

Internet Safety Technical Task Force Technology Submission

Aristotle International, Inc./ John Phillips
<http://integrity.aristotle.com>

JULY 21, 2008

ABSTRACT

Last year, 29,000 Registered Sex Offenders (RSOs) were discovered on MySpace, after initial reports that the number was only 7,000.¹ The number is now 50,000, and reflects only those registering with truthful information.²

Aristotle seeks to limit risk to minors that stems from users – particularly RSOs – registering with false information on social network sites (“SNS”). Aristotle’s Integrity™ is a suite of widely accepted identity verification (IDV), age verification (AV), and Knowledge-Based Authentication (KBA) solutions. Based primarily on instant verification of government-issued ID, the service operates across platforms, including online, interactive voice response (IVR), wireless and other mobile devices.

Keywords

Aristotle, age verification, ID verification, authentication

Functional Goals

Limit/prevent harmful contact between adults and minors

Limit/prevent minors from accessing inappropriate content on the Internet

Limit/prevent minors from accessing particular sites without parental consent

Limit/prevent harassment, unwanted solicitation, and bullying of minors on the Internet.

Limit/prevent adult solicitation of minors who willingly participate (solicitation not “unwanted”).

[REMAINDER OF FIRST PAGE INTENTIONALLY LEFT BLANK PER INTERNET SAFETY TECHNICAL TASK FORCE TECHNOLOGY SUBMISSION TEMPLATE (“INSTRUCTIONS, FORMAT INFORMATION”)]

PROBLEM INTRODUCTION

The primary focus of this Task Force is safety for minors on social network sites. Aristotle is focusing on:

Growing Number of Registered Sex Offenders on SNS

The number of identified RSOs on SNS continues to rise. The problem is considered serious enough that MySpace matches its lists to multi-state registries of RSOs, and deletes the RSO profiles (“RSO Removal”).

It is self-evident that RSOs cannot be identified/removed if allowed to register with false data. As the Kentucky AG recently stated, “They swept over 50,000 registered sex offenders off of MySpace and ladies and gentlemen we’re catching the dumb ones. We’re catching the ones using their registered sex offender email to get on MySpace”.³ We cannot know how many more RSOs are registered under false credentials, beyond the confirmed 50,000. Integrity complements RSO Removal, and shores up this obvious weakness in that process, by providing more confidence that registrants are who they say they are. Otherwise, the RSO Removal process may actually increase the risks to minors by creating a false sense of security, when in truth the process is catching only the “dumb” RSOs.

Dangers to Minors From Posing as Adults on SNS

Teens 15-17 years of age may be the most prone teens to take risks involving privacy and contact with unknown people online.⁴ When minors hold themselves out as adults and engage in risky sexual behavior on SNS (including entering adults-only areas), they create risks for themselves, and for adults who have the right to seek relationships on SNS with those reasonably believed to be adults. Anonymous registration may even provide encouragement to some who might not otherwise behave dangerously but for the fact that they believe their true identities are unknown.

Cyberbullying/ Harassment/Unwanted Solicitation

An exploratory study states that 29% of 10-15 year-old survey respondents who said that using SNS was one of two activities they spent most time doing when online, reported unwanted sexual solicitation.⁵ If SNS users know that cyberbullying/ harassment/unwanted solicitation can be traced back to them and cannot be conducted with anonymity, this is likely to have a deterrent effect on such conduct. Requiring truthful registration information, and verifying it, should limit this type of misconduct.

Age-Restricted Ads to Minors on SNS

Many presume that most SNS registration information is false. As SNS become ad delivery systems, ads for alcohol⁶, gambling, etc. across SNS may be improper⁷. Verification permits delivery of such ads with more assurance that they are not delivered to an unacceptable number of minors, in violation of codes or standards.

Obtaining Parental Consent for Minors to Join

Under principles similar to the Child Online Privacy Protection Act of 1998 (“COPPA”), to register as a minor

on an SNS, some mechanism must be in place to provide notice to a verifiable adult. Under COPPA, whenever personal information is obtained online from a child under 13, a “sliding scale” of proof of parental consent is needed depending on the information sought and the purpose for which it is sought. Aristotle’s Integrity system is the methodology used in the FTC-approved Privo-Lock system for obtaining “verifiable parental consent” under COPPA.⁸

PROPOSED TECHNICAL SOLUTION

How IDV/AV works

IDV means confirming that a person is who he or she claims to be. AV means verifying the person’s age. Client’s application sends user information collected at the website or by some other means for instantaneous IDV/AV. Integrity instantly confirms the information against public record data of US and international citizens. Integrity sends the client’s application a numeric match code (MC), to allow the client to gauge how closely the end-user data has been matched. This MC is generated by taking the data provided by an individual, and cross-checking the data against Integrity databases. Note: the client can select the degree of security by picking MCs that are appropriate for the industry, the law, the site’s objectives, and the availability of the appropriate data.

Integrating the Instantaneous Online Match Service

1. Any platform able to communicate via HTTP protocols can communicate with the online matching service.
2. The client application obtains the user information (For example: name, address, date of birth).
3. The application constructs the URL string with the user’s information and sends it to Integrity for processing. The method for calling the URL within any application will vary, depending on the language used by the application. Nothing needs to be installed on the client. The application code makes a call to Integrity using the syntax provided. This is a secure http call and no information is ever passed back to the application that the consumer has not provided.
4. In all cases, the data is processed against separate, segregated databases including government-issued ID, credit headers, terrorism watch and multi-state RSO lists.
5. The result is returned in this form as:
tid=DUF2JH30142071767476&mc=0&errcode=&errdesc=
6. The application parses the string to obtain the MC.
7. With a valid MC, the application can grant access.
8. Integrity provides a deduplication service to show how many times someone attempts to gain access before submitting their true information. If a user fills in false data on a form to gain entrance, the submission is not validated. They may try again with different false data and fail. Once they submit their correct data they can be verified. In this scenario, one user made three attempts (two with false data) before authentication. This is not viewed as three separate attempts with a 33% success rate; it was 100% successful. In addition, for those that may not be able to get the correct information to match, clients can use off-line verification such as faxing in a valid ID for matching.

Customers also can verify users by collecting the data and sending it in a batch to Integrity for processing and return to the client within 24 hours of receipt.

Use Cases Integrity users include major motion-picture studios, wineries, brewers and distillers, tobacco vendors, financial services firms, event management agencies, transportation security and other government agencies. The success rate for a video gaming network site using the service with deduplication, increased from 60% to 85%.

Effectiveness. Approvals directly correlate with the accuracy of information submitted. A web form needs to have separate fields for first name, last name, address, date of birth, etc. If the person is invalidated, there should be instructions (e.g., use maiden name or previous address if recently moved). If a person wants to be validated, the success rate is extremely high. When a company couples AV/IDV with KBA, an additional level of protection is achieved. While a child may be able to steal a parent's credit card or some other form of ID, KBA provides a higher level of protection by asking security questions that would pertain to that real individual. It also helps prevent a sexual predator from creating a false identity to register. The effectiveness also is measured by the increasing number of companies that are switching to Integrity to help insure that the right people are gaining access to their sites and products. Reports can be generated by the clients that show success rates. Aristotle support will help analyze and suggest ways to improve success. Percentages of completed verifications may or not be a good indicator of effectiveness. Lower raw approval percentage may reflect the system's success in screening out bogus users. *See also* "Analysis of Strengths/Weaknesses" below.

Analysis of Strengths/Weaknesses

"Strengths"

Better Match Rates. Integrity provides better match rates at the levels selected by the site, with least consumer resistance, by using redundant databases consisting of near-universally held government-issued ID for instant IDV/AV.

Guaranteed Verification. Integrity is the only entity with sufficient confidence in the protections afforded by its methodology to guarantee the verifications. Integrity will indemnify against fines or legal fees resulting from any incorrect verification, up to \$1 million, as per contract.

Legal Compliance. The methodology meets or exceeds legally or industry mandated IDV/AV requirements (e.g., COPPA, tobacco marketing and sale laws, motion picture and alcohol marketing guidelines.)

Reputation. Integrity is well-respected and has never been tainted with cases of data misappropriation, suits alleging improper data use or violations of FCRA or DPPA, or enforcement actions by the FTC, SEC, or State AGs.

Global Coverage. Integrity manages a complete database of the 50 United States, US territories, and over 1 billion records on international individuals in 153 countries.

Reliability. Redundant data centers are maintained in the US and UK, to comply with US and EU privacy standards.

Proven and Accepted Services. Integrity is widely used by multiple industries and has successfully performed more than 70 million verification transactions.

Scalability. Integrity has been tested to handle 50,000 transactions per hour with burst rates above that. 99% of all Integrity verification results are completed within 3 seconds following the consumer data submission. With advance notification, Integrity arranges for surge capacity to accommodate significant load estimated in response to specific marketing events. For clients purchasing TV advertising in conjunction with the Super Bowl, temporary surge capability was benchmarked to handle over 10,000 simultaneous transactions.

Data Security. This is established through leading commercial security software and internally developed security. Administrators and Associates are assigned and required to use a unique user ID and password to gain access. Shared or group user IDs are not permitted in production systems. Integrity uses state-of-the-art firewall and intrusion detection equipment to protect and monitor any and all traffic on the network. Firewall policies throughout the organization are centrally managed. All traffic (afferent and efferent) to and from the internal network goes through the firewalls. Data privacy is attained through the use of Secure Socket Layer and requiring encryption (128-bit or better). Afferent and efferent web access is authenticated and logged.

"Weaknesses". IDV/AVKBA are incomplete solutions to the problems addressed, and should be used as part of a layered approach. These solutions do not prevent user sharing of credentials. In the case of parental consent for minors to register as minors, obtaining proof of an actual parental relationship is different and more difficult than obtaining the consent of an adult (as the COPPA model shows). Integrity's US-based coverage (all 50 states and the territories) is more robust than its non-US coverage. Our database comprising 1 billion records on international individuals in 153 countries does not cover all countries, or may not cover some countries with the same amount of redundancy as our US-based coverage. To obtain the broadest possible non-US coverage, Integrity can and will work with other providers to establish a layered solution.

Implementation Requirements and Technical Standards

No specialized user aptitude, and no additional hardware or software is needed. Integrity uses standard HTTP protocols through TCP/IP sockets for processing. Integrity accepts requests using HTTP GET or HTTP POST methods. A technical manual is provided to clients under an NDA.

Technology's Reliance and Use of Law and Policy.

Privacy and other legal considerations are addressed through user's express consent for IDV/AV, and, in case of SNS such as MySpace, through user's warranty and representation that registration information is true and correct.⁹ Integrity thus serves to mitigate risk-creating fraud. Unlike other verification services, Integrity operates without returning information from Integrity databases. Nothing from the user is added to Integrity databases.

Social Security Numbers (SSNs) are not required. Only a numeric MC is returned. Aristotle does not commingle its various public record databases, and does not create dossiers on users. Integrity is transparent, utilizing reliable, widely-accepted government-issued ID and other public records to verify identity and age rather than questionable, “third-party” sources or databases. *See also* COPPA consent considerations, discussed above.

Technology’s Viability in US and International Contexts

See “Analysis of Strengths/Weaknesses” above.

Effectiveness to date/ “Failures” of the technology. *See*

“Analysis of Strengths/Weaknesses” above. While no system will be completely perfect, Aristotle’s Integrity solution is an established method of securing access.

EXPERTISE

Integrity believes it has processed more verifications for more customers than all other AV/IDV vendors, combined. In vertical markets that include major Hollywood studios, financial institutions, casino operators, wineries, distillers, tobacco, , and electronic game manufacturers and retailers, Integrity holds a commanding market share for IDV/AV by means of a database check. Integrity was first to offer such processing in real-time without requiring an SSN. Integrity is the only service that insures and indemnifies its clients against fines or fees related to an unintentional transaction with a minor. IDV/AV constitutes 100% of Integrity business. Since its inception 7 years ago, no Integrity client has been fined or prosecuted for underage access after adopting the service. Since 2006, Integrity also has maintained a self-exclusion registry for problem gamblers to help keep them from entering gaming sites. *See also* “Strengths” above, in “Analysis of Strengths/Weaknesses”.

COMPANY OVERVIEW/MANAGEMENT

Integrity is the IDV/AV offering of Aristotle, the leading non-partisan supplier of compliance services to elected officials in the US. Aristotle offers its clients 24x7x365 technical support. Aristotle is a profitable, privately held company. It was founded 25 years ago by CEO John Aristotle Phillips and his brother, company President Dean Aristotle Phillips. John Phillips graduated with a degree in Aerospace Engineering from Princeton University. Dean Phillips graduated with a degree in Electrical Engineering from MIT. They maintain operational control with a senior management team that oversees over 100 employees working at the company’s headquarters in Washington, DC, and in Atlanta, Salt Lake City, Toronto, London, and San Francisco. In 1999, they accepted venture capital shareholders including Rupert Murdoch’s investment group and Bill Hambrecht.

BUSINESS MODEL OVERVIEW

Integrity is priced on the basis of successful verifications performed, with the cost/verification ranging from \$.10 to \$1.00 for electronic verification, with a surcharge if the consumer cannot be electronically verified and manual or telephone verification of government-issued ID is

requested. The price includes indemnification of up to \$10,000 per incident and \$1 million per client, should an incorrect verification result in fines for underage access. A deposit of anticipated annual usage is made on signing. There is no set-up fee. The vast majority of Integrity clients are global companies that are seeking to verify the identity or age of website visitors with the least friction so as to mitigate risk. Aristotle has provided Integrity services to non-profits at no charge and to start-ups at a discount until such time as they can afford the service.

FOR MORE INFORMATION

See <http://integrity.aristotle.com>. For more news on SNS and sex offenders, see <http://integrity.aristotle.com/sns-rso>.

CONTACT INFORMATION

John.Phillips@Aristotle.com (415-440-1102), 205 Pennsylvania Avenue, SE, Washington DC 20003

CERTIFICATION

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

¹<http://www.foxnews.com/story/0,2933,290660,00.html>

² <http://www.wave3.com/Global/story.asp?s=8437905>

³ *Id.*

⁴ Wolak *et al*, “Online ‘Predators’ and Their Victims”, *American Psychologist* (February-March 2008) at 115.

⁵ Ybarra and Mitchell, “How Risky Are Social Networking Sites?” *Pediatrics*, January 2008, Table 3. The authors warn that “caution should be used in interpreting this small amount of research about a new phenomenon”. (“Online ‘Predators’ and Their Victims”, *supra*, at 118)

⁶http://www.nytimes.com/2008/05/28/business/media/28adco.html?_r=1&partner=rssnyt&emc=rss&oref=slogin, “For Coors Light, a Night Out That Begins on MySpace”

⁷<http://www.beerinstitute.org/BeerInstitute/files/ccLibraryFiles/File/00000000707/CCRB%20Annual%20Report%202007.pdf>, Beer Inst. Advertising Code, Guideline 3c.

⁸http://www.ftc.gov/privacy/privacyinitiatives/childrens_shp.html Letter Approving Privo, Inc’s Safe Harbor Program Application Under COPPA; and Privo, Inc. Safe Harbor Application

⁹<http://www.myspace.com/index.cfm?fuseaction=misc.terms>, § 1.