age of majority. However, in Japan, Taiwan, Thailand, and the Republic of Korea, the age of majority is twenty. In Singapore, Monaco, Honduras, or Egypt, it is twenty-one. The same disparities appear in the United States. While the age of majority is eighteen in most US states, it is nineteen in Alabama and Nebraska, and twenty-one in the District of Columbia and Mississippi.[85]

<52>There are additional complexities when looking at specific areas where minors and adults are subject to different regimes. The age of consent is only one facet of the concept of majority. Consider, for example, the drinking age. In most countries, the legal drinking age is eighteen, but it is twenty-one in the United States, and sixteen in France, Germany, Italy, Belgium, and Portugal.[86]

<53>The definitions of what constitutes "sexual assault" or "statutory rape" vary extensively as well. In the United States, the age of consensual sex varies from fourteen in South Carolina[87] to eighteen.[88] For example, in Texas, while the age of majority is eighteen, a sexual encounter with a fourteen-year-old minor might not be illegal. Section 22.011(e) of the Texas Penal Code provides an affirmative defense to a charge of sexual assault if the victim is over fourteen years old and the actor is less than three years older than the victim.[89]

<54>With such disparities between countries, and such varieties of matters subject to age requirements, the implementation of a global age verification regime becomes highly problematic. How could a website enforce an age verification regime when there is no consensus about the age of individuals to be protected? In addition, even if a consensus were reached, which law would apply to a particular situation that involves an actor in one country and a victim in another country?

Which Content Would Be Restricted?

<55>Implementing an efficient age verification regime would require the identification of sites, venues, or content to which the restrictions apply. It is likely that there would be discrepancies between the

different laws. Even the mere attempt at defining what is prohibited might prove difficult. The famous words of Justice Potter Stewart, "I know it when I see it," as his best attempt at defining what constitutes obscenity are still relevant. Which types of sites would have to create silos? Would the silos apply to all types of information?

<56>A global solution would be even more complex, because countries have different definitions and approaches to issues that are at the center of the problem. What one country may wish to prohibit might be legal in another country. For example, hate speech is a crime in Brazil, but is protected under the First Amendment in the United States. Saudi Arabia bans homosexuality, but it is accepted or legalized in many other countries.

EFFECT ON PRODUCT DESIGN

<57>The evolution of social networking sites and virtual worlds into places where users of all ages interact and the related legal, privacy and security concerns, have a direct effect on the design of websites. Site designers must take into account the measures outlined in the MySpace and Facebook settlements when designing, building, or modifying sites directed to a U.S. audience. Indeed, these settlements do reflect the opinions of the State Attorneys General of the United States on the best practices for handling the provision or exchange of personal information and the interactions between members of social networking sites.

<58>The design of an application would have to provide the site with the ability to interact with registries where identification information might be encrypted. It will have to enable the site to evaluate the user's age. If access to registries is not possible, other methods might be used. Consider multiple questions at the registration stage in order to determine consistency between responses. Questions about the users (e.g., school, degrees) might help infer the age bracket in which the user is situated.

<59>The site might also wish to use credit card ownership as a method to verify the identity of the proposed user or to evaluate the user's access to credit, as indicia that the person might be or not a minor. However, payment cards are only a means of payment. Payment cards are not an identification document and they do not constitute proof that their holder is not a minor. Having access to a credit card may not be a solid proof of a person's age. Many minors use payment cards or credit cards. Payment cards may be legally issued to children if their parents have agreed to be responsible for the expense that their child charges to the card.

<60>The site may also need to be equipped with the ability to track users to avoid repeated requests from individuals who are guessing what might be the key to entry. Cookies and digital fingerprinting of the hardware might be useful. The site should also be equipped with technologies that would help monitor unlawful content and suspicious interactions.

CONCLUSION

<61>There are numerous societal and other issues beyond the legal issues described above. Is age verification the cure to the problem of child predators? Will it help shield children from access to controlled substances or questionable materials? Can we hope to succeed in identifying and authenticating individuals on the Internet when children's creativity and ingenuity – and adults' complacency – have made it impossible to achieve reliable identification or authentication in the brick and mortar world?

<62>Most countries have laws that set a minimum age for the purchase of liquor or tobacco, or access to restricted material that contains sex, nudity, or violence. Nevertheless, minors find ways to obtain alcohol or cigarettes or view X-rated movies. They ask help from older friends. They procure fake identification documents. The clerk at the liquor store only verifies the documents the person provides; he does not verify the identity of the person.

<63>In the brick and mortar world, where it is arguably easier to compare a live person to the photo attached to the persons' identification document, society is struggling to prevent teens from using fake ID documents and other fraudulent means to purchase alcohol and tobacco or access restricted content. How can we expect to succeed in cyberspace where there is even less ability to conduct a reliable identity check?

<64>Social networking sites are a logical – albeit sometimes unfortunate – meeting place for youth and adults. As a matter of public policy, each country will want to establish a system that duplicates the system in place in the brick and mortar world, in order to verify people's age – and possibly identify – before giving them access to restricted areas. Does it make sense to replicate a model that has shown so many flaws?

<65>Parents and schools have an important role to play. Educating children about the dangers that they might encounter on the Internet, and teaching children the appropriate ways to use the Internet would definitely contribute to the better safety of these sites. While legislators are playing whack-a-mole,

chasing child pornography, child predators, and cyber bullying, parents cannot let their children venture on the Internet unprepared and unsupervised. Despite its friendly face and its very approachable demeanor, the Internet is not a nanny. Rather, it is a reflection of the world, a combination of the good, the bad and the ugly.

<< Top

Footnotes

1. Francoise Gilbert is a principal of the IT Law Group, http://www.itlawgroup.com, a law firm based in Palo Alto, California. Her practice focuses on information privacy and security and data governance. She has assisted global and national companies on a wide range of data protection, governance and compliance issues. Ms. Gilbert can be reached at: +1(650) 804-1235 or fgilbert@itlawgroup.com.

2. Peter Steiner, Cartoon, *On the Internet, nobody knows you're a dog*, THE NEW YORKER, July 5, 1993, at 61, *available at* www.cartoonbank.com/item/22230.

3. Doe v. SexSearch.com, 502 F. Supp. 2d 719 (N.D. Ohio 2007), *aff'd*, 551 F.3d 412 (6th Cir. 2008).

4. *SexSearch.com*, 502 F. Supp. 2d at 722.

5. Doe v. SexSearch.com, 502 F. Supp. 2d 719 (N.D. Ohio 2007) (dismissing all fourteen causes of action for failure to state a claim under FED. R. CIV. P. 12(b)(6); holding, alternatively, that all causes of action are barred by the Communications Decency Act, 47 U.S.C. § 230), *aff'd*, 551 F.3d 412, 415 (6th Cir. 2008) (affirming the district court's ruling on the plaintiff's failure to state a claim, but declining to reach the issue the Communications Decency Act barring all causes of action; noting also that the district court's reading of § 230 may be overly broad).

6. *See, e.g.*, Doe v. MySpace, 474 F. Supp. 2d 843, 849-50 & n.26 (W.D. Tex. 2007) (holding that 47 U.S.C. § 230 bars claims against online networking cites in their "publishing, editorial, and/or screening capacities," for content found on the website posted by third-party users in a case where a 13 year old girl represented herself as being 18 and was later assaulted during a face-to-face meeting with a user she met online; alternatively, holding that claims for negligent or "ineffective security measures and/or policies relating to age verification," are barred under § 230), *aff'd*, 528 F.3d 413 (5th Cir. 2008) (discussed *in the following section infra*).

7. Doe v. MySpace, Inc., 474 F. Supp. 2d 843 (W.D. Tex. 2007), *aff'd*, 528 F.3d 413 (5th Cir. 2008).

8. Section 230 of the Communications Decency Act provides: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."; 47 U.S.C. § 230(c)(1) (2006). The court reasoned that an argument that MySpace was liable in negligence for abuse stemming from posted content was essentially an argument that MySpace was liable for the content itself. The court found that immunity under the Communications Decency Act extends to the presence of third-party content and the consequences of that content.

9. Keeping the Internet Devoid of Sexual Predators Act of 2008, Pub. L. No. 110-400, 122 Stat. 4224 (2008) (codified as 42 U.S.C.A. § 16915 (2008)) (hereinafter KIDS Act of 2008).

10. Providing Resources, Officers and Technology to Eradicate Cyber Threats to Our Children Act of 2008, Pub. L. No. 110-401, 122 Stat. 4229 (2008) (codified in scattered sections of 42 U.S.C. and 18 U.S.C.) (hereinafter PROTECT Our Children Act of 2008).

11. The term "Internet Identifier" includes email address and other designations used for self-identification or routing in Internet communications or postings.

12. KIDS Act of 2008, §2(b), 122 Stat. at 4224. Sections 3(c)(5) and 3(c)(6) of the KIDS Act provide limitations of liability for the benefit of the social networking sites. Section 3(c)(5) exempts social networking websites from civil claims arising from the use of the National Sex Offender Registry unless the social networking website engages in actual malice, intentional misconduct or reckless disregard to a substantial risk of causing injury. Section 3(c)(6) clarifies that social networking sites are not required to use this system, and that no federal or state liability, or any other adverse consequence may be imposed on a website based on its decision not to use the information provided in the Registry.

13. *Id.*

14. § 3(a), 122 Stat. at 4225.

15. § 3(c)(2), 122 Stat. at 4226.

16. PROTECT Our Children Act of 2008, Pub. L. No. 110-401, 122 Stat. 4229 (2008).
17. PROTECT Our Children Act of 2008, 18 U.S.C.A. § 2258A(a) (West 2008)).
18. 18 U.S.C.A. § 2258A(b).
19. 18 U.S.C.A. § 2258A(e).
20. Press Release, Connecticut Attorney General's Office, General Law Committee Leaders Announce Bill Requiring Age Verification, Parental Permission And Access At Social Networking Web Sites (Mar. 7, 2007), *available at* http://www.ct.gov/ag/cwp/view.asp?A=2341&Q=333088.
21. S. 59, 149th Gen. Assem., Reg. Sess. (Ga. 2007), *available at* http://www.legis.state.ga.us/legis/2007_08/fulltext/sb59.htm.
22. H.R. 4874, 95th Gen. Assem., 2d Reg. Sess. (Ill. 2008).
23. H.R. 2202, 82d Gen. Assem., Reg. Sess. (Iowa 2008).
24. H.R.B 2586, 123d Leg., Reg. Sess. (Miss. 2008) (dying in commission).
25. Protection from Sexual Predators Act, 2008 N.C. Sess. Laws 2008-218, *available at* http://www.ncleg.net/Sessions/2007/Bills/Senate/PDF/S132v6.pdf.
26. H.R. 2734, 48th Leg. 1st Reg. Sess. (Ariz. 2007), *available at* http://www.azleg.gov/FormatDocument.asp?inDoc=/legtext/48leg/1r/summary/h.hb2734_04-11-07_astransmittedtogovernor.doc.htm.
27. S. 65, Gen. Assem., Reg. Sess. (Ky. 2007).
28. Press Release, Commonwealth of Virginia Office of the Attorney General, Virginia First State to Partner With MySpace.com in Requiring E-mail Registration of Sex Offenders (Dec. 11, 2006), *available at* http://www.oag.state.va.us/PRESS_RELEASES/NewsArchive/121106_MySpace.html.
29. Good Practice Guidance for the Providers of Social Networking and Other User Interactive Services 2008, http://police.homeoffice.gov.uk/publications/operational-policing/social-networking-guidance (last visited Jan. 4, 2008).
30. Office of Communications (OFCOM), Social Networking: A Quantitative and Qualitative Research Report Into Attitudes, Behaviours, and Use (2008), *available at* http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/report.pdf .
31. Good Practice Guidance for the Providers of Social Networking and Other User Interactive Services 2008, http://police.homeoffice.gov.uk/publications/operational-policing/social-networking-guidance (last visited Jan. 4, 2008).
32. El Mundo, SPAIN: The Spanish Data Protection Supervisor Launches Children Privacy Handbook (October 14, 2008), http://www.ibls.com/internet_law_news_portal_view.aspx?s=sa&id=1426. The handbook provides an overview of the fundamental data protection principles set forth in the Spanish Data Protection Act. It addresses the special protection of children's privacy rights.
33. *Id.*
34. *Id.*
35. *See generally*, Press Release, N.C. Attorney General, AG Cooper Announces Landmark Agreement to Protect Kids On-Line (Jan. 14, 2008), *available at* www.privo.com/privoPDF/Myspace%20and%20State%20AG%20agreement.pdf.
36. *See generally*, Press Release, N.C. Attorney General, AG Cooper Announces Landmark Agreement to Protect Kids On-Line (Jan. 14, 2008), *available at* www.privo.com/privoPDF/Myspace%20and%20State%20AG%20agreement.pdf.
37. *Id.* at 3.
38. *Id.* app. B at 1.
39. *Id.*
40. *Id.*
41. *Id.* at 3-4.
42. *Id.* at 3.

43. *See generally*, Press Release, N.C. Attorney General, AG Cooper Announces Landmark Agreement to Protect Kids On-Line 2, app. A at 3 (Jan. 14, 2008), *available at* www.privo.com/privoPDF/Myspace%20and%20State%20AG%20agreement.pdf.

44. *Id.* at 1-2.

45. Stephanie Reitz, *Facebook, States Set Predator Safeguards*, MSNBC, May 8, 2008, http://www.nytimes.com/2008/05/09/technology/09face.html.

46. *Id.*

47. *See* Facebook's HelpCenter on Privacy, http://www.facebook.com/help/new_user_guide.php#/safety/ (last visited May. 22, 2009) (including education efforts towards users).

48. 15 U.S.C. § 6501 (2006).

49. *Id.*

50. *See generally*, Children's Online Privacy Protection Rule, 16 C.F.R. § 312 (2009), *available at* http://www.ftc.gov/os/1999/10/64fr59888.htm.

51. § 312.3(b).

52. § 312.5(b)(1).

53. *See* § 312.5.

54. § 312.5(b)(2).

55. Federal Trade Commission, How to Comply With The Children's Online Privacy Protection Rule, http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus45.shtm (last visited Apr. 26, 2009).

56. 16 C.F.R. § 312.6.

57. A practice would be deemed "deceptive" under 15 U.S.C. § 45 if it is likely to mislead and affects behaviors or decisions about a product or service. It would be deemed "unfair" if it causes or is likely to cause substantial injury, not outweighed by other benefits, and not reasonably avoidable.

58. Complaint, *United States v. Sony BMG Music Entm't*, No. 08 CV 10730 (F.T.C. Dec. 11, 2008), *available at* http://www.ftc.gov/os/caselist/0823071/index.shtm.

59. Press Release, Federal Trade Commission, Sony BMG Music Settles Charges Its Music Fan Websites Violated the Children's Online Privacy Protection Act (December 11, 2008), *available at* http://www.ftc.gov/opa/2008/12/sonymusic.shtm.

60. Complaint, *United States v. Sony BMG Music Entm't*, No. 08 CV 10730 (F.T.C. Dec. 11, 2008), *available at* http://www.ftc.gov/os/caselist/0823071/index.shtm.

61. *Id.* at 9.

62. *Id.*

63. Consent Decree, *United States v. Sony BMG Music Entm't*, No. 08 CV 10730 (F.T.C. Dec. 11, 2008), *available at* http://www.ftc.gov/os/caselist/0823071/081211consentp0823071.pdf.

64. *See generally id.*

65. *Id.* at 4.

66. *Id.* at 5.

67. *Id.* at 9.

68. *Id*.

69. Texas v. Doll Palace Corp., No. 1:2007cv00988 (W.D. Tex. Mar. 13, 2008), *available at* http://www.oag.state.tx.us/newspubs/releases/2007/120507dollpalace.pdf.

70. *Id.* at 6-7.

71. Amy E. Bivins, *Internet: Texas Assistant AG Shares Lessons Learned From Recent COPPA Enforcement Lawsuit*, BNA Privacy & Sec. L. Report, Apr. 21, 2008.

72. Utah Code Ann. §§ 13-39-101-304 (2005); Mich. Comp. Laws §§ 752.1061– 752.1068, 752.796a-752.796b (2005).

73. Interestingly, the legal drinking age in the United States is 21. The Child Registry Laws would not shield individuals between 18 and 21 from offers to purchase alcohol even though it is

illegal for them to purchase alcohol.

74. *See, e.g.*, UTAH ANN. CODE § 13-39-301.

75. *See, e.g.*, UTAH ANN. CODE § 13-39-201.

76. *See, e.g.*, IDology Inc, http://www.idology.com/ (last visited Jan. 10, 2009); *see also*, ChoicePoint Age Verification, http://www.choicepoint.com/products/age_verification.html (last visited Jan. 10, 2009).

77. *See, e.g*, ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT (OECD), OECD RECOMMENDATION ON ELEC. AUTHENTICATION AND GUIDANCE FOR ELEC. AUTHENTICATION 25-26 (2001), http://www.oecd.org/dataoecd/32/45/38921342.pdf.

78. *See generally*, Thomas J. Smedinghoff & David A. Wheeler, *Addressing the Legal Challenges of Federate Identity Management*, BNA PRIVACY & SEC. L. REPORT, Mar. 3, 2008, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1121127.

79. *Id.* at 2.

80. *Id.*

81. *See, e.g.*, Leslie Harris, *MySpace: Coming of Age for Coming of Age*, ABC NEWS, Feb. 28, 2008, http://abcnews.go.com/Technology/story?id=4355851&page=1; *see also* Press Release, Center for Democracy & Technology (CDT), Task Force Faces Complex Issues in Protecting Children Online: CDT Appreciates Opportunity to Participate, Remains Skeptical (Feb. 28, 2008), *available at* http://www.cdt.org/press/20080228press.php.

82. Federal Trade Commission, Fair Information Practice Principles, http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last visited May 21, 2009).

83. 47 U.S.C. § 223 (1996).

84. 47 U.S.C. § 231 (1996).

85. Wikipedia.com, Age of Majority, http://en.wikipedia.org/wiki/Age_of_majority (last visited May 28, 2009).

86. International Center for Alcohol Policies, Policy Table: Minimum Age Limits Worldwide, http://www.icap.org/PolicyIssues/YoungPeoplesDrinking/PolicyTableMinimumAgeLimitsWorldwide/tabid/206/Default. (last visited May 21, 2009).

87. Wikipedia.com, Ages of Consent in North America, http://en.wikipedia.org/wiki/Ages_of_consent_in_North_America#United_States (last visited May 28, 2009) (see age listing for South Carolina).

88. Wikipedia.com, Ages of Consent in North America, http://en.wikipedia.org/wiki/Ages_of_consent_in_North_America#United_States (last visited May 28, 2009) (see State laws section).

89. TEX. PENAL CODE ANN. § 22.011(e) (2003) provides:

> (e) It is an affirmative defense to prosecution under Subsection (a)(2) that:
>
> (1) The actor was not more than three years older than the victim and at the time of the offense:
>
> (A) Was not required under Chapter 62, Code of Criminal Procedure, to register for life as a sex offender; or
>
> (B) Was not a person who under Chapter 62, Code of Criminal Procedure, had a reportable conviction or adjudication for an offense under this section; and
>
> (2) The victim:
>
> (A) Was a child of 14 years of age or older; and
>
> (B) Was not a person whom the actor was prohibited from marrying or purporting to marry or with whom the actor was prohibited from living under the appearance of being married under Section 25.01.

90. Jacobellis v. Ohio, 378 U.S. 184, 197 (1964) (Stewart, J., concurring).