Open Access

Open Journal of Information Systems (OJIS)
Volume 2, Issue 1, 2015

www.ronpub.com/journals/ojis
ISSN 2198-9281

Using Nuisance Telephone Denial of Service to Combat Online Sex Trafficking

Ross A. Malaga

Department of Information Systems and Operations Management, School of Business,
Montclair State University, 1 Normal Ave. Montclair, NJ 07869, USA,
malagar@mail.montclair.edu

ABSTRACT

Over the past few years, sex trafficking has been linked to online classified ads sites such as Craigslist.com and Backpage.com. However, to date technology-based solutions have not been used to attack classified ad sites or the advertisers. This paper proposes and tests a new approach to combating online sex trafficking promulgated via online classified ad sites – nuisance telephone denial of service (TDoS) attacks on the advertisers. The method of attack is described and implications are discussed.

TYPE OF PAPER AND KEYWORDS

Short communication: *telephone denial of service, mobile phone, World Wide Web, sex trafficking*

1 INTRODUCTION

Online classified ads have provided a method for buyers of sex (known as Johns) to find providers of sex (sex workers). Authorities are also concerned that some of the ads posted on these sites involve sex trafficking and/or minors. While there is no universal definition of sex trafficking, in general it describes any situation where the trafficker (known as a pimp) uses force, coercion, or other forms of control in order to require a person to engage in sex work. Minors engaged in sex work are always considered to be trafficked. The focus of this research is on sex trafficking as opposed to independent sex workers - those who have chosen to engage in sex work without coercion or control from another.

Over the past few years legal, policy, and advocacy approaches have been used to try to convince classified ad sites (e.g., Craigslist, Backpage, etc.) to remove their commercial sex related ads (these ads typically appear under categories such as adult services, escorts, massage, body rubs, etc.). These approaches have had only minor success and suffer from major limitations (as detailed below).

Until recently the computer science and information technology fields have not been applied to the problem of combating sex trafficking promulgated via online classified ads. This has begun to change. For example, Mark Latonero has conducted extensive research into the role of technology in human trafficking, calling particular attention to the relationship between mobile devices, classified ad sites and sex trafficking [11] [12]. However, to date, technology-based solutions have not been used to attack classified ad sites or the advertisers. This paper proposes, and tests via a proof of concept, a new approach to combating online sex trafficking

promulgated via classified ad sites – nuisance telephone denial of service attacks (TDoS) on the advertisers. In developing this approach already existing technologies and methods are used, but they are combined in a unique manner in order to tackle the problem of online sex trafficking.

2 BACKGROUND

Online classified ad sites, such as Craigslist.com and Backpage.com, have a long history of involvement in sex trafficking. In 2009, Craigslist began charging a fee for posting ads in its erotic services (later adult services) section. Under pressure from law enforcement and other interest groups, Craigslist agreed to close its adult services section in 2010. The revenue generated from this section of the site is estimated to have been about $3.7 million per month [1]. With the shut down of the adult services section of Craigslist, at least some of the ads that appeared in that section have now gone to Backpage.com.

According to AIM Group (an interactive media and advertising consulting firm) [1], in August 2012 Backpage had 3.9 million unique visits and published 88,895 listing for escorts and body rubs. AIM also estimates that Backpage receives about $2.3 million in monthly revenue from just 23 of its almost 400 total US market sites and that Backpage is the revenue leader among similar web sites.

Although Backpage has refused to shut down its adult service ads, it has agreed to limited cooperation with the National Center for Missing and Exploited Children (NCMEC). According to testimony from Ernie Allen [14], President and CEO of NCMEC, in 2011 Backpage referred 2,695 cases suspected of involving the sex trafficking of children. In an interview on CNN [6], Liz McDougall, a lawyer for Backpage.com, indicated the site first scans ads for 25,000 key words and terms and then an internal team of about 100 reviews the ads and identifies approximately 400 ads to be forwarded to NCMEC every month.

The speed at which advertisers post ads and the redundancy of ads across sites makes the manual policing of ads a daunting task. Monitoring ads and prioritizing those that are more likely to involve sex trafficking or minors is difficult. In the classified ads, age is self reported and images tend to be “fake” or altered.

Given the significant scope of sex trafficking and the relative ease of using classified ad sites in its promulgation, the objective of this paper is to review the problems with current technology based approaches to combating sex trafficking via online ads. The author details and tests a new approach - telephone denial of service attacks (TDOS) against the phone number appearing in the ads.

3 POTENTIAL SOLUTIONS

In attempting to deal with online sex trafficking law enforcement personnel have a number of options. First, law enforcement can monitor sites such as Backpage to setup undercover stings to catch those buying and selling sex. Many jurisdictions have been doing this for some time and it has become a standard approach [17]. However, this method is extremely resource intensive and only catches a few people at a time. Furthermore, the difficulty of accurately identifying ads involving trafficking victims, particularly minors, among the multitude of ads posted on these sites hinders the potential reach of this approach as a method of policing online sex trafficking.

Second, law enforcement personnel can attempt to convince the site running adult services ads to shut down that part of the site. While this approach worked with Craigslist, the significant amounts of money to be made by allowing adult services ads is a strong incentive to keep them. As has been noted above, Backpage generates about $32 million per year in revenue from its adult services ads [1]. Thus far, coercive attempts to persuade the owners of Backpage to shut down its adult-services section have failed. In addition, legislative efforts have also failed. In a recent case [20] Backpage was successful in fighting the newly proposed SB 6251 law, which sought to limit its ability to publish adult-services ads.

In addition to the revenue challenge, there are also problems of displacement. The first problem of displacement involves the ability for ad placers to move their ads to another site, which was observed in the Craigslist shut down. As reported by AIM, nearly two years after Craigslist shut down its adult services section, Backpage’s revenue from such ads jumped by 38.2 percent [1]. Given the ability of ad placers to find alternative sites, in the absence of an industry wide ban, this approach becomes the equivalent of combating online sex services advertising whac-a-mole.

Another problem of displacement has to do with ads going from well-known sites that law enforcement can monitor more easily to underground sites that are more opaque and difficult for law enforcement to penetrate. Law enforcement officers seem to be of two minds about whether the shut down of sites like Craigslist and Backpage is desirable. While some in law enforcement have benefited from cooperation with Craigslist and Backpage, others argue that shutting down the sites is the right thing to do [12].

Third, appropriate law enforcement agencies might launch a distributed denial of service (DDoS) attack on

the site as a whole or just the adult services portion of the site. It should be noted that it might not be possible to target only the adult services sections of many sites as they reside on the same servers as the main site. This approach would render the site unusable to those seeking to post an ad or to engage the services of a sex worker. There are two main drawbacks to this approach. The first is that taking the site down via a DDoS attack might cause the advertisers to flee to another site – setting up the same whac-a-mole problem discussed above. In addition, the legality of such an attack is questionable.

Finally, instead of targeting the site for a DDoS attack, the author suggests it might be more effective to target those posting the ads with a nuisance telephone denial of service attack (TDoS). A TDoS attack occurs when an attacker floods a phone number with incessant calls and/or text messages making the number unreachable by legitimate callers [15]. Attackers typically use free PBX software, such as Asterisk (http://www.asterisk.org/) and Internet telephony to launch TDoS attacks. In fact, some attackers are even advertising their services (about $20 per day) on hacker sites [3]. A nuisance TDoS attack needs not make the number unreachable as the goal is to merely annoy the owner of the phone to a point where he or she stops responding to incoming calls and texts.

This type of attack has many advantages over the other solutions detailed above. First, since it targets those posting the ad, it is site agnostic – so it can be used in conjunction with sex services ads placed on any site. Second, it disrupts the advertisers' main means of communicating with buyers, namely mobile phones. Third, it is difficult to defend against a TDoS attack, especially attacks targeted at individual phones. Finally, as detailed below, a TDoS attack is relatively easy and inexpensive to setup.

4 TDoS Details

Traditionally, TDoS attacks have been used in conjunction with some type of other fraud or criminal behavior. The goal is to deny the user the ability to receive any legitimate calls. For example, an identity thief might use TDoS to flood the victim's phone line so that financial institutions cannot contact the victim to verify activity [19].

In order to combat online sex trafficking a complete denial of service is not required. Instead the goal is to cause a nuisance to such an extent that it makes advertising online, which requires posting a contact phone number, infeasible. In fact, allowing some legitimate calls or text messages through might enhance the nuisance factor as the target cannot determine beforehand which calls are from potential buyers (johns) and which are just nuisance calls.

The TDoS approach to combating online sex trafficking has three main technical elements. The first is using a Web crawler to find all of the ads on a given site and scrape the content on them. Second, is the automated harvesting of the phone number from the body of the posted advertisement. The third is using the number to implement the TDoS attack. The entire process is detailed in Figure 1.

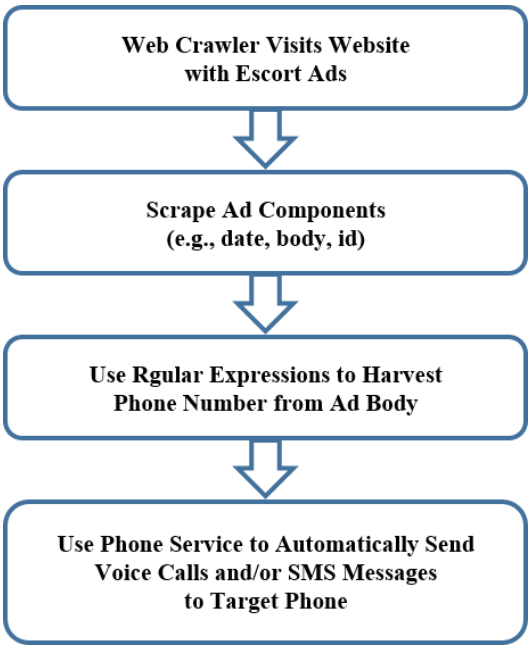

Figure 1: The TDoS Proccess

4.1 Finding the Ads

A standard Web crawler can be used to navigate through the various pages of interest on a particular Website that contains sex trafficking ads. These sites can be found via simple Google searches for terms such as "escort ads" or "local escorts". On each ad page the ad details (ad id, date, ad body) are scraped and stored in a database or processed in real time. The scrapping algorithm needs to be adjusted for each Website as the format of each is different. For example, on Backpage.com the posting date and time are contained within a DIV class called AdInfo. On LocalEscortPages.com the date and time occur immediately after the Posted On: text. Since date and time are useful, but not necessary for the TDoS approach, the entire page can be scraped if needed.

4.2 Phone Number Harvesting

The main problem in automating the harvesting of the phone number is that they are posted in a variety of

formats. For example, some may post the phone number as 555-555-5555, while others may use (555) 555-5555 or 555 555 5555. In addition, in some cases those advertising sex services attempt to obfuscate the number by using text – 5 five 5 or 5I5 (that's an I not a 1) for example. It should be noted that there is a practical limit to this type of obfuscation as advertisers need the johns to easily decipher the number.

Extracting a number pattern from within a larger body of text is relatively easy. Many programming languages allow for the use of regular expressions to match specific number patterns. The concept of regular expressions dates back to 1956 [9]. The concept of pattern matching via regular expressions has been incorporated into core UNIX functions (such as *awk*) and is a core feature in the PERL programming language [18].

If TDoS attacks prove successful, it is anticipated that advertisers and publishers (e.g., Backpage.com) might attempt to hinder phone number harvesting. Two methods that might be tried are placing the number within an image file and using CAPTCHA technology.

Fortunately, there are many algorithmic solutions for finding text within an image, known as text information extraction (TIE) [7]. These typically involve some form of preprocessing, such as localization to bound the text area, and filtering to remove color and background noise. The text area is then enhanced and fed through an optical character recognition (OCR) system.

Advertisers might attempt to use some form of CAPTCHA (Completely Automated Public Turing test to Tell Computers and Humans Apart) to obfuscate the phone number. This would be risky on their part, however, as CAPTCHA images are sometimes difficult to read – which might deter potential johns. Mori and Malik [13] have detailed a method for breaking visual CAPTCHA. More recently, researchers at Stanford University [4] have developed a program called Decaptcha, which is able to break the most widely used CAPTCHA schemes anywhere from 1% to over 50% of the time.

If advertisers develop an obfuscation method that cannot be broken easily algorithmically, then law enforcement may need to use human resources to harvest the phone numbers. This can be done internally, by law enforcement agents, or outsourced on sites like Amazon's Mechanical Turk (MTurk).

The phone numbers would need to be harvested (either automatically, manually, or some combination) on a continuous basis and fed to the voice and SMS attack systems.

4.3 TDoS Voice Attacks

For the TDoS attack it is important to cover both voice and text messaging (SMS). For voice, a programmable PBX with phone lines (either hard line or VOIP) or multiple VOIP lines (e.g., Skype) are required. Multiple lines are needed for throughput (ability to make multiple simultaneous calls). The programmable PBX, which can be a physical PBX or software based, is used to obscure the caller ID in order to prevent blocking by the subject of the attack. With a programmable PBX system the attacker can use the same phone lines, but spoof the caller ID with each call – making them appear to be from different phone numbers.

The precise number of lines required would depend on how many phones are to be attacked, the rate of attack, and the dial time required by the system. For example, if the aim is to attack 20 phones simultaneously with an attack rate of two calls every minute, this would require 40 calls every minute with a system that can dial, connect, and hang up every 15 seconds. This is a realistic estimate based on a small test; it is presumed that the user would hang up if the caller does not. In this scenario, 10 phone lines would be needed, as each line would be capable of making 4 calls per minute. The number of lines would be reduced, of course, with a decrease in the number of phones to attack, reduction in attack rate, or increase in connection time.

According to law enforcement personnel running undercover sting operations [2], sex services ads often receive an almost immediate response at the time the ad is placed, with further responses decreasing over the next few hours. In areas where this tendency holds up, the goal would be to attack the phone as soon as the ad is posted and continue the attack at a high rate for at least the next hour. The attack could continue at a slower pace after that. Based on data collected from Backpage.com, in high volume geographic areas (like New York City) the rate of new ads can run as high as 300 per hour. Since the goal of the attack is not to render the target's phone useless for calls, but rather to harass or annoy the target, a high number of connections per minute are not needed. For harassment purposes, it is estimated that about 2 to 3 calls per minute would be sufficient. Therefore, this attack could be done with about 150 lines for a low-end attack.

It is important to consider that the target of the attack might allow the phone to go to voice mail, calling back those potential "dates" who leave a legitimate message. In this case, one goal of the attack would be to flood the voice mailbox. This could be done with hang-up calls, but a more efficient method might be to use a prerecorded message. The message could even contain

instructions for calling a hot line or law enforcement number.

4.4 TDoS SMS Attacks

As text messaging is often used to arrange meetings, it is important to deny this means of communication. Fortunately, launching a TDoS against text messaging is fairly simple. First, the attacker could use the mobile number to lookup the carrier (e.g., Verizon, AT&T, etc.). There are numerous sites that provide lookup databases; APIs are also available. Each carrier maintains an e-mail domain that can be used to send SMS messages to a specific phone. For example, if the advertiser's phone number is 555-555-5555 and it is determined that the carrier is Verizon, the attacker could send a text message by e-mailing 5555555555@vtext.com. Clearly, the attacker would need to vary the sending e-mail address so the attack would not be blocked easily. The exact number of messages that would need to be sent in order to deter online sex advertising is not known. However, if the attack used random texts that sounded legitimate, the nuisance factor would become very high.

4.5 TDoS Legal Issues

The legal issues surrounding TDoS appear to be somewhat different than traditional DDoS attacks, as TDoS is not dealing with developing botnets or attacking computer systems (although it may be argued that a smart phone is computer system). In the United States TDoS attacks appear to fall under the Telephone Consumer Protection Act (TCPA) of 1991 (see http://www.fcc.gov/guides/unwanted-telephone-marketing-calls). This act covers unsolicited marketing calls. It also covers calls made with an autodialing system. However, it explicitly excludes calls made by non-profit organizations and calls and messages placed with prior permission. Advertising online and posting a phone number may constitute prior permission. Additional rules under the Act state that callers must provide caller ID information, even when prior permission has been given.

It is not clear whether and how the Act would apply to law enforcement agencies. Non-profit organizations appear to be exempt from the law. In theory, an advocacy group may be allowed to initiate a TDoS attack legally. Even if the organization was not exempt, it is not likely that the targeted party would initiate a complaint under the Act.

In addition, the law clearly only applies to TDoS attacks that occur in the United States. Other nations may or may not have similar laws. Therefore, it might be useful for law enforcement and/or advocacy groups to test the TDoS concept outside of the United States.

5 PROOF OF CONCEPT

Due to the vague legal status of TDoS in the United States a full scale test could not be conducted. Instead the authors developed a proof of concept in order to test each of the components of a TDoS attack on a small scale. This test was divided into two main parts; the automated extraction of phone numbers from Backpage.com escort ads, and the automated voice and SMS attack on a mobile phone.

First, the authors developed a PHP program to crawl the Backpage.com escort ads, extract the ad components (e.g., ad id, date, body, etc.) and store them in a relational database. A convenience sample of 95,940 ads were successfully crawled, extracted, and stored.

Another PHP program was developed that uses regular expressions on the body of each ad in order to extract the phone number. We began with regular expressions that searched for standard phone number formats such as (555) 555-5555, 555-555-5555, 555 555 5555. Using the standard regular expression formats we were able to extract 65,857 phone numbers from our sample – for a success rate of 68.64%.

We used two main methods to improve our success rate. First, we used a search and replace algorithm to replace all text numbers (e.g., one, two, three, etc.) with actual digits. We also replaced the letter o with the digit 0 and the letter l with the digit 1 as this was a popular method of obscuring the actual number. This allowed the system to handle phones numbers such as 6oo one41seven (this is an actual example that has been slightly altered). Second, we added additional regular expression patterns for more obscure phone number formats. For example, (555)555-5555 (no spaces) and 555--555--5555. The combination of replacing letters and words with digits, and additional regular expressions allowed the extraction rate to increase to 88.58%.

Finally, we ran the extraction algorithm on a smaller subset of ads (300) in order to test the accuracy of the program. This was an important step as we would want to ensure the system is not dialing an incorrect phone number. The program extracted 273 phone numbers from the subset and these were checked manually to ensure accuracy. All of the extracted numbers proved to be accurate.

Next, the authors used Twilio (twilio.com) for voice and SMS attacks. Twilio was chosen due to its PHP API integration and relatively low cost. The voice service cost is $1 per month for each number, plus $0.015 per minute for each call. The SMS service cost is $1 per month for each number, plus $0.0075 per message to

send. Volume discounts are available. In addition, other services or using a private PBX might prove more cost efficient.

The ads in the subset of 300 were altered so that the original phone numbers were replaced by those under the control of the authors. In all cases the original formatting was retained. For example, if the phone number in the ad was 5one5 555 one2one2 then the new number might be 6one6 666 one2one2. The Twilio API calls were added to the PHP program so that the numbers extracted were called about every 30 seconds with rotating caller ID's. When the phone is answered a sample voice message is heard. This process was repeated for five minutes.

A similar process was used to test the SMS messaging attack capability. Again the modified harvested numbers were used for the attack. In this case a stream of text messages were sent about every 5 seconds. The attack was kept up for two minutes.

The success of this proof of concept shows that the idea of using TDoS as a nuisance attack on sex traffickers would work. Phone numbers can be automatically extracted from online ads with a high degree of success and accuracy. The estimated cost of launching such an attack in the New York City area would be about $150 per month for phone numbers and about $10 per hour for phone calls and another $14 per hour for SMS. While the monthly cost for an all out TDoS attack would run over $35K per month, this figure could be brought down through bulk pricing and timing attacks only when activity is high (e.g., evenings, weekends, holidays, etc.).

6 CONCLUSIONS

There are a number of challenges associated with the common approaches to combating online sex trafficking via classified ad sites. The TDoS attack discussed in this paper provides an alternative approach. The proof of concept conducted shows that such an attack can be launched in an automated format, with a high degree of accuracy.

The TDoS method is not without some concerns. First, it is clear that this type of attack can and has be used for other, less altruistic, purposes. TDoS attacks have already been launched against emergency response numbers [10] and have factored in extortion schemes [16].

Second, more research is needed to determine whether the TDoS approach may cause unintended harm to victims of trafficking or independent sex workers. For example, if a trafficking victim has reached out to a hotline or friend for help, attacking her phone might prevent a return call.

Third, TDoS may have unintended negative consequences if the phone number attacked belongs to the sex worker and not the trafficker (pimp). For example, in cases where the sex worker has a daily quota, the TDoS attack might make it difficult for her to meet her quota. Failing to meet a quota imposed by a pimp typically results in abuse. Therefore, the trafficker should be the main target of the attack. Fortunately, in a recent thesis, Kennedy [8] details a method for identifying ads that are more likely to have been posted by traffickers (as opposed to individual victims or sex workers).

Fourth, it is not clear if conducting a TDoS attack would be legal in the United States. In addition, it may be that the legality of such an attack depends on the entity initiating it (e.g., law enforcement). Until the legal issues surrounding TDoS are addressed a pilot program using this method to thwart sex trafficking cannot be implemented in the United States. However, a review of online sex trafficking and the applicable laws in other countries might find a suitable arena for a pilot test of TDoS.

Clearly, additional research among sex trafficking victims, survivors, and law enforcement on the potential impact of TDoS is needed prior to implementation. Finally, if proven to be effective in combating online sex trafficking, TDoS may prove a viable alternative to combat other forms of illicit behavior (i.e., drug sales, weapons sales, etc.) facilitated through the Internet, mobile devices and other networked technologies.

REFERENCES

[1] AIM Group: "August prostitution-ad revenue down slightly year-year", http://aimgroup.com/2012/09/20/august-prostitution-ad-revenue-down-slightly-year-to-year/, accessed March 4, 2015

[2] Anonymous: Interview with Anonymous Law Enforcement Officer. Conducted via telephone with the authors, 2012.

[3] Brook, C.: "Firm Sees More DDoS Attacks Aimed at Telecom Systems", http://threatpost.com/firm-sees-more-ddos-attacks-aimed-telecom-systems-073112, accessed on March 5, 2015.

[4] Bursztein, E., Martin, M. and Mitchell, J.: "Text-based CAPTCHA strengths and weaknesses", In *Proceedings of the 18th ACM conference on Computer and communications security*. New York, NY, USA, 2011.

[5] Cook County Department of Homeland Security: "Situational Awareness Alert – TDoS Attacks on Public Safety Communications", http://krebsonsecurity.com/wp-content/uploads/2013/04/DHSEM-16-SAU-01-LEO.pdf, 2013, accessed on March 5, 2015.

[6] Feyerick, D. and Steffen, S.: "A lurid journey through Backpage.com", http://thecnnfreedomproject.blogs.cnn.com/2012/05/10/a-lurid-journey-through-backpage-com/, accessed on March 5, 2015.

[7] Jung, K., Kim, K.I. and Jain, A. K.: "Text information extraction in images and video: a survey", *Pattern recognition*, 37(5), pp. 977-997, 2004.

[8] Kennedy, E.: "Predictive Patterns of Sex Trafficking Online", *Dietrich College Honors Theses*, Carnegie Mellon University, http://repository.cmu.edu/hsshonors/155, accessed on March 5, 2015.

[9] Kleene, S. C., Shannon, C., McCarthy, J.: "Representation of Events in Nerve Nets and Finite Automata", *Automata Studies*, Princeton University Press, pp. 3–42, 1956.

[10] KrebsonSecurity.com: "DHS Warns of 'TDos' Extortion Attacks on Public Emergency Networks", http://krebsonsecurity.com/2013/04/dhs-warns-of-tdos-extortion-attacks-on-public-emergency-networks, accessed on March 5, 2015.

[11] Latonero, M., Berhane, G., Hernandez, A., Mohebi, T., and Movius, L.: "Human Trafficking Online: The Role of Social Networking Sites and Online Classifieds", *Center on Communication Leadership & Policy: Research Series.* University of Southern California, http://technologyandtrafficking.usc.edu/report/, accessed on March 7, 2015.

[12] Lantonero, M., Musto, J., Boyd, Z., Boyle, E., Bissel, A., Gibson, K. and Kim, J.: "The Rise of Mobile and the Diffusion of Technology-Facilitated Trafficking", *Center on Communication Leadership & Policy: Research Series.* University of Southern California. http://www.ungift.org/doc/knowledgehub/resource-centre/USC-Annenberg-Technology-and-Human-Trafficking-2012.pdf, accessed on March 7, 2015.

[13] Mori, G. and Malik, J.: "Recognizing objects in adversarial clutter: Breaking a visual CAPTCHA", *IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2003.

[14] National Center for Missing & Exploited Children (NCMEC): "Testimony of Ernie Allen, President and CEO", The National Academies, Washington, D.C. Institute of Medicine Committee on Commercial Sexual Exploitation and Sex Trafficking of Minors in the United States. http://www.missingkids.com/missingkids/servlet/NewsEventServlet?LanguageCountry=en_US&PageId=4632, Jan. 4, 2012, accessed March 7, 2015.

[15] Peterson, J.: "Secure Telephone Identity Threat Model", https://tools.ietf.org/html/rfc7375, accessed March 5, 2015.

[16] Prince, B.: "DHS, FBI Warn of Denial-of-Service Attacks on Emergency Telephone Systems", http://www.eweek.com/security/dhs-fbi-warn-of-denial-of-service-attacks-on-emergency-telephone-systems, accessed March 5, 2015.

[17] Shively, M., Kliorys, K., Wheeler, K., and Hunt, D.: "National Overview of Prostitution and Sex Trafficking Demand Reduction Efforts. Washington, DC: National Institute of Justice," https://www.ncjrs.gov/pdffiles1/nij/grants/238796.pdf, accessed March 5, 2015.

[18] Vansummeren, S.: "Type inference for unique pattern matching." *ACM Trans. Program. Lang. Syst.* vol. 28, no. 3, pp. 389-428, 2006.

[19] Woodruff, B.: "Phony Phone Calls Distract Consumers from Genuine Theft", http://www.fbi.gov/newark/press-releases/2010/nk051110.htm, accessed March 5, 2015.

[20] Zollman, P. M.: "Backpage wins Wash-state adult-ad fight," http://aimgroup.com/2012/12/11/backpage-wins-wash-state-adult-ad-fight, accessed March 5, 2015.

AUTHOR BIOGRAPHIES

Dr. Ross Malaga is a Professor of Information Systems and Entrepreneurship at Montclair State University. He has over 20 years of experience in the information technology field as a consultant, educator, and serial entrepreneur. Dr. Malaga's academic research focuses on SEO, trust and privacy online, Web 2.0, and teaching in hybrid and online environments. His research has appeared in prestigious journals such as Communications of the ACM, International Journal of Electronic Commerce, and the Journal of Organizational Computing and Electronic Commerce. He currently serves on the editorial review boards of Information Resources Management Journal, the Journal of Electronic Commerce in Organizations and the International Journal of Mobile and Blended Learning.