Webcam Child Prostitution: An Exploration of Current and Futuristic Methods of Detection

Kemal Veli AÇAR[1]
Turkish National Police, Turkey

Abstract

Webcam Child Prostitution (WCP) is an emerging form of online child sexual abuse which the victim simply sells his/her live sexual images through Voice-over IP (VoIP) applications. Although it doesn't directly create some of the negative effects of traditional child prostitution such as sexual transmitted diseases, it may provide future abusers and victims to traditional child prostitution and child sex tourism. Therefore, appropriate and effective prevention strategies for this heinous act should be introduced accordingly. In this respect, this article discuss the efficiency of current methods of detection and propose some futuristic methods such as metadata and content analysis of VoIP communications by private sector and fully automated chatbot for undercover operations. Applicability of such new methods in real life heavily relies on legal amendments and it also requires further research on technical aspects.

Keywords: Online Child Sexual Abuse, Crime Prevention, Law Enforcement, Webcam Child Prostitution, VoIP, Cyber crime.

Introduction

Internet and related techological developments have made the communication between people faster and cheaper. Voice-over-IP (VoIP) is one of those more efficient ways which users have greatly benefited since the beginning of 2000s. In VoIP technology, audio and video communications are divided into several packets of digital information and transmitted through IP networks (Varshney, Snow, McGivern, & Howard, 2002). Unlike traditional phone services, particular features such as encrypted communications between parties, distributed structure of some networks and foreign-based popular VoIP service providers make lawful interception to illegitimate uses of this technology harder (Bellovin et al., 2006). For these reasons, like all groundbreaking inventions in history, VoIP applications are also embraced by malicious actors such as organized crime syndicates (Dunn, 2009) and online child sexual abusers (Hughes, 2002).

By using video streaming feature of VoIP applications, live child abuse images are produced and sometimes also sold for profit. Online grooming (Whittle, Hamilton-Giachritsis, Beech, & Collings, 2013), self-produced child pornography/sexting (Leary,

[1] Superintendent, Unit Manager, Technical & Operational Support Unit, Department of Cybercrime, Turkish National Police, Turkey. Email: kemalveli.acar@egm.gov.tr

2009) and sexual extortion (Kopecký, 2017) are the prime and most common examples of which VoIP technologies have been used for non-commercial purposes. On the other hand, in the commercial version, either an offender sexually abuse victim or child expose himself/herself in a lascivious manner in return for a payment from consumer (Crawford, 2014; Aurén & Kuhlmann, 2015). It's believed that the session is shaped with the sexual requests of consumer. And thus, intensity and price of the sexual abuse increase throughout the session. In addition to horrific psychological consequences for the victim, this heinous act also makes an effective, profitable and flexible business model for abusers, particularly compared to the trade of still images of online child sexual abuse.

Although Europol claims that Webcam Child Prostitution (WCP) is not an emerging crime but an established reality (Europol, 2015) and it has ties with child sex tourism (Europol, 2016), publicized cases supporting these remarks are rare. During Operation Endeavour, the only publicly known example, 29 international arrests were made and 15 Filipino children were rescued (Cohen-Almagor, 2015). However, this is not even the tip of the iceberg according to Swiss-based non-governmental organization Terre des Hommes (TDH). To show a glimpse of the problem's true scale, TDH Netherlands created a 3D model of a 10 years old Filipino girl and called her "Sweetie". In a sting operation conducted by TDH in public chat rooms and online dating sites, 1000 potential abusers offered Sweetie, money for sexual acts in 10 weeks (Crawford, 2013; Lemz, 2014).

As stated earlier, live child abuse images can be produced by different methods and with varied intentions. However, all this alternative ways don't have deep and tight relationship with child prostitution. In essence, WCP is not very different from the traditional form of prostitution as a child satisfies someone else's sexual needs in return for a fee through internet. The diverse method of interaction chosen by the parties doesn't really affect the incriminating core of the offence. Therefore, I prefer the term webcam child prostitution (WCP) instead of live streaming of child abuse (Europol, 2015) and webcam child sex abuse/tourism (Puffer, McDonald, Pross, & Hudson, 2014; Masri, 2015) since the term is more suitable and exact to define the act. Furthermore, this article largely ignores socio-psychological aspects while it puts the focus on the detection, intervention and disruption of WCP. I will analyze and discuss the current and possible methods of detection for WCP. In doing so, the main aim of the article is to start a technical and legal debate which hopefully leads practical solutions and encourage further research on this issue.

Literature Review

In the beginning of internet age, commercial sexual exploitation of children was rampant. Lax or none regulation over online environments and inadequate law enforcement response led the proliferation of several websites which sold child abuse images (Esposito, 1998). As time had passed, several international and national legal amendments had been drafted for a more effective global fight against online child sexual abuse (Akdeniz, 2016). International cooperation between law enforcement agencies (LEAs) also improved and successful police operations were carried out (Krone, 2005). Thanks to these developments, at the moment, it is considered that commercial sexual exploitation of children in online environments such as websites is not a big threat as it was before (European Financial Coalition against Commercial Sexual Exploitation of Children Online, 2010; ICMEC, 2016) However, while commercial websites were leaving the scene, a new and more resilient form emerged. WCP provides to offenders a

relatively safer environment where the lawful interception by law enforcement is almost impractical and effective detection of it by traditional methods is difficult.

Socio-psychological aspects of the child prostitution such as the affects on victims and the reasons led to prostitution have been examined thoroughly in the literature (Cusick, 2002). Aurén and Kuhlmann (2015) and Terre des Hommes Netherlands (2013a) confirm the findings of these studies for the online version of child prostitution. Furthermore, it is widely accepted that socio-economic conditions such as poverty, unemployment and lack of education greatly contribute to the proliferation of child prostitution. Therefore, prevention strategies also heavily depend on policy decisions for removing such socio-economic obstacles in general and improving the situation of vulnerable communities in particular (Rafferty, 2013). In this respect, it is reasonable to assume that same intervention programmes also would fight with WCP effectively.

In addition to these solutions, specific technical and legal methods can be applied in order to disrupt the online version of child prostitution. Unfortunately, crime prevention strategies and policies regarding the detection and interception of WCP have not been studied before. As the Luxembourg Guidelines nicely put, since the evolution in information and communication technologies is extremely rapid, it is not appropriate to overemphasise the focus on the technological aspect such as the current tools and devices that used in the commission of offences (Interagency Working Group, 2016). However, since the beginning of 2000s, VoIP technologies have steadily gained a big and almost irreplaceable part of the people's communications. And it seems this trend wouldn't change drastically in near future unless an unexpected technological development emerges. For these reasons, specific features of such tools bear great importance on the analysis, interception and detection of WCP. Since particular tools and applications are at the centre of this offence to the extent that it is not executable without them, naturally, methods of detection and prevention also can be extracted from the mechanism of related technologies used in the commission of crime. Therefore, instead of underestimating the current role of VoIP applications, it is actually important to emphasise them until they become obsolete.

Current Methods of Detection

To communicate in privacy is one of the most important and basic human rights. Therefore, in most countries, lawful interception of private communications is restricted as much as possible. Law enforcement agencies (LEAs) generally need solid evidence and/or probable cause and only apply this exceptional measure for limited number of serious offences (Gorge, 2007). These legal rules are essentially brought for traditional communication methods whose content itself is not criminal. However, VoIP chats in WCP cases are very different from traditional phone calls in terms of criminality. For example, a phone conversation between two offenders may give away the information of an actual crime before it takes place or after it committed. And thus, lawful interception of that phone call helps LEAs for taking preventive measures or collecting evidence. But at any point in investigation process, such phone communication itself isn't considered as a separate crime. It only provides a proper connection between illicit activities and offenders. On the other hand, VoIP communications of WCP itself is criminal despite the fact that it's just another type of communication in essence. It takes place completely within an online chat without leaking a clue to the real world. If the abuser and child

cannot connect with each other in video chat, this offence definitely will not occur. In WCP, communication and criminal act are inseparable and rarely witnessed by third parties. Therefore, revealing incidents of this offence heavily relies on the actions of parties involved since the communication between abusers and victims are highly private in nature. Unfortunately, due to monetary benefits and strong perception that it is less harmful than the traditional prostitution, reporting by victims is unlikely (Terre des Hommes Netherlands, 2013b). For these reasons, only publicized investigation of this severely underreported offence emerged as the result of a routine visit to a registered sex offender (Leyden, 2014). In addition to the attentive observation of law enforcement agents, they were also lucky. Because, video chat records of VoIP applications can not be usually recorded unless offender uses third party applications to save chats. That is the reason, at most times, why forensic examination of the digital belongings of possible WCP suspects is bound to be fruitless.

In an unlikely event, the abuser and child might be detected while the offence is committed. The lawful interception of real-time communications between parties can present undoubtable evidence in this case. However, due to legal and technical limitations, this option is almost impossible at the moment. To begin with, a company must abide in the legal framework of countries where its headquarters and/or operational centres are located. In order to prevent international conflicts, every country has similar legal measures and safeguards which actually designed to solve jurisdictional problems of traditional crimes (Brenner, 2006). And in most WCP cases, neither victim nor abuser is somehow related to the country where VoIP company operates. For example, the US legal framework only allows real-time monitoring of communications in investigations of which either it occurs in the US soil or at least one of the parties is an US citizen. Therefore, lawful interception of a WCP incident between 10 years old Filipino and a European adult who use the US-based VoIP services in the commission of crime seems to be out of jurisdiction for the US legal authorities. Possible interpretations of this legal rule by LEAs in such situations is not clear at the moment, but theoretically it doesn't seem feasible to monitor every WCP incidents in real time (Evripidis, 2008).

In addition to the inadequacy of current legal framework, there are technical problems about the real-time monitoring of possible WCP cases as well. From a technical viewpoint, VoIP technologies offer companies flexible schemes for the structure of their services. Besides traditional client/server models, distributed network based applications such as peer-to-peer structure of Skype are present (Soares, Neves, & Rodrigues, 2008). Regarding mostly Internet telephony, there are theoretical frameworks for the lawful interception of some types of these services (Milanovic et al., 2003; Seedorf, 2008). However, applicability of these solutions in real life is not clear at the moment. Furthermore, as the privacy concerns of users increased in the Post-Snowden era (Rainie & Madden, 2015), most VoIP companies have eagerly advertised additional security features such as encryption and peer-to-peer structure. It is very likely that such extra security measures would disrupt the working of proposed/further lawful interception schemes. These technical diversities and complexities make it impossible to apply a one-size-fits-all lawful interception regime for all type of VoIP technologies.

Undercover agents can also be used for identifying potential abusers and victims before the offence takes place (Mitchell, Wolak, & Finkelhor, 2005). At the beginning of internet age, there were limited online environments where abuser and victim may meet. However, attack surfaces of website forums and public chat rooms has expanded with the

inclusion of new meeting grounds such as social media, online gaming sites and mobile dating apps. Even though the traditional online environments are still preferred by abusers, constant expansion of attack surface to children remains challenging (Livingstone & Smith, 2014). Furthermore, internet users and time having spent online have multiplied while the resources of LEAs haven't keep up with this unprecedented increase. For every potential abuser, an undercover agent should be assigned. In Sweetie experiment, TDH Netherlands dealt with 1000 potential abusers in ten weeks and even they couldn't handle all of them despite the fact that researchers only focused on a particular online offence. Therefore, understandably, LEAs prioritize cases and allocate their limited resources of undercover capabilities to high profile investigations such as takeover of darknet websites (Cox, 2016). Limited human resources dedicated to fight against online child sexual abuse compel them to do such an unfortunate but inevitable preference. In addition to these general restrictions, as a specific requirement for the success of undercover WCP operations, the victim must show his/her face to abuser in order to convince abuser that he/she is real. According to the report of TDH, as soon as abusers see Sweetie's face, they are more willing to expose their real life identity in a very short notice (Terre des Hommes Netherlands, 2013b). However, in online grooming and child pornography cases, undercover law enforcement either persuade the potential abuser with childlike written statements or send him/her controlled child abuse images to persuade that he/she is a real child or abuser (Vendius, 2015). Unless LEAs employ real children for undercover operations, which is ethically and legally unacceptable, they would not convince potential abusers in most cases. Therefore, traditional manipulative methods of sting operations are also bound to be useless for the detection of WCP.

Possible Methods of Detection

1. A Fully Automated Chatbot: Sweetie 2.0?

LEAs should create new crime prevention strategies which rely on emerging technologies as criminals have always used such developments for their malicious activities. In this vein, Sweetie experiment of TDH is a remarkable example of how this simple principle can be applied in fighting against WCP. Unfortunately, current Sweetie doesn't remove traditional obstacles for effective and cost-friendly undercover operations. The reliance of researcher/police officer being present for every potential abuser makes it unmanageable to conduct an extensive swoop. If every human behind Sweetie is replaced by artificial intelligence, this groundbreaking method would be more effective in terms of creating high productivity from scarce resources.

As stated earlier, most potential abusers lose their control when they see the 3D modelled face of a child. The image of Sweetie is so powerful and convincing for them, past suspicions on the identity of a child give their place to sexual fantasies about further interaction. This cognitially distorted and sexually aroused situation of potential abusers makes them more vulnerable to be deceived. That is the main reason why majority of them almost instantly gave personally identifiable information about themselves during Sweetie operation. Exploiting this vulnerability in a big scale can only be made by developing an automated chatbot in which human intervention is minimized. Angga et al (2015) discussed the possibility of a fully automated chatbot which combines several different technologies. The proposed chatbot would take speech recognition to take input

from user, and then proceed it to chatbot API to receive the chatbot reply in a text form. The reply will be processed to text-to-speech recognition and created a spoken, audio version of the reply. Lastly, the computer will render an avatar whose gesture and lips are sync with the audio reply. The next version of Sweetie can be developed in a similar concept to this proposed approach. Furthermore, there are some particular aspects which make it easier to create such chatbot for this purpose. Firstly, convincing the people that the bot is a real human has always been a challenge. However, due to disturbed psychological situation of potential abusers, they would have a tendency to accept the mistakes of a chatbot as the normal communication troubles between an adult and a 10 year old Asian child. Secondly, since the Sweetie poses as a 10 year old Filipino girl who uses a very basic and mostly broken English, construction of a chatbot knowledge would be a relatively easier job compared to other types of chatbots (Jia, 2004; Huang, Zhou, & Yang, 2007). Records of previous Sweetie operation might be also used in the construction of the knowledge as assistance. For these reasons, a fully automated chatbot would be a feasible and an effective way for dealing with thousands of potential abusers simultaneously.

The algorithm behind the proposed next version of Sweetie can be developed in a way that entrapment defence could be nullified. Since it is a robot which operates with zero human intervention, it would be more difficult to back up the allegations of manipulation than traditional undercover investigations (Roiphe, 2013). On the other hand, other legal requirements for this idea would be harder to achieve. In most countries, conditions of undercover agents are essentially defined for the prevention and detection of traditional organised crimes. There are strict rules on who the undercover agent is and personal qualifications are exhaustively emphasized in the related legal documents. Therefore, presence of a human being is the necessary element of undercover investigations at the moment. However, in the proposed approach, humans would only involve in the evaluation of stored communications between chatbot and potential abusers, not during undercover operation. The legal framework for online child sexual abuse investigations should be changed in order to conduct such human less undercover operations.

2. Big Data Analysis on Metadata of Communications by VoIP Companies

Metadata is data which describes attributes of a resource (Dempsey & Heery, 1998) or simply "data about data" (Burnett, Ng, & Park, 1999). While content data reveals the true nature of the VoIP communications between parties such as texts, audio and video files; metadata only shows some attributes of communications such as date, creator and IP addresses without severely compromising the privacy of communications. Therefore, collecting metadata is easier both technically and legally since it takes up less space on disk and involves less intrusive information than content data. Understandably, internet service providers have analyzed the big data that their users have created for commercial reasons such as showing the right ads. Varying on particular features of the products, VoIP companies can conduct such analysis on the metadata of their users' communications. For example, if centralised servers are involved in, all types of metadata of every communication can be subject to analysis. In case the structure of services is based on a decentralised system such as Skype, metadata is limited but still exists to some extent. The idea is to detect possible WCP cases by an analysis on the metadata of VoIP communications.

It's not fair to claim that commercial sexual exploitation is only limited to a specific geographic location (Huynh, Scheuble, & Dayananda, Nd) but Southeast Asian countries have an infamous reputation for traditional child prostitution (Lim, 1998). Additionally, only publicized example of WCP also point out victims from Philippines exclusively. According to TDH, some parts of the country have become hubs for WCP. Besides mostly family-run individualistic schemes, "dens" disguised as legal enterprises are also involved in the production. For these reasons, location-based metadata analysis can reveal some irregular patterns of communication and help LEAs to identify victims and offenders.

In this regard, IP addresses of the parties are the basic information which might show the location of the parties. It is very reasonable to claim that every VoIP company already has or can effortlessly have the technical capability to capture such information. On the assumption that victim does not use anonymization technologies such as Virtual private networks or the onion router (TOR) network in order to conceal his/her true location (Savchenko & Gatsenko, 2015), analysis of IP addresses can reveal majority of WCP cases. For example, a Filipino girl from the Cebu district contacts 3 abusers from 3 different countries in a week. It is an undoubtedly red flag for WCP that a resident of a very poor city chats with multiple foreigners from relatively wealthier countries. If the related VoIP company performs big data analysis on metadata of communications in order to detect such irregular patterns of international calls, it is likely to reveal that incident. Later, VoIP company would refer the IP addresses and other helpful information such as e-mail addresses to related law enforcement agency for deeper examination. This method can be applied for other places where traditional child prostitution is common in case it would be successful in Philippines.

3. Big Data Analysis on Content Data by VoIP Companies

Content data analysis should be an exceptional method of detection for WCP due to its highly intrusive nature on privacy. Nonetheless, it cannot be ruled out completely. In certain conditions and also with strict legal and technical procedures, this measure might create remarkably great results in terms of crime prevention and child protection. The theoretical idea here I will present is not the only way to conduct such analysis on VoIP communications. And it only applies to recently introduced real-time translation feature of the leading VoIP company, Skype Inc. This technology instantly translates some languages by combining Automated Speech Recognition, Machine Translation engine and Text-to-Speech (Lewis, 2015). Skype is the most popular VoIP application at the moment and it's reasonable to assume that bulk of the victims and offenders also use it. In this respect, real-time translation feature of Skype chats may bring a viable solution for scattering the black clouds over WCP. However, since the technical aspects on whether the translated conversations can be intercepted and/or analyzed are unclear and probably classified information for the company, I will propose a raw idea with the hope that it will be tested by further research or it will influence related technological developments in the future.

Millions of people around the world communicate via Skype simultaneously, so it looks nearly impossible to detect WCP at first glance. However, it's not as a tough job as it seems because communications of WCP have two distinctive attributes in its content: methods of child sexual abuse and methods of payment. Since the consumer directs the session by sexual requests, it's reasonable to see some words such as "boobs", "masturbate", vagina" within the records of chats. In addition to sexual/abusive terms,

methods and quantity of payment would be discussed during the session as well. According to TDH, most victims use Western Union and a local money-transferring company called Cebuana L'huillier (Terre des Hommes Netherlands, 2013a), but, "bitcoin", "paypal", "ukash" and other related financial terms are also expected to be seen. This is a rare combination for occasional chats between law-abiding citizens. Nevertheless, to avoid positive falses as much as possible, the process should be divided into two different parts that each takes 2-3 months: Detection and Identification.

In the detection phase, suspicious activities would be discovered by the help of keywords regarding WCP. Probably with the help of LEAs, Skype Inc. would form two separate sets of keywords for abusive and financial terms. And then, the communications which combine the keywords from these two different sets would be set aside for the identification phase so that a deeper examination would be carried out. As mentioned before, it is observed that one victim at the center provides WCP to the consumers from several different countries. Therefore, location analysis on metadata can also be included into this process as supporting evidence or some type of a verification tool. Furthermore, to minimize the detection of consensual sexual activity between adults, It can be given a lot weight to the combination of undeniably suspicious words such as "child" and "bitcoin" more than others.

In the identification phase, after required judicial permission is granted, communications of possible victims would be recorded for 2-3 months period in the supervision of LEAs. If any of the recordings shows signs of child sexual abuse, evidence will be referred to law enforcement agency of related country immediately. If not, the recordings would be deleted instantly. In this way, negative impact on the privacy of ordinary users would be greatly minimized. I would like to emphasize that no mass communication recording would take place in any part of these phases. Detection phase would bring some suspicious users to the front without recording actual communications. And during identification phase, only the recordings of criminal activity would be kept and referred to LEAs. At worst, detection phase would not yield any positive results. Thankfully, we would be able to say that WCP is not prevalent as feared. At best, it would be the most sensational crackdown on child sexual abusers in history, which several victims would be rescued. Additionally, it's likely that connections with other crimes such as traditional child prostitution and child trafficking would be also revealed in the aftermath of this operation. Lastly, without a doubt, it would be a monumental move for the public-private partnership regarding cyber crime investigations.

Discussion

Of all the proposed solutions for WCP, a fully automated chatbot is the most probable idea to be actualized. Terre des Hommes Netherlands can improve the current Sweetie in a way that this article has described. First draft of this article, which only included the idea of content data analysis, was welcomed by Terre des Hommes Netherlands. However, I could not get a response from them on the idea of a fully automated chatbot. Nevertheless, due to level of dedication on the subject matter that they have showed so far, I believe they will seriously consider this theoretical solution. On the other hand, in a legal viewpoint, it's ideal that every country adapts their legal frameworks in order to conduct such human less undercover operations. But, in reality, even one country may be adequate for triggering a global swoop. LEAs of other countries can not ignore such serious allegations on the basis that the information is provided by a chatbot, not a human.

Therefore, a local investigation would be probably initiated after the tip from Sweetie 2.0 arrived. The legal technicalities might prevent a conviction for the abuser in the end of judicial process, but, possible further criminal activities by the abuser such as child sex tourism and physical child sexual abuse could be avoided since the abuser is caught by the radar of local LEAs.

On the other hand, for metadata and content analysis on communications by VoIP companies, there are major challenges in practice. To begin with, private sector has greatly helped LEAs for individual online child sexual abuse cases, but they have never done big data analysis for this purpose. Considering the global response after the revelations of Edward Snowden, companies wouldn't be eager to conduct massive scale analysis on their users' data even for a noble cause such as the prevention of WCP. Even though it is known that a company is technically capable, it is not possible to compel them to actualize this idea in case the company is not willing to cooperate. Moreover, if a company is willing to do such an analysis for WCP at the moment, there might be similar operational ideas for other types of crimes in the future. The possibility of such expansion would compel private sector to avoid involvement in the current operations. Furthermore, in case the frightening capability of such power on users' data is revealed to public, even though the company declares that they never use it again, privacy concerns regarding mass surveillance would grow and customer base of the related VoIP product might shrink as a result. Lastly, unlike intelligence gathering, legal background of these proactive and highly intrusive approaches does not exist for criminal investigations. Particularly for content data analysis, there needs a predefined and strict legal procedures to prevent misuse of such analysis both for LEAs and the companies.

Conclusion

Since the current methods of detection heavily rely on the reporting by the parties of WCP incidents, they are highly ineffectual to reveal the true scope of this offence. Undercover operations can detect some of the incidents. However, enormous financial and human resources are needed in order to keep up with thousands of possible abusers. As criminals have always adapted their modus operandi to new technologies, LEAs should come up with new measures accordingly. In this respect, this article discussed the feasibility of a fully automated chatbot, metadata and content analysis on communications by VoIP companies. Compared to legal and socio-psychological complications, technical difficulties of these proposed ideas can be overcome easily. The real problem is to persuade policymakers and private sector. As long as outdated views of policymakers on crime prevention and profit-centred approach of private sector prevail over unconventional methods of fighting crimes, these types of theoretical solutions are doomed to stay on paper.

References

Akdeniz, Y. (2016). *Internet child pornography and the law: national and international responses*. Abington, Oxford, UK: Routledge.

Angga, P. A., Fachri, W. E., Elevanita, A., & Agushinta, R. D. (2015, October). Design of chatbot with 3D avatar, voice interface, and facial expression. In *2015 International Conference on Science in Information Technology (ICSITech)* (pp. 326-330). IEEE.

Aurén, S., & Kuhlmann, D. F. (2015). Nipa Huts with High Speed Internet: Commercial Exploitation of Children in the 21st Century. A Qualitative investigation of Webcam Child Prostitution in the Philippines.

Bellovin, S., Blaze, M., Brickell, E., Brooks, C., Cerf, V., Diffie, W., & Treichler, J. (2006). Security implications of applying the Communications Assistance to Law Enforcement Act to voice over IP. *Information Technology Association of America, 13*.

Brenner, S. W. (2006). Cybercrime jurisdiction. *Crime, law and social change*, *46*(4-5), 189-206.

Burnett, K., Ng, K. B., & Park, S. (1999). A comparison of the two traditions of metadata development. *Journal of the Association for Information Science and Technology*, *50*(13), 1209.

Cohen-Almagor, R. (2015). *Confronting the Internet's Dark Side. Moral and Social Responsibility on the Free Highway*. (pp. 299). Cambridge, UK: Cambridge University Press.

Cox, J. (2016, January 5). The FBI's 'Unprecedented' Hacking Campaign Targeted Over a Thousand Computers. *Motherboard*. Retrieved from http://motherboard.vice.com/read/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers

Crawford, A. (2013, November 5). Computer-generated 'Sweetie' catches online predators. *BBC News*. Retrieved from http://www.bbc.com/news/uk-24818769.

Crawford, A. (2014, January 14). UK paedophiles pay to watch webcam child sex abuse in Philippines. *BBC*. Retrieved from http://www.bbc.com/news/uk-25729140.

Cusick, L. (2002). Youth prostitution: A literature review. *Child abuse review*, *11*(4), 230-251.

Dempsey, L., & Heery, R. (1998). Metadata: a current view of practice and issues. *Journal of Documentation*, *54*(2), 145-172.

Dunn, J. E. (2009, February 11). Criminals using Skype, say Italian police, *Networkworld*. Retrieved from http://www.networkworld.com/article/2262802/collaboration-social/criminals-using-skype--say-italian-police.html.

Esposito, L. C. (1998). Regulating the Internet: The new battle against child pornography. *Case W. Res. J. Int'l L., 30*, 541.

European Financial Coalition against Commercial Sexual Exploitation of Children Online. (2010). 14 months on: A combined report from the European Financial Coalition 2009-2010. Retrieved from https://www.ceop.police.uk/documents/efc%20strat%20asses2010_080910b%20final.pdf.

Europol. (2015). The Internet Organised Crime Threat Assessment (IOCTA) 2015. Retrieved from https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web_2015.pdf.

Europol. (2016). The Internet Organised Crime Threat Assessment (IOCTA) 2016. Retrieved from https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_w

eb_2016.pdf.

Evripidis, R. (2008). Lawful Interception and Countermeasures: In the era of Internet Telephony. Master's Thesis submitted to the Royal Institute of Technology, Stockholm, Sweden. Retrieved from http://www.diva-portal.org/smash/get/diva2:511012/FULLTEXT01.pdf.

Gorge, M. (2007). Lawful interception–key concepts, actors, trends and best practice considerations. *Computer Fraud & Security*, *9*, 10-14.

Huang, J., Zhou, M., & Yang, D. (2007, January). Extracting Chatbot Knowledge from Online Discussion Forums. *IJCAI,* 7, 423-428.

Hughes, D. M. (2002). Use of New Communications and Information Technologies for Sexual Exploitation of Women and Children, *The Hastings Women's LJ, 13*, 127.

Huynh, T. N., Scheuble, L., & Dayananda, V. (Undated). Child Prostitution in 12 Countries: An Exploratory Study of Predictors. *The Penn State McNair Journal*, 135.

Interagency Working Group. (2016). Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Retrieved from www.interpol.int/Media/Files/News-Media-releases/2016/Terminology-Guidelines.

International Centre for Missing & Exploited Children. (2016). Child pornography: Model legislation and global review (8th edition). ICMEC. Retrieved from http://www.icmec.org/wp-content/uploads/2016/02/Child-Pornography-Model-Law-8th-Ed-Final-linked.pdf.

Jia, J. (2004). The study of the application of a web-based chatbot system on the teaching of foreign languages. In *Proceedings of SITE* (Vol. 4, pp. 1201-1207).

Kopecký, K. (2017). Online blackmail of Czech children focused on so-called "sextortion" (analysis of culprit and victim behaviors). *Telematics and Informatics*, *34*(1), 11-19.

Krone, T. (2005). *International police operations against online child pornography*. Canberra, Australia: Australian Institute of Criminology.

Leary, M. G. (2009). Sexting or Self-Produced Child-Pornography-The Dialog Continues-Structured Prosecutorial Discretion within a Multidisciplinary Response. Va. *J. Soc. Pol'y & L., 17*, 486.

Lemz. (2014, February 17). 'Sweetie' for Terre des Hommes [Video File]. Retrieved from https://vimeo.com/86895084.

Lewis, W. D. (2015). Skype translator: Breaking down language and hearing barriers. *Proceedings of Translating and the Computer (TC37).*

Leyden, J. (2014, January 17). International child abuse webcam ring smashed after routine police check. *The Register.* Retrieved from http://www.theregister.co.uk/2014/01/17/webcam_abuse_ring_dismantled.

Lim, L. L. (Ed.). (1998). *The sex sector: The economic and social bases of prostitution in Southeast Asia*. International Labour Organization.

Livingstone, S., & Smith, P. K. (2014). Annual research review: Harms experienced by child users of online and mobile technologies: The nature, prevalence and management of sexual and aggressive risks in the digital age. *Journal of child psychology and psychiatry*, *55*(6), 635-654.

Masri, L. (2015). Webcam Child Sex Abuse. Retrieved from http://academicworks.cuny.edu/cgi/viewcontent.cgi?article=1107&context=gj_etds.

Milanovic, A., Srbljic, S., Raznjevic, I., Sladden, D., Skrobo, D., & Matosevic, I. (2003, September). Distributed system for lawful interception in VoIP networks. In *EUROCON 2003. Computer as a Tool. The IEEE Region 8, 1*, 203-207.

Mitchell, K. J., Wolak, J., & Finkelhor, D. (2005). Police posing as juveniles online to catch sex offenders: Is it working?. *Sexual Abuse: A Journal of Research and Treatment*, *17*(3), 241-267.

Puffer, E., McDonald, K., Pross, M., & Hudson, D. (2014). Webcam Child Sex Tourism: An Emerging Global Issue. Retrieved from http://digitalcommons.cedarville.edu/cgi/viewcontent.cgi?article=1131&context=research_scholarship_symposium.

Rafferty, Y. (2013). Child trafficking and commercial sexual exploitation: A review of promising prevention policies and programs. *American journal of orthopsychiatry, 83*(4), 559-575.

Rainie, L., & Madden, M. (2015). Americans' privacy strategies post-Snowden. *Pew Research Center.*

Roiphe, R. (2013). The Serpent Beguiled Me: A History of the Entrapment Defense. *NYLS Legal Studies Research Paper*, (13/14), 73.

Savchenko, I. I., & Gatsenko, O. Y. (2015). Analytical review of methods of providing internet anonymity. *Automatic Control and Computer Sciences, 49*(8), 696-700.

Seedorf, J. (2008). Lawful interception in P2P-based VoIP systems. In *Principles, Systems and Applications of IP Telecommunications. Services and Security for Next Generation Networks* (pp. 217-235). Springer Berlin Heidelberg.

Soares, V. N., Neves, P. A., & Rodrigues, J. J. (2008, June). Past, present and future of IP telephony. In *Communication Theory, Reliability, and Quality of Service, 2008. CTRQ'08. International Conference on* (pp. 19-24). IEEE.

Terre des Hommes Netherlands. (2013a). An Exploratory Study on the Background and Psychosocial Consequences of Webcam Child Sex Tourism in the Philippines. Retrieved from https://www.terredeshommes.nl/sites/tdh/files/uploads/research_report_2.pdf.

Terre des Hommes Netherlands. (2013b). Becoming Sweetie: a novel approach to stopping the global rise of Webcam Child Sex Tourism. Retrieved from https://www.terredeshommes.nl/sites/tdh/files/uploads/research_report.pdf

Varshney, U., Snow, A., McGivern, M., & Howard, C. (2002). Voice over IP. *Communications of the ACM*, *45*(1), 89-96.

Vendius, T. T. (2015). Proactive Undercover Policing and Sexual Crimes against Children on the Internet. *European Review of Organised Crime*, *2*, 6-24.

Whittle, H., Hamilton-Giachritsis, C., Beech, A., & Collings, G. (2013). A review of online grooming: Characteristics and concerns. *Aggression and violent behavior, 18*(1), 62-70.

Willis, B. M., & Levy, B. S. (2002). Child prostitution: global health burden, research needs, and interventions. *The Lancet*, *359*(9315), 1417-1422.