31st international conference of data protection and privacy commissioners

Madrid, 4th, 5th and 6th, november 2009

Online Age Verification for Our Children

A Report on the Tools and Resources Available
for Safeguarding the First Generation of Digital Natives

Jules Polonetsky

THE FUTURE OF PRIVACY FORUM
WWW.FUTUREOFPRIVACY.ORG

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Online Age Verification for Our Children

A Report on the Tools and Resources Available for Safeguarding the First Generation of Digital Natives

Protecting the privacy and safety of children and ensuring they do not access inappropriate content or environments continues to be a priority for parents. Service providers, educators, governments and others are working to ensure that children can obtain the benefits of technology while being shielded from the excesses. What are the current techniques being used to establish the age of Internet users and are they effective? What are the emerging techniques that may be available in the future? What are the adverse consequences or the new opportunities provided by new technologies? And how can we ensure that our efforts are relevant to the lives of this first generation of digital natives?

This report is available as part of the materials published by the 31st International Conference of Data Protection and Privacy Commissioners in Madrid.

It can also be accessed on the Future of Privacy Forum's web site at http://www.futureofprivacy.org/.

Thanks are due to Future of Privacy Forum Policy Fellow Andrew Samuel, who played a lead role in the preparation of this report.

Thanks also to Wim Nauwelaerts of Hogan & Hartson for his willingness to share his time and expertise about the European market.

Introduction: the Goals of Age Verification for Children:

The goals of performing online age verification are to protect the privacy and safety of our children, and ensure that they do not gain access to inappropriate content.

1. **Privacy**: Maintaining children's privacy means keeping children out of environments where personal data may be collected and used for marketing purposes without parental consent, or made public in a manner that has negative social implications or is broader than originally intended.
2. **Safety**: Children should be protected from the potential risk posed by forms of contact that are inappropriate. This includes inappropriate contact with strangers, such as advances made by sexual predators, as well as harmful contact with individuals with whom the child is familiar offline, such as cyber-bullies.
3. **Content**: Children should be restricted from accessing objectionable content such as pornography, web sites related to gambling, drug-abuse, and violence.

Attempts to perform age verification online are hampered by the fact that children generally lack the credentials to prove their age themselves. Therefore, methods of age verification often fall into one of two categories. In the first, access to a web site is restricted to users who can prove that they are adults; if a user fails to prove that he or she is an adult, appropriate measures are taken. In the second, a web site performs identity authentication for an adult, on whose authority as a legal guardian age verification for his or her children can be performed thereafter.

Determining that a User is an Adult

A. Self Verification
    a. The site asks the user in a neutral way what his or her birth date is, and if the user is underage, a session cookie is placed in their browser preventing access for the duration of their web browsing session.
        i. Self-verification of this sort is the standard in the USA, where the Children's Online Privacy Protection Act (COPPA) requires all web sites which collect personally identifiable information (PII) of children to obtain verifiable parental consent. Sites that are not aimed at children that collect personal information may rely on the neutral age screen to ensure that users are adults. And, as noted in the DG Infosoc report[1], self-verification is the technique favored by many adult web sites and social networking sites in Europe.
        ii. Advantages: Cheap and easy to implement.
        iii. Concerns: Easy for people to lie.

[1] See Information Society & Media Directorate-General (DG Infosoc): Background Report on Cross Media Rating and Classification, and Age Verification Solutions, p.18

1. Denise Tayloe on the current COPPA-mandated self-verification scheme: "Children quickly learned to lie about their age in order to gain access to the interactive features on their favorite sites. As a result, databases have become tainted with inaccurate information and chaos seems to be king where COPPA is concerned."[2]

i. Current Examples:

2. The technology for this is ubiquitous. Virtually all social networks are reliant upon self-verification to know the age, and any other personal information, about their users.

B. Peer Based Verification

a. Some web sites and online social networks employ some aspect of peer-review to determine whether a user's participation in an online environment is appropriate. Peers may vote, recommend or rate an individual based on personal knowledge established offline or elsewhere other than their profile itself.

i. Advantages: Cheap and easy to implement.

ii. Concerns: Individuals could conceivably create multiple profiles and use them to gain access for themselves. Also, any rating system includes the potential for collective cyber-bullying.

iii. Current Examples:

1. From the Report of the Internet Safety Technical Task Force: "Facebook uses a peer verification system for users who identify themselves as under 18. MySpace has a closed school section that relies on peer approval and moderation to separate current students from alumni and provides a report abuse category that allows current users to report underage users."

C. Semantic Analysis

a. Semantic Analysis works on the principle that people of a certain age will employ different and identifiable levels of sophistication when constructing, for example, a social networking profile. Technology is used to analyze an individual's profile page, determine an age-range for the user, and flag users to administrators if the content they have posted indicates that they are underage.

i. Advantages: Can be used to supplement self-certification on social networking sites.

ii. Concerns: The technology is still in its infancy. Moreover, people have different levels of maturity. There will always be outliers who pose difficulties for the technology on either end: exceptionally mature children, or developmentally handicapped adults. Also, as stated above, semantic analysis can at best only establish a relatively broad range of potential ages.

The technology can be problematic in multilingual environments.[3]

iii. Current Examples:

1. MySpace:

a. "*New York, January 14, 2008* – In a joint effort to increase the safety of teens online, MySpace and the Attorneys General in the

---

[2] "From: COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech" by Berin Szoka and Adam Thierer, p.14

[3] See DG Infosoc: Background Report on Cross Media Rating and Classification, and Age Verification Solutions, p.21

Multi-State Working Group on Social Networking representing 49 states and the District of Columbia today unveiled a Joint Statement on Key Principles of Social Networking Sites Safety (attached) designed for industry-wide adoption. This common set of Principles relates to online safety tools, technology, education and law enforcement cooperation."[4]

2. From the ISTTF Report, p.221:
    a. "While there is currently no effective age verification mechanism due to technical, legal, and data challenges, MySpace has adopted a number of technical solutions and procedures to enforce the age restriction. For example, the MySpace registration page requires prospective members to select their year of birth from a drop down menu currently ranging from 1908 to 2008, and individuals who enter a date that does not meet the requisite age are not permitted to register. MySpace also places a session cookie on the registration page so that a prospective member cannot change his/her age if the initial age was below that specified in our Terms of Use.

    To combat a situation where an underage minor lies about his or her age, MySpace employs a strengthened search algorithm, utilizing terms commonly used by underage users, to find and delete underage profiles. The site is scanned for such terms, and the database of search terms is updated to reflect changes in user behavior and terminology.

    Profiles that have been reported by MySpace members or parents as belonging to an underage user also are reviewed by MySpace. Whenever an underage user is identified, the profile is deleted. MySpace similarly will remove members if we believe they are over 18 and they represent themselves as under 18."

D. Credit / Debit Cards
    a. Advantages: Ubiquitous.
    b. Concerns: Credit/Debit cards are not intended for age verification. They cannot verify age, only whether a user is under/over 18, and even this line is becoming blurry with the rise of some new technologies. The Visa Gift Card, for example, is a prepaid card that can be used anywhere Visa is accepted, and is indistinguishable from a credit card in processing an online transaction.
        i. Minors may be able to access cards without their parents' or guardians' knowledge.
        ii. Use of a credit card requires a charge. Though age verification can be performed with a perfunctory $1.00 charge that is immediately refunded, some users may be suspicious of purportedly free services that require them to input credit card information. Furthermore, many sites prefer to make their content available for free, and might not wish to insert such a credit card transaction into their relationship with the consumer.

Current Examples: Ubiquitous. This is the most widely utilized

[4] http://www.newscorp.com/news/news_363.html

method of age verification on the Internet today.

Identity Authentication: Database Methods

A. Publicly Accessible Data
   a. Forms of data about adults publicly available or available to certain businesses in some countries can include information from credit reports, criminal history, real estate transfers, and voter registration. Such data can be compiled to produce a portfolio on an individual and, among other uses, serves as a basis to present challenge questions to ensure proper ID. Databases constructed from information gathered by the Post Office or the DMV have been suggested as well. Finally, some have suggested databases compiled from school records, which could serve both to perform effective age verification of children, as well as to ascertain the identity of their legal guardian.
      i. Advantages: Requires little effort on the part of the user: information has already been compiled and stored elsewhere.
      ii. Concerns: Dissemination of this data and potential onward transfer for secondary uses raises significant data protection concerns.
         1. Though most of these types of information are useful in determining whether someone is a child or an adult, it is difficult to ascertain whether an adult is the legal guardian of a particular child, except when using school records.
         2. The use of school records as a means of age verification and identity authentication on a large scale is difficult. In addition to privacy concerns, doing so would pose an undue administrative burden or many school systems which are already understaffed and underfunded, in addition to already being explicitly prohibited in some jurisdictions.
   b. Current Examples:
         1. Aristotle's Integrity[5]:
            "Integrity is a versatile, cost-effective and popular identity and age verification tool. It works by verifying standard issue driver license or other government-issued ID of citizens of 157 nations."
         2. Veratad[6]:
            Veratad provides age verification solutions for companies selling tobacco, alcohol, rated entertainment, etc. online. Methods of age verification include credit card data and other publicly available information. "Our system responsibly compares an online visitor's data entry against billions of records from multiple trusted data sources empowering you to verify visitor age."
         3. Danish: Certified Kid[7]:
            This Danish system makes us of on-site age verification subject to teachers or parents. Not exactly using school records, but age can be verified on the authority of a schoolteacher.
         4. British: GB Group[8]:

[5] http://integrity.aristotle.com
see also: http://integrity.aristotle.com/content/view/380/72/
[6] http://www.veratad.com/age_verification_AgeMatch.html
[7] http://www.certifiedkid.com
[8] http://www.gb.co.uk/gbgroup/what-we-do

GB Group is a British company that does both ID verification as well as "ID analysis," which is essentially consumer targeting. Sources of ID information include passports, utility bills, credit cards, and other documents which are commonly used to establish identity.

5. 192 Business Services[9]:
   192 Business Services focuses on age verification for online gaming (gambling) sites. Their information is drawn from voter databases, credit reference agencies, passports and travel visas, insurance numbers, tax information, and most interestingly, voiceprint capture technology.[10]

B. Social Security Numbers (SSN) or Similar Identifiers:
   a. A site or service requests an SSN or other such data which can be verified against a government database to verify one's age and identity. SSN need not be full SSN, and in some cases the last 4 digits will suffice. Driver's license and passport information are also commonly used.
      i. Advantages: Highly trustworthy and reliable data source.
      ii. Concerns: Huge data protection and privacy concerns, and considering the sensitive nature of this data, these concerns are even greater than those associated with the collection of publicly available information. Consumers may be particularly concerned about providing such sensitive information to third parties.
         1. Use in cross-border applications is limited.
      iii. Current Examples:
         1. Search Engines in Korea[11]:
            All search portals operating in South Korea are required to perform age verification for certain types of content accessed through their search engines. To access mature content, as determined by a list of over 700 search terms maintained by the Korean Government itself, users will have to input their NRRN, (national resident registration number) to be checked against a database. Similar Internet filtering technology at Korean search engines Naver, Empas, and Daum is used to block access altogether for sites containing information deemed politically sensitive.

C. Offline Verification
   a. Third-party services offer offline verification, using direct contact with a parent/legal guardian to perform age verification of minors and obtain parental consent. This may include face-to-face contact at a post office or DMV, a phone call, or faxed forms. Offline verification is particularly effective in a mobile context, where face-to-face ID and age verification must take place at the point of sale.
      i. Advantages: Effective, strong, reliable.
      ii. Concerns: Costly and cumbersome. Also, if offline verification corresponds to a PIN code or password which grants authorization to certain sites online, minors may obtain this information and thereby defeat the purpose of offline ID.

---

[9] http://www.192business.com/oursolutions/verification/age
[10] http://www.192business.com/oursolutions/verification/voice
[11] http://www.zdnetasia.com/news/internet/0,39044246,62013656,00.htm
also, see: http://abcnews.go.com/Technology/PCWorld/story?id=3184458

Furthermore, since not all sites have such stringent rules as to require offline ID, many sites requiring it have seen user migration to other platforms.

iii. Current Examples:

1. Privo[12]:
   Privo uses a number of different methods to perform ID authentication: credit card information, driver's license, phone calls, faxed forms, and last 4 digits of one's SSN. Once a parent or legal guardian has been positively ID'ed, Privo obtains and keeps a database of verifiable parental consent, which permits their clients—including a number of social networking sites—to collect and store the PII of children under the age of 13.
   a. In the US, according to COPPA regulations, sites aimed at children must take the additional step of obtaining verifiable parental consent to be able to collect and use PII. This authorization is sometimes obtained through emailing a parent or through third-party services, such as Privo, which maintain certification of parental consent for their clients.
2. German Offline Verification Program
   The DG Infosoc Background Report states that this form of offline verification is favored by the German government, and that a nation-wide system has been in place since the ratification of the "Interstate Treaty on the Protection of Human Dignity and the Protection of Minors in Broadcasting and in Telemedia" which went into force on Jan 1, 2009.[13]

---

[12] http://www.privo.com/

[13] From the DG Infosoc Background Report, pp.23-24:

Age Verification for the protection of minors in Germany

The German law on the protection of Minors mandates the use of Age Verification Solutions. According to Article 4 (2) of the Interstate Treaty on the protection of Minors in the Media (JMStV) content proven to seriously impair the development of children, and adolescents is only legal (in "telemedia") if the provider can assure that the content may only be accessed by adults.

The law makes a distinction between content that is absolutely illegal, content endangering minors and content that is harmful to minors. Content endangering minors includes content for adults only such as pornography and gambling, and providers are obliged to use what is referred to as a strict age verification solution, which intends to ensure that content is not available to minors. What is referred to as, "Basic Age Verification", is applied to harmful content, like violent games and similar elements in games and chat rooms, as well as communities with a minimum of supervision.

Strict Age Verification implies a one-time physical identification, where the identity is checked against a valid identity card, either at the post office (e.g. PostIdent), at the point of sale in mobile phone shops, or at lottery offices. Other accepted forms of identification that rely on identity checks done in the past, and for purposes other than accessing harmful content, are bank cards with an age criteria (65 million in Germany). The identity check is done in connection with the opening of a bank account, or the entering into of a credit card contract (e.g. Schufa-Q-Bit). A digital identity card with a build in age criteria for age verification purposes will be launched in 2010.

Identity Authentication: eID Cards

A. An eID is an identification card that contains information about the user stored in a chip embedded in the card itself. Existing technology allows information stored electronically on an eID to be used in performing authentication and age verification online. Though in some contexts “eID” is used to refer only to those cards issued by governments themselves (e.g. Belgium, Germany), the term can refer to any ID containing electronically stored information. eID’s have the potential to translate the credibility of widely accepted forms of government-issued ID into a new form which is compatible with the modern requirements of today’s digital marketplace.
    a. Advantages: eID’s are based on trustworthy data sources that, when fully developed, can overcome many of the hurdles associated with other age verification technologies. For example, governments have the authority and the credibility to collect and store PII, and when widely implemented throughout an environment, an eID could suffice as an non-invasive form of AV online.
    b. Concerns: Degrees of implementation vary throughout the vast network of the Internet. Furthermore, difficult to enforce broad implementation, especially of a single standard. Additionally, migration to other services becomes common: e.g. not all sites on the Internet will hold themselves to such a high standard of age verification, which means that objectionable content and environments will likely still be accessible. In many cultures, significant objections to the concept of national ID’s may also make this option controversial.
    c. Current Examples**:**
        i. Belgian National eID Cards:

The Kids-ID project is based upon the association of an interactive protection service, an internet service, and a specific version of the application of the Belgian national ID card. Kids-ID is the same size as a credit card and holds secure information. It offers three functions:

- It is first and foremost an official electronic identity and travel document that is compliant with the ICAO standard valid in most European countries and contains the identity data and the child’s photo stored on the electronic chip. The parents’ name is also featured on the card.
- Secondly, it protects the child in emergency situations. If the child is lost or has an accident, the card features a telephone number that can be used to contact the child's relatives. The caller dials the special number, entering the eleven digits which identify the child on the national register. The call is immediately transferred to the first number in a list that may feature up to seven contacts selected by the parents at the time of issuing of the card. If this person cannot be reached, the call is redirected to the second number in the list, and so on, until somebody answers. If none of the contacts can be reached, the request is redirected to Child Focus, a Belgian foundation for child assistance, accessible 24/7, which can be assisted by the national police force if required.
- Lastly, the Kids-ID card may be used on the Internet for safer access to on-line chat rooms and for services requiring ID. An integrated PIN code automatically identifies the child and only allows him/her access to those internet services that he/she is allowed to use.

ii. Geldkarte[14]

Geldkarte is a German chip-based electronic purse system which is increasingly being used as a proxy for age verification. Approximately 75% of German bank cards make use of Geldkarte technology.[15]

Identity Authentication: The Identity Metasystem

A. A new method of ID authentication is being built on a platform known as the Identity Metasystem. It allows users to authenticate online by selecting from a collection of digital identities known as Information Cards. There are two components: the first is a selector, which stores a user's Information Cards and allows them to choose a particular one in response to an authentication request from a site they have navigated to. The other component of the ID Metasystem is the collection of Info Cards, which can be self-issued by the user or issued by a third party.
   a. Advantages: The premise of the Identity Metasystem is that "relying parties," sites that are seeking to make sure that users who visit are of a certain age, do not have to perform age verification themselves. This process can be costly and time-consuming, and as a result is often not done properly. Instead, through information cards, the age verification transaction becomes much more efficient for the user and for the relying party because proof of age can be taken on the authority of a credible third party.
      i. Users can choose what level of PII to give to the sites which ask for it. Information Cards can satisfy varying levels of security requirements, from very secure ones which are meant to grant access to sensitive information to self-issued ones which can indicate no more than that the user is an individual.
   b. Concerns: Although the Identity Metasystem provides users with the means to demonstrate that they are of a certain age once they have been verified, it does not provide any specific age verification solutions. Other methods of age verification, such as credit card transactions or databases of public information, must be used to conduct age verification before the Information Card can be issued.
   c. Current Examples:
      i. Equifax I-card
      Equifax, a member of the Information Card Foundation, has developed a number of different Information Cards. These cards can be used to verify claims ranging from full ID authentication, to simple over-18 age verification, and are available for download along with a selector developed by Azigo.[16]

---

[14] http://www.geldkarte.de/_www/en/pub/geldkarte/geldkarte_users.php

[15] http://www.geldkarte-jugendshutz.de

(cont'd footnote 12)

A subsequent authentication process takes place every time the identified person intends to access harmful content. To prevent multiplication of access data and the distribution of access data to third parties this includes the use of Unique Identifiers (copy protected hardware), bank or ID cards with age criteria or SIM cards, and clearly identifiable devices such as PCs or set top boxes, or so called PIN/TAN systems.

Basic Age Verification relies on the control of ID card control numbers, credit card numbers and sometimes web cam checks, intended to verify that the person is above 16 years old. The authentication is simpler than under the Strict Verification Process and uses a one time authentication and a pin code provided by SMS.

Based on the legal requirements of Article 4 (2) of the Interstate Treaty on the protection of Minors in the Media (JMStV),

ii. IDology uses challenge questions derived from a database of publicly available information to perform ID authentication and issue Info Cards.[17]
iii. Microsoft has developed a set of new Windows capabilities code-named CardSpace, which functions as a Windows-based selector. It can be used to generate self-issued Information Cards and is compatible with Cards issued by third parties as well.[18]

Biometrics

A. New technology can allow a user's age to be determined through an analysis of fingerprints, bone density, unique patterns on the surface of the iris, or through other biologically unique identifiers. Though most systems are based on inherent characteristics such as those mentioned above some platforms function by identifying behavioral traits such as walking gait or typing style.
    i. Advantages: Trustworthy and difficult to circumvent.
    ii. Concerns: There are some ethical issues surrounding the cataloguing of detailed personal information, especially certain characteristics which might touch on medical information or characteristics about which individuals are self conscious. It definitely means that individual information, of a much more inherently personal nature than even a name and address, will be stored somewhere, often by a third party.
        1. Most, if not all, systems cannot determine a user's exact age.
        2. Age verification through these types of technology tend to be costly and hardware-reliant.
    iii. Current Examples:
        1. See annesdiary.com, a social networking site for girls age 6-14, where membership fee includes a fingerprint scanning device which girls use to authenticate themselves, as opposed to a password or other login.
        2. A UK company called Verificage[19] has developed an age verification device that is not dependent on using or storing personally identifiable information. The technology is based on a USB device that conducts an ultrasound scan of the bone density of a user's hand. The results can be used to determine the user's age, and are accurate up to the age of 13, though not beyond.
        3. From the GMAC media room:

(cont'd footnote 12)
and what is referred to as Common Guidelines developed by Jugendschutz (KJM), Jugendschutz approves solutions and solutions providers in Germany to assure conformity to the legal requirements. To date the KJM has approved 24 providers of Age Verification Solutions40.

According to the KJM the approval process is viewed as a seal of approval by industry. It has considerably reduced open access to adult content sites hosted in Germany.

[16] https://equifaxicards.com/myeid/about.do
[17] http://www.idology.com/
[18] http://msdn.microsoft.com/en-us/library/aa480189.aspx
[19] http://www.verificage.com/site/index.php

> "The GMAT exam is currently the only examination that utilizes the new PalmSecure palm vein identification technology. PalmSecure features a near-infrared light that captures a palm vein pattern, generating a unique encrypted biometric template that is matched against the pre-registered candidate's palm vein pattern, thus ensuring the test taker is that candidate. It offers a highly reliable form of authentication because it utilizes no trace technology, no image is ever stored, and the data cannot be read by other devices. The CNIL noted in its approval, 'It is not likely to be captured without the knowledge of the person concerned and therefore presents very little risk for the civil liberties and fundamental rights of the individuals.'"[20]

Age Verification on the Mobile Internet

A. As mobile broadband proliferates and becomes increasingly similar in speed and capability to what one's desktop computer can do at home, new challenges will arise regarding age verification for inappropriate content. Mobiles represent a new frontier in the incorporation of the digital world into our everyday lives. However, they also present new risks concerning the protection of personally identifiable information, especially for children. A number of measures have shown promise in allaying these concerns.
    a. European Mobile Providers have adopted a set of self-regulatory principles regarding age verification and access control on mobile networks, referred to as the "Framework."[21]
        i. The Framework outlines a five-point plan to control access to inappropriate content on mobile phones with Internet capabilities. The points are:
            1. Access Control Mechanisms
            2. Raising Awareness and Education
            3. Classification of Commercial Content
            4. Fighting Illegal Content on Mobile Community Products or on the Internet
            5. Implementation, stakeholder consultation and review
                a. Success in the implementation of the previous five points was evaluated and published in an Implementation Report in April 2009.[22]
    b. The FTC issued a report in April 2009, entitled "Mapping the Mobile Marketplace," in which they dedicated one section to Children and Teens. Some points on the future of children and mobile phones from their panels:
        i. "...the top five U.S. wireless carriers currently offer, at no cost, a relatively common set of parental controls, including: 1) the ability to turn off Internet access; 2) the ability to filter web content; and 3) the ability to block unwanted text messages or phone calls. They also offer web-based mobile bill monitoring. Diggs [David Diggs, Vice President and Executive Director of The Wireless Foundation] predicted that, in the near future, wireless carriers will compete for subscribers based on their ability to provide family-friendly controls. In an effort to

---

[20] http://gmac.mediaroom.com/index.php?s=43&item=80
[21] http://ec.europa.eu/information_society/activities/sip/self_reg/phones/index_en.htm
[22] The Implementation Report on the principles in the Framework can be viewed here: http://www.gsmeurope.org/documents/PwC_Implementation_Report.pdf

make this information more readily available to parents, each of the leading wireless carriers' websites now gathers this information under the common search term "parental controls." (page 32).

c. Privacy concerns associated with the usage of social networks are becoming increasingly relevant to the mobile world, at a very fast pace. As smart phones get smarter, and our digital and social worlds more tightly knit, mobile phones rather than computers are becoming the medium of interaction between individuals and the social networks they belong to. For example, 18 months ago, only 3-5% of Australians used their mobile phones for anything besides calling and texting. Today, that figure stands at 40%, with a majority of this growth having been driven by social networking. In the coming years, there will be a need for greater efforts to protect the PII of individuals, and especially of children, on mobile phones specifically.[23]

Age Verification Challenges in Massively Multiplayer Online Games (MMOG's) and Virtual Worlds

A. The magnitude and flexibility of emerging virtual worlds represents new challenges in keeping children safe from inappropriate content and environments. Panelists at a 9/25/2009 Progress and Freedom Foundation conference on Next Generation Parental Controls and Child Safety Efforts stressed the similarities between online worlds and real worlds, noting that no reasonable parents would feel comfortable allowing their children to roam unsupervised in New York City, and that as online worlds become more sophisticated, they will begin to approximate such an experience more closely. The massive, dynamic nature of online worlds makes it difficult to find a balance between prohibiting children from participating at all, and finding a way to ensure that they have appropriate, positive experiences. Panelists at the conference agreed that emerging technologies will provide a more nuanced way for children to experience the positive aspects of online worlds more fully, while remaining shielded from those aspects which are not age-appropriate.

a. Linden Labs, makers of the popular virtual world Second Life, have sequestered all adult-themed content of their virtual world on a new continent called "Zindra." Users must verify their age before they can access this continent through an age verification process, based on either a credit card transaction or through Aristotle's age verification service (see above, under Database methods).[24]

i. Some gamers have reportedly used the personal information of celebrities, or even dead people, which are available online to defeat Integrity's age verification process. Users are required by the Terms of Service only to state that the information is correct, not that it is their own. Moreover, both Linden Labs and Aristotle have ensured that they will not retain any PII for longer than is necessary to perform the age verification process, thereby making it impossible to go back and determine which users were age-verified using false information

---

[23] http://www.heraldsun.com.au/news/national/facebook-twitter-call-the-shots/story-e6frf7l6-1225774162951

[24] see: https://support.secondlife.com/ics/support/default.asp?deptID=4417&task=knowledge&questionID=6362

also: http://news.digitaltrends.com/news-article/19774/second-life-getting-content-filters-adult-continent

and: http://www.netfamilynews.org/labels/Zindra.html

from celebrities or the deceased.[25]

b. World of Warcraft, the world's largest Massively Multiplayer Online Role Playing Game, now claims over 14 million subscribers. Blizzard Entertainment, creators of World of Warcraft, requires a valid government-issued document for ID as part of their registration process. For minors to participate, Blizzard requires their parents to register and provide government-issued ID for themselves.
c. Another set of challenges comes from the world of live gaming, where gamers can interact with each other in real time. Not only are there concerns of cyber-bullying or predation as there are with other openly accessible Internet environments, there are concerns about the content itself; consider the now infamous prostitute solicitation scene from Grand Theft Auto, or the incredible popularity of some violent and bloody games.
    i. The newest generation of video game consoles come equipped with parental controls, and the first time they are activated, gamers must go through the parental controls menu as part of system setup before they can even play. Given the expense of these gaming systems, it is expected that parents will be the ones buying them for their children, and therefore that they will be there to set the system up at an appropriate age level the first time a game is played.
        1. Due to age restrictions on video games at the point of sale, it is now more difficult for underage children to obtain video games than it is for them to obtain R-rated movies in American retail stores.
        2. There are resources, such as the Microsoft-supported web site, GetGameSmart.com, which seek to promote ongoing and effective engagement by parents in this part of their children's lives.[26] Features of the site include a message board where parents can communicate with each other, information about the resources available to parents, games for children, and a "Family Challenge" where families can earn gold stars for completing tasks such as signing a pact establishing family gaming rules, or watching an informative video.
        3. Some online games aimed at younger children allow for a limited level of interactivity, such as messages users can send to each other from a drop-down list of acceptable terms and phrases.
        4. Finally, as mentioned above, Crisp Thinking offers software that can analyze long-term interactions between users in MMOG's using pattern recognition technology to determine whether interactions between users might have aspects of cyber-bullying or predation.

Filtering / Monitoring / Auditing: Appropriate Responses to Confirmed-Underage Users

A. Client-side Software
    b. There are many resources available for parents who wish to install programs on their home computers which can monitor the activity of their children on the Internet, filter the content they see, and prevent them from accessing content which has been identified as objectionable (pornography, violence, gambling, etc.) A wide array of programs have

[25] http://www.massively.com/2007/12/09/aristotle-integrity-el-dia-de-los-muertos/
[26] http://www.getgamesmart.com/

been deployed for over a decade now, and are available in any price range, including some which can be downloaded for free. Additionally, parental controls are becoming increasingly customizable. The restrictiveness of the filtering is variable and dependent on user preferences, and can usually be tailored based on broadly defined categories corresponding to what has been deemed appropriate for particular age groups.

i. Microsoft's Windows Vista ships with parental control features already built-in. Parents have the ability to determine which games and programs their children use, and control their children's Internet activity with having to install any additional features, aside from regular updates.[27]

ii. Google and other popular search engines have options which enable parents to restrict the web sites returned when their children conduct searches.[28]

1. Advantages: Parental controls are generally easy to install and implement. Also, many even among less computer-savvy parents are aware of parental controls as a resource to help control their children's Internet experience.
2. Concerns:
    a. Filtering programs can be rendered ineffective without frequent updates.
    b. Restrictive filters sometimes prohibit access to useful information.
    c. Such programs tend to focus on preventing access to objectionable content, but may still allow access to unsafe environments where users can divulge PII, especially in unfiltered instant messaging.
    d. Parental controls tend to function on an all-or-nothing basis, meaning that they will either permit access to the entirety of a web site or prohibit it. This puts parents who want their children to have access only to certain parts of a web site in a difficult position.
    e. Programs such as these can provide a false sense of security to parents. Some may become lax in monitoring their children's web activity themselves, feeling that the program does a sufficient job of limiting their children's access to objectionable content.
3. Current Examples:
    a. IMSafer[29]:

        IMsafer is one example of filtering programs that work in a more nuanced way than the older generation of filters, which were all-or-nothing. "The IMSafer tool respects a child's privacy since parents are not allowed to read the full transcripts of online communications. Instead, the application only monitors IM conversations for content that is considered dangerous. Importantly, however, this includes the trading of phone numbers or other personal information."[30] IMsafer is part of the Crisp Thinking company, whose server-side services are discussed in the next section.

    b. Other examples of client-side filtering programs:
        i. Ishield: http://www.guardware.com/is_overview.php

---

[27] http://www.microsoft.com/windows/windows-vista/features/parental-controls.aspx
[28] http://www.google.com/support/websearch/bin/answer.py?hl=en&answer=35892
[29] http://www.imsafer.com/
[30] from Parental Controls & Online Child Protection, by Adam Thierer

ii. Cyber Sitter: http://www.cybersitter.com/cybdefault.htm
iii. Cyber Patrol: http://www.cyberpatrol.com/
iv. Both of the following links lead to web sites where parents can access information and resources on how to protect their children online. Though both of these web sites are excellent resources to parents, it is worth noting that there are others which are more of an attempt to prey on net-unsavvy parents with dubious offers by exploiting their fear of what their children might be exposed to.
    1. http://www.getnetwise.org/
    2. http://netfamilynews.org/

c. Dubestemmer.no is an excellent resource for parents and children for parents and children, both inside the E.U. and out, seeking to learn about issues of privacy and the Internet. Dubestemmer means "You Decide" in Norwegian. It is one of the few web resources which is focused specifically on privacy and is meant to appeal to a broad audience. The web site includes specific information for 9-13 year olds and 14-17 year olds, as well as short clips, funny anecdotes, and an appealing graphic design. The site aims to place the onus of making conscious privacy-related decisions on young adults themselves.

"You decide... is a cooperation between the Norwegian Board of Technology, the Norwegian Data Inspectorate and the Norwegian Directorate for Education and Training. The aim of the project is to increase young people's knowledge of privacy and to raise their consciousness about the choices they make when they use digital media such as the Internet and mobile phones."[31]

D. Server-side Approaches
   a. These are systems in which filtering of content takes place before content reaches the user's computer and is bounded by the standards of the website or service platform itself. The term is often used in reference to ISP-level filtering, though it can refer to other forms of filtering which function at the network-level. Server-side approaches can be thought of as content filtering in a cloud-computing context.
   b. Many social networks use peer reporting as a means of discovering inappropriate behavior or behavior that flags another user as in need of psychological treatment. Though this isn't peer-based verification of age or identity, it can serve as a means of controlling objectionable content in concert with software.
      i. Advantages: Server-side technologies are less susceptible to some of the shortfalls of client-side programs that result from human error. There is no need for them to be updated by users, and they are generally easier for less tech-savvy parents, for whom server-side filtering amounts to a turn-key solution. Filtering at the server level has also been used by web sites looking to filter user-generated content that might be inappropriate for some users (e.g. Youtube flags some videos as appropriate only for those 18 and over).
      ii. Concerns: The perception of server-side filtering as a turn-key solution is accompanied by concerns that parents may have less specific control over the

[31] http://www.dubestemmer.no/en/

degree to which content is filtered. Moreover, when useful or appropriate content does become restricted, the issue can be more burdensome to resolve. Also, as with client-side software, there are issues that parents may become more lax in monitoring their children's behavior if they believe the responsibility for doing so falls to ISP's. At the most extreme, there may be concerns of censorship.

iii. Current Examples:

1. AOL: AOL provides their customers with standard Internet filtering and parental control technology.[32]
2. Rulespace is one company which provides back-end filtering technology to many major ISP's, and providers of mobile Internet as well.[33]
3. Crisp Thinking[34]:
   Crisp Thinking, makers of the IMsafer technology discussed in the Client side software section, are part of the next generation of parental controls technology that will be more nuanced than the current all-or-nothing approach to content filtration. Their programs allow for behavior analysis of each individual user in MMOG's or other online environments, and provide a quantified breakdown of the degree to which users have had inappropriate interactions with other users. Their systems use pattern recognition software over extended periods to determine whether interactions between users may take on potentially harmful aspects of cyber-bullying or sexual predation. Their system can also block messages containing objectionable content in real-time before the recipient sees them.
4. ChatS.O.S. is an Israeli company which provides real-time IM monitoring and filtering capabilities to parents, including the ability to block inappropriate messages from reaching their intended recipients.

Challenges

1. There is a lack of unifying international standards, or even general industry agreement about best practices or future goals.
2. It is difficult to strike a balance between complete certainty of age verification and the maintenance of user anonymity. Being able to identity a particular user as verifiably over a certain age entails collecting some sort of personal information about them. On the other hand, maintaining complete user anonymity might mean compromising the safety and interests of children, in addition to making companies legally liable for failing to obtain legal consent from some users who were unable to give it in the first place. How can we determine where to draw the line?
3. One of the main concerns with virtually all methods of age verification is the storage and protection of data. As techniques of age and identity verification become more advanced, both the likelihood and the risk of information theft increase. The more PII stored in various

---

[32] https://parentalcontrols.aol.com/parconweb2/home/landingPage.jsp?encodedOrigUrl=http%3A%2F%2Fparentalcontrols.aol.com%2Fparconweb2%2Fhome%2FviewMain.do

[33] http://www.rulespace.com/customers.php
http://www.rulespace.com/parental.php

[34] http://www.crispthinking.com/technology.htm

places, the easier it becomes for hackers to gain access; likewise, the more we become reliant on various PII-dependent systems to work and function in the online world, the greater the potential becomes for identity theft to cause damage.

COPPA 2.0

A. Though an FTC review of COPPA legislation had originally been scheduled for 2015, the FTC has accelerated the process to issue a review and potential suggested updates of COPPA in mid-2010. In the interim, many states have taken the matter into their own hands and brought the matter up before state legislative bodies. Maine, for example, passed a law in early 2009 requiring verifiable parental consent to collect and use PII, not just from children under the age of 13, but all minors 18 and under. The Attorney General indicated that it is legally flawed and would not be enforced. As of the publication of this report, the Judiciary Committee had voted to repeal the act, making a repeal in the near future very likely, though the full legislature has yet to vote on the issue. The Chairman of the Judiciary Committee of the Massachussetts State Legislature stated that "…the committee felt that this was an important issue that needs to be addressed, but that the current statute conflicts with existing Federal law, and there is no way to change the text to bring it into conformity."[35]

[35] http://www.research-live.com/news/government/maine-legislature-votes-to-repeal-child-data-law/4001204.article

Conclusion

Conventional wisdom states that innovation takes place so quickly on the Internet that new developments are practically obsolete as soon as they are released. Nevertheless, conclusions drawn from two of the leading comprehensive reports issued on this topic continue to hold true today, eleven and thirteen months since their respective releases. Presented here are important insights from reports by the Berkman Center at Harvard Law School an European Commission's Information Society & Media Directorate-General.

From the Report of the Internet Safety Technical Task Force at the Berkman Center for Internet and Society at Harvard Law School:

"The Technology Advisory Board and the Task Force note that almost all technologies submitted present privacy and security issues that should be weighed against any potential benefits. Additionally, because some technologies carry an economic cost and some require involvement by parents and teachers, relying on them may not protect society's most vulnerable minors."

"The Task Force remains optimistic about the development of technologies to enhance protections for minors online and to support institutions and individuals involved in protecting minors, but cautions against overreliance on technology in isolation or on a single technological approach. Technology can play a helpful role, but there is no one technological solution or specific combination of technological solutions to the problem of online safety for minors. Instead, a combination of technologies, in concert with parental oversight, education, social services, law enforcement, and sound policies by social network sites and service providers may assist in addressing specific problems that minors face online. All stakeholders must continue to work in a cooperative and collaborative manner, sharing information and ideas to achieve the common goal of making the Internet as safe as possible for minors."

From the "Background Report on Cross Media Rating and Classification, and Age Verification Solutions, by the European Commission's Information Society & Media Directorate-General:

"A number of Age Verification Solutions are available for the protection of minors within the EU, some of which were presented at the Safer Internet Forum. In some Member States there are legal requirements for their use. There is an overall consensus, however, that existing technologies are not sufficiently effective and should not be used to replace educational efforts, parental control and other means of protecting minors online. Despite the shortcomings, there is a certain market acceptance for their use. Concerns were also raised about the false sense of security that might be provided and the adverse effects on safety this might have. Privacy and data protection were also raised as important issues. Additional research is needed, and a standard for Age Verification can be pursued."

In conclusion, the authors of this report would like to leave their readers with some thoughts on the tools and resources presented in this paper:

- The use of certain methods of age verification or authentication may result in an increase of the detrimental effects of fraud, especially phishing.
- Many commonly used methods are reliant on data collected for purposes other than age verification.
- There are some methods that might easily be circumvented.
- Some technologies may give parents a false sense of their child's security online.
- Some technologies have the potential to be subverted for illegitimate purposes, such as monitoring one's spouse.
- In the name of protecting privacy, parents may be required to divulge more personal information about their children. Though many emergent technologies have shown promise in being able to protect our children from the risks of the Internet, it is important to remember that each also has its shortcomings. Most systems can be effective in proving someone is an adult, but not that they are a child of a certain age.

At this point in time there appears to be no all-encompassing single solution, nor silver bullet that protects privacy and ensures safety for children. Any realistic current efforts must include a focus on educating both parents and children, in addition to the use of technology. We must find a way to provide parents with the resources to make this new world of technology more easily comprehensible, and help them more effectively mentor in their children's online experience.