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

Kemal Veli AÇAR[1]
Turkish National Police, Turkey

Abstract

Webcam child prostitution is an emerging form of online child sexual abuse which the victim simply sells his/her lives sexual images through Voice-over-IP (VoIP) applications. Although it doesn't directly create some negative effects of traditional child prostitution like sexually transmitted diseases, it may provide future offenders and victims to the traditional crimes such as 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 data analysis of VoIP communications by the private sector and the use of fully automated chatbots for undercover operations. The applicability of such new methods in real life heavily relies on legal amendments and requires further research on technical aspects in particular.

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

Introduction

The Internet and related technological 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 the 2000s. In VoIP technology, audio and video communications are divided into several tiny packets of digital information and transmitted through IP-based networks (Varshney, Snow, McGivern, & Howard, 2002). Unlike traditional phone services, particular features such as encrypted communications between parties, distributed and decentralized structure of some networks and the market dominance of foreign-based popular VoIP service providers make lawful interception to the illegitimate uses of this technology harder (Thanthry, Pendse, & Namuduri, 2005; Bellovin et al., 2006). For these reasons, like all groundbreaking inventions throughout history, VoIP applications are also embraced by malicious actors such as organized crime syndicates (Dunn, 2009) and online child sexual abusers (Hughes, 2002).

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

By using the 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, 2009) and sexual extortion (Açar, 2016) are the prime and most common examples of which VoIP technologies have been used for non-commercial purposes. Non-commercial types of live streaming of child abuse don't have a deep and tight relationship with child prostitution. On the other hand, in the commercial version, either abusers sexually exploit victim(s) or the child exposes himself/herself in a lascivious manner in return for a payment from the offender/consumer (Crawford, 2014). In essence, webcam child prostitution (WCP) is not much different from its traditional form as the victim satisfies someone else's sexual needs in return for a fee through the internet. The diverse methods of interaction chosen by parties don't actually affect the incriminating core of the offense. Therefore, the author prefers the term webcam child prostitution 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.

Although Europol proclaims 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 of WCP investigations, 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 the non-governmental organization Terre des Hommes (TdH) Netherlands. To show a glimpse of the problem's true scale, TdH Netherlands created a 3D model of a 10-year- old Filipino girl and called her "Sweetie". In a sting operation conducted by TdH Netherlands in public chat rooms and online dating sites, 1000 potential abusers from 71 different countries offered Sweetie money for sexual acts over 10 weeks (Crawford, 2013; Lemz, 2014). Hans Guijt, the head of special programs and campaigns of TdH Netherlands, elaborated on this experiment. Over 20000 individuals sought to get into contact with Sweetie during the course of the experiment. And, that was more than the four operators could handle. While two of them were handling the chats, the other two were trying to identify the individuals with the information rising from the chats (Hans Guijt, personal communication, 16 January, 2017).

Furthermore, it's believed that the sessions of WCP are shaped with the sexual requests of the consumer. And thus, intensity and price of the sexual abuse might increase throughout the session. In addition to the 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. Since every interaction, even ones with the same victim(s), creates a unique and unsubstitutable experience for the offender, it becomes rational to pay for the live images although free child abuse materials are abound in the Internet. Economic aspect of WCP and the specific determinants of the perceived value of produced live images are an entirely different concept than this article aims to examine. However, this dark area also should be researched thoroughly in order to develop actionable strategies for diminishing demand and supply of WCP from an economic viewpoint.

This article largely ignores socio-psychological aspects while it puts the focus on the detection, interception and disruption of WCP. The author will analyze and discuss the current and futuristic 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 to new or better practical solutions and also encourage further research on this matter. Lastly, there are many private sector entities which offer customers VoIP-enabled services as a side benefit to their main products such as Google and Facebook, in addition to the completely VoIP-centered companies like Skype. Since the underlying technology and its implications for WCP remains the same, the term "VoIP companies" is used to cover the both types throughout the article as a convenience.

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. LEAs generally need solid evidence and/or probable cause, and only apply this exceptional measure for a limited number of serious offenses (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 was committed. And thus, lawful interception of that particular phone call helps LEAs for taking preventive measures or collecting evidence. But at any point in the investigation process, such phone communication itself isn't considered a separate crime. It only provides a proper connection between illicit activities and offenders. Conversely, VoIP communications of WCP itself is criminal despite the fact that it's just another type of a communication in essence. It takes place completely within an online chat without leaking a clue to the real world. If the offender and child, cannot connect with video chat, this offense definitely will not occur.

In WCP, communication and criminal act are inseparable and rarely witnessed by third parties. Therefore, revealing incidents of this offense heavily relies on the actions of the parties involved, since the communication between offenders and victims are highly private in nature. Unfortunately, due to monetary benefits of WCP 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 offense 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. The computer of the offender or victim can record video chats, but one should use special third party applications to do that for most VoIP products. That is the reason, at most times, why the forensic examination of the digital belongings of possible WCP suspects is bound to be fruitless.

In an unlikely event, the offender and child might be detected while the offense is committed. The lawful interception of real-time communications between parties can present solid 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 centers are located. To prevent international conflicts, every country has similar legal safeguards which actually designed to solve jurisdictional problems of traditional crimes (Brenner, 2006). And in most WCP cases, neither victim nor offender is somehow related to the country where the VoIP company operates. For example, US legal framework only allows

real-time monitoring of communications in investigations of which either it occurs in US soil or at least one of the parties is a US citizen. Therefore, lawful interception of a WCP incident between 10-year-old Filipino and a European adult who use US-based VoIP services in the commission of crime seems out of jurisdiction for 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 incident in real time (Evripidis, 2008).

In addition to the inadequacy of the current legal framework, there are technical problems with 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 like the 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, the applicability of these solutions in real life is not clear at the moment. Furthermore, as the privacy concerns of consumers 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 likely that such extra security measures would disrupt the working of the 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 types of VoIP technologies.

Undercover agents can also be used for identifying potential offenders and victims before the offense takes place (Mitchell, Wolak, & Finkelhor, 2005). At the beginning of the internet age, there were limited online environments where offenders and victims may meet. However, attack surfaces of website forums and public chat rooms have expanded with the inclusion of new meeting grounds such as social networking sites, online gaming sites and mobile dating applications. Even though the traditional online environments are still preferred by abusers, the 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 kept up with this unprecedented increase. For every potential offender, an undercover agent should be assigned. In Sweetie experiment, TdH Netherlands dealt with more than 20000 potential offenders over ten weeks and even they couldn't handle all of them even though researchers only focused on a particular online offense. Therefore, understandably, LEAs prioritize cases and allocate their limited resources of undercover capabilities to high profile investigations like the 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 conclusion, LEAs have the legal authority to fight WCP with undercover operations, yet they completely lack the requisite resources for a meaningful victory.

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 the offender so as to convince that he/she is real. According to the report of TdH Netherlands, as soon as offenders see Sweetie's face, they are more willing to expose their real life identity in a short notice (Terre des Hommes Netherlands, 2013b). However, in online grooming and child pornography cases, undercover law enforcement agents either persuade the targets with childlike written statements or send him/her controlled child abuse images to

persuade he/she is a real child or an abuser (Vendius, 2015). Unless LEAs employ real children for undercover operations, an ethically and legally unacceptable method, they would not convince potential offenders in most cases. Therefore, traditional manipulative methods of sting operations are also bound to be useless for the detection of WCP.

Futuristic Methods of Detection

1. Fully automated chatbots

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 Netherlands is a remarkable example of how this simple principle can be applied in the fight against WCP. Unfortunately, current Sweetie doesn't remove traditional obstacles for effective and cost-friendly undercover operations. The reliance of the researcher/police officer being present for every potential offender 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 offenders 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 about the identity of a child give their place to sexual fantasies about further interactions. This cognitively distorted and sexually aroused situation of potential offenders makes them more vulnerable to be deceived. This was the main reason why the majority of the offenders 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 the 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. This is not the only way of creating a chatbot for the purpose of the detection of WCP. As will be explained thoroughly later, TdH Netherlands developed the Sweetie 2.0 as a hybrid - not fully automated - model of chatbot. In the future, hopefully, as new technological innovations and proof of concepts arise, there might be several different Sweeties until one rules them all or all work together fine.

Furthermore, there are some particular aspects which make it easier to create such chatbots for this purpose. Firstly, convincing the people that the bot is a real human has always been a challenge. However, due to the disturbed psychological situation of potential offenders, they would have a tendency to accept the grammatical mistakes of a chatbot as the normal communication troubles between an adult and a 10-year-old Asian child. In a similar vein, the video quality of chats might also be knowingly manipulated to hide the visual flaws of a computer-generated character. Since the victims are generally poor and less educated, it would be convincing to make additional excuses for such deliberate interruptions such as "I am using my neighbor's internet", "I am downloading a movie" or "I think I have virus". Secondly, since Sweeties would pose as a 10-year-old

Filipino girl who uses a 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). As an actual example, records of previous Sweetie operation were successfully used in the construction of the knowledge (Hans Guijt, personal communication, 17 January, 2017). For these reasons, fully automated chatbots would be a feasible and an effective way for dealing with thousands of potential offenders simultaneously.

Recently, the legal requirements and implications of a fully automated Sweetie 2.0 are extensively discussed (Schermer et al., 2016). There are several legal aspects of the subject matter which the full coverage exceeds the scope and purpose of this article. Therefore, the author focused on the most important legal aspects of fully automated chatbots: entrapment and the legal conditions of the undercover agents. The algorithm behind the fully automated chatbots can be developed in a way that the entrapment defense could be nullified for them. A cold and patient artificial intelligence might avoid the possibility of entrapment easier than humans do. Since it is a robot which operates with zero human intervention, for defense, it would be more difficult to back up the allegations of manipulation than traditional undercover investigations (Roiphe, 2013). In most countries, conditions of undercover agents are essentially defined for the prevention and detection of traditional organized crimes. LEAs are the preferred source of undercover agents, yet it is possible to employ someone who is not a member of LEAs in some countries. However, in both situations, generally there are strict rules on who the undercover agent is and the personal qualifications of his/her are exhaustively emphasized in the related legal documents. Therefore, a human being seems a necessary element of undercover investigations at the moment. However, in the proposed approach, humans would only involve in the evaluation of stored communications between chatbots and potential offenders, not during undercover operations. The legal framework for online child sexual abuse investigations should be changed to conduct such humanless undercover operations.

2. Big Data Analysis of Metadata 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 personal information than the content data have. Understandably, internet service providers have analyzed the big data that their users have created for commercial reasons like 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 centralized servers are involved in, all types of metadata of every communication can be subjected to analysis. In case the structure of services is based on a decentralized system like Skype, metadata is limited but still exist to some extent. The idea is to detect possible WCP cases by an analysis of 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, Undated) but Southeast Asian

countries have an infamous reputation for traditional child prostitution (Lim, 1998). Additionally, only publicized example of WCP also points out victims from the Philippines exclusively. According to TdH Netherlands, 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 reasonable to claim every VoIP company already has or can effortlessly have the technical capability to capture such information. On the assumption that the victim does not use anonymization technologies such as Virtual private networks or the onion router (TOR) network to conceal his/her true location (Savchenko & Gatsenko, 2015), analysis of IP addresses can reveal the majority of WCP cases. For example, a Filipino girl from the Cebu district contacts three offenders from three 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 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 like email addresses to the 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 the Philippines.

3. Big Data Analysis of Content Data by VoIP Companies

Content data analysis should be an exceptional method of detection for WCP due to its high intrusive nature on privacy. Nonetheless, it can't be ruled out completely. In certain conditions and with strict legal and technical procedures, this measure might create remarkable results in terms of crime prevention and child protection. The author believes future technological developments, artificial intelligence in particular (Clark, 2017), will present new possibilities for better and more extensive solutions. However, for the time being, the theoretical idea here the author will present is one of the few possible ways to conduct such analysis on VoIP communications. And, it only applies to recently introduced real-time translation feature of the leading VoIP company, Skype. 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 some 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, the author 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 Netherlands, most victims use the Western Union and a local money-transferring company called Cebuana L'huillier (Terre des Hommes Netherlands, 2013a), but, "Bitcoin", "PayPal" 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 with the help of keywords regarding WCP. Probably with the help of LEAs, Skype 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 live images to the consumers from several different countries. Therefore, location-based analysis on metadata can also be included into this part of phase 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 of weight to the combination of undeniably suspicious words like "Masturbate" and "Bitcoin" more than others.

In the identification phase, after required judicial permission is granted, communications of possible victims would be recorded in 2-3 months period under the supervision of LEAs. If any of the recordings shows signs of child sexual abuse, evidence will be referred to law enforcement agency of the 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. The author 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 activities would be kept and referred to LEAs. At worst, detection phase would not yield any positive results. Thankfully, we would be able to say WCP is not prevalent as feared. At best, it would be the most sensational crackdown on child sexual abusers in history, which several victims also would be rescued. It's also 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 in case it is sensational as this article envisioned.

Discussion

Of all the proposed solutions for WCP, fully automated chatbots are the most probable ideas to be actualized. Thankfully, TdH Netherlands recently finished its Sweetie 2.0 project. During the review of this article, the software package was launched in Manila in February 2017 and presented to LEAs in the Philippines (Hans Guijt, personal communication, 16 January, 2017). It is very early to observe the outcomes of such implementation, let alone evaluation. However, it is an undoubtedly right and important first step in the long and rough way to detect and deter possible offenders of WCP. Technically, the Sweetie 2.0 will record and analyze the chats between the chatbot and

possible offenders. The main aim is basically to profile "online predators" and identify repetitive patterns in communications afterwards. Largely constructed from the previous chat records of Sweetie experiment, conversation model will determine if a chat partner displays indecent/illegal intentions and if so, obtain additional information about him/her. It is also possible for the users to switch manual function whenever they find it more appropriate (Hans Guijt, personal communication, 17 January, 2017). Apparently, the Sweetie 2.0 puts its focus on the determination of the textual characteristics of WCP incidents. It is not a flaw but strength for further possibilities. Thus, it is possible to develop other types of Sweeties which rely on different technological solutions and targets different aspects of WCP, as in the way of this article has described or other ways. If these diverse options come to life as the author hopes, then at some point, it would be much more difficult to distinguish these multiple chatbots from real children for the potential offenders. And thus, hopefully, this situation would increase the risk of identification of potential offenders and it would also function as a highly efficient deterrent of WCP in the future.

From a legal viewpoint, it's ideal that every country adapts their legal frameworks to conduct such humanless undercover operations. But, in reality, even one country may be adequate for triggering a global swoop. LEAs of other countries can't 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 the chatbot arrived. The legal technicalities might prevent a conviction for the offender in the end of the judicial process, but, possible further criminal activities such as child sex tourism and physical child sexual abuse could be avoided since the offender is caught by the radar of local LEAs. Thanks to the Netherlands again, the Dutch House of Representatives recently approved an amendment to draft Cyber Crime Legislation which will enable LEAs to carry out undercover operations and to apply virtual children such as 'Sweetie' in investigating and prosecuting online child sex abusers ("Dutch House", Undated; Hans Gujit, personal communication, 17 January, 2017). However, it is not clear whether the legal framework of the Philippines allows the use of the Sweetie 2.0 as an investigative measure at the moment (Schermer et al., 2016). Therefore, they might not involve in such humanless undercover operations in the short term.

Conversely, for metadata and content data analysis of communications by VoIP companies, there are major challenges in practice. To begin with, the 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 to the revelations of Edward Snowden, companies wouldn't be eager to conduct massive scale analysis on their users' data even for a noble cause like the prevention of WCP. Even though it is known a company is technically capable, it is impossible to compel them to actualize this idea in case the company is unwilling 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 operational expansion would compel the private sector to avoid involvement in the current operations. Furthermore, in case the frightening capability of such power on users' data is revealed to the public, even though the company declares they never use it again, privacy concerns regarding mass surveillance would grow and customer base of the related VoIP product might shrink consequently. 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 offense. Undercover operations can detect some incidents. However, enormous financial and human resources are needed to keep up with thousands of possible offenders. As criminals have always adapted their modus operandi to new technologies, LEAs are already coming up with new measures accordingly. In this respect, this article examined the current Sweetie 2.0 project and discussed the need for other types of fully automated chatbots. Additionally, metadata and content data analysis of communications by VoIP companies are discussed. Compared to legal and socio-psychological complications, technical difficulties of these proposed ideas can be overcome easily. The real challenge is to persuade policy makers and the private sector. As long as outdated views of policy makers on crime prevention and profit-centered approach of the private sector prevail over unconventional methods of fighting crimes, these types of theoretical solutions are doomed to stay on paper.

References

Açar, K. V. (2016). Sexual Extortion of Children in Cyberspace. *International Journal of Cyber Criminology, 10(2).*

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.

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.

Clark. J. (2017, January 9). Why Artificial Intelligence is the answer to the greatest threat of 2017, cyber-hacking. *Independent*. Retrieved from http://www.independent.co.uk/voices/artificial-intelligence-cyber-hacking-russia-malware-2017-biggest-threat-a7516916.html.

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.

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.

Dutch House of representatives approves "Sweetie". (Undated). *Save Sweetie… Now!*. Retrieved from https://www.savesweetienow.org/news/house-of-representatives-approves-application-of-sweetie-in-the-netherlands.

Europol. (2015). The Internet Organised Crime Threat Assessment (IOCTA) 2015. Retrieved from 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 www.europol.europa.eu/sites/default/files/publications/europol_iocta_web_2016.pdf.

Evripidis, R. (2008). Lawful Interception and Countermeasures: In the era of Internet Telephony.

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

Huang, J., Zhou, M., & Yang, D. (2007, January). Extracting Chatbot Knowledge from Online Discussion Forums. In *IJCAI* (Vol. 7, pp. 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.

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).

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.

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* (Vol. 1, pp. 203-207). IEEE.

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.

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.

Schermer, B. W., Llm, I. G., Hof, S., & Koops, B. (2016). Legal Aspects of Sweetie 2.0. Retrieved from https://www.terredeshommes.nl/sites/tdh/files/uploads/2016_10_03_sweetie_legal_aspects_report.pdf.

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.

Thanthry, N., Pendse, R., & Namuduri, K. (2005, October). Voice over IP security and law enforcement. In *Proceedings 39th Annual 2005 International Carnahan Conference on Security Technology* (pp. 246-250). IEEE.

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.