# The Cyberworld and Human Trafficking: A Double-Edged Sword

Bridget Dukes

Research Mentor: Philip Mann, J.D.

Old Dominion University

Word Count: 6298

ABSTRACT

This report examines the advantages and disadvantages associated with the growth of technology within the United States, specifically how technology, digital literacy, and cybersecurity can be used to both facilitate and combat sex trafficking and sexual exploitation on the Internet. The first part of the report addresses trafficking statistics in the United States, as well as legal intervention the country has taken against this epidemic, including an explanation of the Trafficking Victims Prevention Act and the FOSTA-SESTA bill. The second part of the report addresses the online recruitment of buyers and sellers, as well as how the use of open-source intelligence, biometric facial recognition, and hashing assist in the fight. And finally, an overview of Operation Innocent Images, the Endangered Child Alert Program, and Operation Peer Pressure, is provided to highlight steps taken to stop the victimization of innocent human beings.

**Keywords:** technology, digital literacy, cybersecurity, sex trafficking, sexual exploitation, open-source intelligence, biometric facial recognition, hashing, victimization

## INTRODUCTION

As technology and digital literacy continue to vastly accelerate and grow in many directions within the United States and throughout the world, the advantages and disadvantages associated with these assets follow suit. Technological innovation and transformation now assist in the facilitation of communication and discourse between individuals from across the globe, reaching broader audiences despite extended distances and time zones. The Internet is a virtual reality where almost anything can happen. The digital world is certainly beneficial in several ways including but not limited to: effortless access to a breadth of information, a space for collaboration and cooperation between parties in private and public sectors, and a way to gain knowledge and education without having to waste colossal amounts of time and money. Although Internet access is not universally obtainable or accessible, globally, technology's influence is making a lasting impression on about every individual from most, if not all, countries.

While the Internet Corporation for Assigned Names and Numbers (ICANN) is largely in charge of monitoring and maintaining the practicality and functionality of the Internet, no one entity specifically controls what happens within this digital space. ICANN, thus, can manage the Internet's global reach but cannot regulate it. This is not to say, however, that a country cannot shut down its Internet. Simply, this lack of regulation speaks to the amount of freedom and leeway online users have when it comes to Internet conduct, legally or illegally (Packard 2013). Fortunately, many people use technology and the Internet for positive, constructive purposes to further societal and national prosperity. Unfortunately, there are countless others who use them for negative, destructive purposes to target vulnerable, susceptible, endangered victims. This report will explore and discuss the latter.

## ADDRESSING THE DOUBLE-EDGED SWORD

As the title of this report implies, the cyberworld shares a dichotomous relationship with the use of technology in that it can be utilized for progressive and regressive purposes with little activity in the gray area. This report will focus on human trafficking as a leading issue in the digital environment and elaborate on the cyberworld's involvement in both its exacerbation and resolution in the United States. Human trafficking is a serious federal crime with penalties of up to imprisonment for life that overarchingly involves the exploitation and profiteering of human beings. Principally, there are two types of human trafficking that are by and large studied and researched within academic disciplines. This report will focus exclusively on the first type, sex trafficking, but for the sake of education, briefly touch on the second type, labor trafficking. There are numerous cases and examples where the use of technology and the Internet was enabled to facilitate both sex and labor trafficking, and therefore, neither should be given precedence over the other. This report specifically addresses sex trafficking solely because of the researcher's interest and curiosity to learn more about that subject matter.

Sex trafficking involves commercial sex acts induced by force, fraud, or coercion on any person as well as commercial sex acts in which the person induced to perform the acts has not attained the legal age of eighteen years old (22 USC 7102). Labor trafficking involves the recruitment, harboring, transportation, provision, or obtaining of a person for labor or services induced by force, fraud, or coercion (22 USC 7102). This loosely includes bonded labor, forced labor, forced child labor, peonage, and involuntary domestic servitude. The Federal Bureau of Investigation (FBI) goes as far as to say that human trafficking serves as a form of modern-day slavery, speaking to the condition and circumstances of how victims, chiefly women and children, of such acts are treated, handled, controlled, and constrained without their consent.

*Human Trafficking Statistics For the United States* (Polaris 2019)

The following statistics come from the Polaris Project webpage, a nonprofit organization fighting to end the worldwide recrudescence of human trafficking that manages the National Human Trafficking Hotline. It is important to note that while the data are valid and the most accurate representation available, there are countless human trafficking cases that are never reported and never discovered. The real number of cases is likely much higher than what is recorded and described here; however, the dark figure of crime prohibits the possibility of complete disclosure. The 2019 data report identities 22,326 victims and survivors of human trafficking. Of those, 14,597 (almost two thirds) were victims and survivors of sex trafficking. The report additionally identifies 11,500 trafficking situations and 4,384 traffickers. The demographic profile of the victims and survivors of these incidents are largely unknown, but of those that are known, minors, females, and foreign nationalities, possess a higher number of cases than their counterparts (adults, males, and U.S citizens).

The 2014 data reveals the steep increase in human trafficking cases in the United States over a relatively short period of time. Comparatively, the 2014 data report identifies 5,042 human trafficking cases. Of those, 3,598 were sex trafficking cases. Therefore, the number of sex trafficking cases reported in 2019 roughly tripled the sex trafficking cases reported in 2014.

*Human Trafficking Statistics For Virginia (Polaris 2019)*

This report will focus on statistical numbers in the Commonwealth of Virginia. The following statistics come from the National Human Trafficking Hotline webpage, which is run by the Polaris Project. As noted earlier, it is important to remember that the data recorded and described here likely underrepresents the actual number of cases within the state due to the many cases that go unreported. The 2019 statistics identify 555 contacts and 189 human trafficking

cases in Virginia. Contacts are defined as any time an individual references the state of Virginia to the Hotline during communication. Of the 189 cases, 132 were sex trafficking situations. Consistent with the Polaris Project numbers for the country, females and foreign nationalities recorded a higher number of cases than their counterparts. Inconsistent with the Polaris Project numbers for the country, adults recorded a higher number of cases than their counterparts. These results are the most accurate portrayal and representation of the degree of human trafficking in the United States.

## UNITED STATES RESPONSE TO HUMAN TRAFFICKING

The United States has taken the initiative to implement several bills and acts to combat human trafficking and its detrimental, persisting effects. An explanation of two of these anti-trafficking laws, arguably the most successful, will be discussed below.

### *The Trafficking Victims Protection Act*

The Trafficking Victims Protection Act (TVPA) was passed by the United States Congress in 2000 naming human trafficking as a federal crime (Federal Code 22 USC 7102(8)). The act substantially details a federal framework for how to address and attack human trafficking once it has been identified. Utilizing a three-pronged process that prioritizes protection, prosecution, and prevention, the TVPA stresses the importance of being proactive in human trafficking situations both nationally and internationally to decrease potential ramifications. The protection prong focuses on offering victims and survivors an abundance of necessary services and resources, from advocacy to mental and physical health outreach to legal advice and representation. The prosecution prong focuses on the criminalization of human trafficking and providing victim restitution and offender retribution. Federal prosecutors and other legal professionals go to great extents to ensure justice is served with these types of cases. The final

prong, prevention, focuses on helping potential victims and targets and decreasing the vulnerabilities and susceptibilities of those who are considered at-risk. The TVPA also introduced the Office to Monitor and Combat Trafficking in Persons in the State Department, which annually assesses the effectiveness of the prevention programs set forth (National Human Trafficking Hotline 2020).

*FOSTA-SESTA (S.3165)*

The FOSTA-SESTA bill is a combination of two bills: one from the House and one from the Senate. FOSTA, The Fight Online Sex Trafficking Act, and SESTA, The Stop Enabling Sex Traffickers Act, collectively aim to end illegal sex trafficking on the Internet. The bill package was passed in April of 2018 and has since become a topic of controversy amongst advocates, victims & survivors, sex workers, law enforcement officials (DOJ), web providers, and the general public as some believe the strengths outweigh the weaknesses and vice versa. The FOSTA-SESTA bill suggests that web servers, providers, and publishers can be held accountable and can potentially receive criminal sanctions if they are found to have engaged in the facilitation of illegal sex trafficking on their platform. For this reason, web providers can be sued civilly and prosecuted at the state and federal levels if they are suspected of partial or full responsibility for user-generated content and activity that occurs on their websites. While this bill unquestionably and unequivocally makes it easier to police sex trafficking online and identify patterns and signs across the Internet, individuals from the legal, social, and political sides of the debate continue to inquire about its constitutionality (Romano 2018).

The most controversial aspect of the FOSTA-SESTA bill is its connection to Section 230 of the Communications Decency Act. Section 230 of this Act states: “No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information

provided by another information content provider" (47 USC 230). Knowingly, FOSTA-SESTA directly opposes what is said in Section 230. The former exposes web providers, while the latter protects them. Section 230 was initially created to protect individuals who were posting objectionable content and material on the Internet from being regulated. The FOSTA-SESTA bill may be found to violate the First Amendment of the U.S. Constitution. Many argue that the FOSTA-SESTA bill violates the freedoms in the First Amendment by not allowing certain speech on these platforms. Others argue that the First Amendment may, in fact, protect harmful or offensive speech and expression in the digital world (Romano 2018).

Web providers and publishers openly expressed anger and frustration with the passing of this bill, claiming that there is an opportunity for bad people to utilize any part of a website to do bad things if they wish. They insisted that misuse of the Internet is inevitable regardless of what roadblocks and checkpoints are set up to try and stop it. As a result, web providers and publishers did one of two things. Some took the initiative and censored parts of their websites that they thought might be misused for illegal sex trafficking or banned portions altogether. For example, Craigslist chose to rid their site of the "personals" section that previously allowed users to find and communicate with local people in their area. The second option was moving their web servers out of the United States, to get around rules and restrictions set forth by laws like FOSTA-SESTA and the United States government.

*FOSTA-SESTA AND BACKPAGE*

In April of 2018, the United States Department of Justice seized and shut down Backpage.com, an advertisement website which covertly doubled as a buy and sell marketplace for sexual exploitation and trafficking. A staff report published by the Committee on Homeland Security and Governmental Affairs named Backpage as the second-largest classified advertising

website and noted its involvement in 73% of child trafficking cases that were reported to the National Center for Missing and Exploited Children (NCMEC). If the FOSTA-SESTA bill were enacted into law, Backpage could possibly be charged because they deliberately and intentionally assisted in the facilitation of illegal prostitution, sex trafficking, and child exploitation on their webpage. By censoring keywords and programming an electronic filter to delete lexicon relating to trafficking schemes, Backpage initiated participation and contribution. Backpage filtered words and phrases that could potentially indicate the trafficking of children for illegal sex purposes, including "Lolita," "teenage," "amber alert," and "schoolgirl." Previously, Section 230 of the Communications Decency Act permitted this activity, awarding immunity to Internet Service Providers like Backpage (Portman and McCaskill 2017). Eventually, its complicity and failure to step in became obvious and grounds for prosecution.

Following a federal grand jury trial, seven people involved with Backpage were indicted and charged. Of those seven were co-founders Michael Lacey and James Larkin. The CEO, Carl Ferrer, pled guilty to the charges and agreed to testify against several accomplices. The indictment against the Backpage conspirators listed 93 counts that included charges such as (1) crimes of conspiracy to facilitate prostitution using a facility in interstate or foreign commerce, (2) facilitating prostitution using a facility in interstate or foreign commerce, (3) conspiracy to commit money laundering, and (4) concealment of money laundering (Portman and McCaskill 2017). Even with the shutdown of Backpage, law enforcement must be aware that traffickers will inevitably find another space in the digital world for misconduct.

## THE ROLE OF TECHNOLOGY IN FACILITATING TRAFFICKING

With the increased use and dependence of technology in the United States, the potential for abuse is heightened when placed in the hands of the wrong individuals. Human traffickers

have subjugated the digital community by using both the surface web, the visible web that is available to the general public, and the dark web, which requires special authorization to access, to exploit vulnerable individuals, specifically children, for illegal purposes. The Internet has become an ideal space for this type of crime, providing countless opportunities for interactions among traffickers and victims. From popular social media icons, such as Twitter and Facebook, to commonly used advertisement websites, like Craigslist and eBay, traffickers are extensively manipulating and deceiving users on these platforms. There have been several cases where traffickers have even used dating websites, like Tinder and Bumble, to seek out victims from marginalized communities (i.e., women, children, foreign nationals) before beginning the grooming process.

The Internet provides traffickers with an enormous scope and access to unlimited alleyways for exploitation and recruitment. As traffickers disguise themselves and impersonate friendly, congenial identities, potential victims feel less threatened and are more easily manipulated. Within the cyberworld, there is no such thing as a paper trail but instead a digital footprint that, with the right knowledge and understanding, cybercriminals can easily erase from the public eye (Musto and Boyd 2014). This makes it harder for law enforcement to identify human trafficking and possible trafficked persons, giving traffickers a sense of anonymity and inconspicuousness. The online domain and its users have gone as far as exploiting the Internet, specifically through online classified advertisements, making it a digital market for buying and selling human beings. Classified ads, consequently, become a marketing technique and tactic of supply and demand (Barney 2018). Initially, the advertisements are used to lure in victims with false promises and then, once secured, they are used to promote the business of these same victims to buyers in search of commercial sex.

*Online Recruitment of Victims*

Human trafficking statistics mentioned above state those targeted are namely minors, females, and foreign nationals. That said, the tactics used to entice and recruit victims is similar for each of these populations. Sex traffickers mainly utilize two different types of deception and coercion to draw in victims after tirelessly working to form online bonds, friendships, and relationships with them. They go through a deliberate process to identify the suitable target and tactic to gain their trust and confidence. The first grooming technique commonly involves traffickers using a word of honor and the assurance of love, romance, affection, and a lifetime of appealing guarantees, gifts, and protection. The second grooming technique involves traffickers making promises for successful jobs and work. This ensures victims a better life with the lure of constant and secure income and benefits, which equate to prosperity, profitability, and health and happiness (Internet Safety 101 2020). Both techniques require manipulation, control, lying, and subterfuge on the trafficker's part and innocence and naivety on the victim's part.


This sample advertisement, constructed by the researcher, depicts several techniques used by human traffickers to lure in innocent young children. Some of the major red flags in this ad include: the desired age of youth, the access to quick cash, the guarantee of free ventures, the calling to bring other friends, and the contact person being a woman, for easier comfortability.

These grooming techniques prove to be particularly successful because they appeal to the vulnerability and susceptibility of the possible trafficking targets. Traffickers tend to seek out

those who show signs of substance abuse issues, destabilization within the home and peer group (i.e. emotional and physical isolation from friends and family), domestic violence, nomadic tendencies, runaway behavior, and social discrimination and separation (Internet Safety 101 2020). Offering these individuals a roof over their head, a well-paying job, consistent monetary gains, social inclusion, and the opportunity to bond with a close friend or companion manipulates them into thinking this option is a way out of their current situation. The promises and guarantees present the idea of a means to start over and get another chance at life. Often, this is just what vulnerable individuals need to hear during some of the most difficult times in their lives. Traffickers are well aware of this and use it to their advantage during online recruitment.

*Online Recruitment of Buyers*

Once victims have been successfully scouted, manipulated, and trapped, traffickers are tasked with creating the perfect online classified advertisement to show off their supply to potential clients in demand. Technological advancements have made this simpler in that now clients can interact with commercial sex actors through digital cameras, webcam footage, and online chatrooms (Barney 2018). Webcam sex is particularly dangerous because it can lead to transnational exploitation, as footage can be seen all around the word at any time. Additionally, this type of commercial sex is often completed through a livestream, which makes it easier for criminals to escape blockers and censors put in place by law enforcement officials to detect and monitor child pornography and child exploitation on the Internet. Webcam sex is not usually recorded so the probability that a digital footprint is left behind is highly unlikely. Surveillance is limited (Barney 2018).

Traffickers usually begin by finding classified ad websites that allow online advertisements for commercial sex. The shutdown of Backpage was a major downfall for

individuals partaking in sexual exploitation on the Internet, causing traffickers to find alternative domains in order to continue with their illegalities. Some of the websites that are now being used are escortindex.com, escortfish.ch, and skipthegames.eu (Vosler 2020). With a quick Google search of these websites, it is obvious that its users are targeting a specific population, as many of the advertisements contain explicit images of nude men and women. One of the hardest parts of law enforcement's job when trying to identify trafficking online is being able to tell the difference between an advertisement looking for consensual, commercial sex versus one looking for non-consensual, coercive, illegal exploitation. Several advertisements posted on these websites explicitly state no law enforcement involvement, which already raises a red flag. Many of these escort platforms, however, are designed with a software that denies automated programming systems that rake websites. This web crawling, or spidering, technique is often used by law enforcement to sift through advertisements and spot possible points of concern. Not being able to do this makes the policing and patrolling of these platforms incredibly difficult.

To recruit the perfect buyer, traffickers are very careful with the way they structure and word advertisements and their descriptions. The first aspect of the advertisement that is of interest is the images themselves. Usually just by looking at the individual in an image, considering their height, weight, and health status, it is relatively simple to identify if the services are being offered by a minor or an adult (Vosler 2020). Almost always if the image is blurred, for instance the face of the individual is censored, it is most likely a child being advertised. Once the child becomes of age, the blurring and censoring will be taken away. It is important to note again that foreign nationals are at a higher risk of being trafficked (Musto and Boyd 2014), so advertisements containing images of people of different races and ethnicities should be more heavily scrutinized, as this could be a possible indicator of exploitation. The second aspect of the

advertisement that is of interest is the description that accompanies it. The lexicon used by traffickers is peculiar and distinctive, which is fundamental in identifying patterns in sex trafficking jargon across posts and platforms. Language, movement, and the elucidation of services tend to be three of the most common similarities found in sex trafficking advertisements.

Common keywords and phrases used in sex trafficking advertisements to relay this information are listed in Figure 1 below, derived from a research study completed by Jessica Whitney, Murray E. Jennex, Aaron Elkins, and Eric Frost in 2018. Within this same study, the researchers also compiled a list of emojis and their ensuing meanings that can indicate trafficking of minors in advertisements. This compilation can be found in Figure 2 below.

| Indicator | Keywords / Phrases |
|---|---|
| Sale of Services | Donation(s), price, rose(s), dollar(s), jacks, jacksons, hundreds |
| Minor Victims | Fresh, young, new, tiny, little, new in town, girl, & college |
| Ethnicity / Race<br>African American<br>Asian / Pacific Islander<br>Caucasian<br>Latina | <br>AA, African American, Brown Sugar, Black (Beauty)<br>Pocahontas, Asian, Pacific Islander<br>Caucasian, White, European<br>Latina, Hispanic |
| Country of Origin / Nationality | South / East Asia, Eastern / Western Europe, Central America |
| Transient Activity / Movement of Victims | New in town, just arrived, weekend only, limited time, new arrival, brand new, in town for the weekend, gone, back, leaving soon, only for the weekend, new |
| Non-Independent Worker/Restricted Movement | In-call only, no outcall, only in-calls, come to me, my house |

*Figure 1: Keywords/Phrases Found in Sex Trafficking Ads* (Whitney, Jennex, Elkins, and Frost 2018)

| Emoji | Emoji Name | Emoji Meaning |
|---|---|---|
| 🌹, 💮 | Rose, rosette | used as subtle indicators of price: |
| 💗 | Growing Heart | used by pedophiles to indicate young girls |
| 🍒, 🌸 | Cherry, Cherry Blossom | used as a reference to a women's virginity, and a minor |
| ✈, 🛬 | Airplane, Airplane Arrival | Both indicate movement of the poster with the airplane arrival tending to show movement of a minor |
| 👑 | Crown | Indicated that the poster is usually a minor with a pimp controlling them |

*Figure 2: Emojis and their Meanings Found in Sex Trafficking Ads (Whitney et al. 2018)*

Knowing and understanding the language used by traffickers in their advertisements is beneficial to not only buyers looking for commercial sex, but also law enforcement officials investigating said cases. It is possible to see the same advertisements on different platforms, but with different names or descriptions associated with the same images. This is another indication of movement if the advertisements list different cities, states, or even countries where the services will be performed. The contact information will likely remain the same because the person(s) behind one of the advertisements is behind all of them. The next section of this report will go into further detail about how these similarities can be discovered and used to potentially track down traffickers and trafficked persons through analytical work. From the investigative side of this issue, being able to pick out indicators of sex trafficking on these platforms can save the lives of not just one but thousands of victims who can then be commemorated as survivors.

## THE ROLE OF TECHNOLOGY IN COMBATTING TRAFFICKING

Fortunately, the advances and developments of technology can also be positively used to combat and reverse its negative effects. The functional cybersecurity measures and initiatives that law enforcement use are highly effective in controlling, preventing, and ending this epidemic. To better understand the scope and extent to which law enforcement officials utilize technology in the digital world to tackle sex trafficking on the Internet, an interview was conducted with Agent David Desy at the Norfolk Federal Bureau of Investigation Office. While Agent Desy (2020) did note that there are technological challenges and complications that make investigations more difficult at times, cybersecurity is generally an effective, efficient means of protection against sex trafficking.

Most of the information that law enforcement officials use to uncover and solve sex trafficking cases involves the application of open-source intelligence, often referred to with the acronym OSINT. Open-source intelligence refers to information that is publicly available to everyone that can be accessed without restriction or limitation, in most cases (Vosler 2020). While the downfall of using OSINT in an investigation is the sheer volume of data that law enforcement must screen, it is beneficial because all one needs to gain access to this breadth of information is a computer, an Internet connection, and the strategies and skills to effectively search (Hassan and Hijazi 2018). For sex trafficking cases, OSINT is helpful to government departments, like the Federal Bureau of Investigation, because it does not require investigators to overcome the barriers and roadblocks associated with private and classified information. OSINT plays an important role in the processes and procedures that agents go through to find out who is behind the screen and any possible co-conspirators.

*The Categories of Open-Source Information* (Hassan and Hijazi 2018)

When conducting open-source intelligence analysis during an investigation, cyber-analysists often deal with four different types of information: open-source data (OSD), open-source information (OSINF), open-source intelligence (OSINT), and validated open-source intelligence (OSINT-V). For better understanding, their differences and similarities are explained below.

Open-source data (OSD) is essentially exactly that. It is data that comes from an original source of information. This can include data or metadata from telephone calls, video recordings, images or photographs, and the like.

Open-source information (OSINF) is slightly more complicated than open-source data because instead of coming from a primary source, it comes from a secondary source. OSINF generally is altered and changed to meet a specific purpose or need. This can include information from chapter books, textbooks, articles, dissertations, and the like that were created to focus on a certain topic, issue, or subject matter.

Open-source intelligence (OSINT) includes public information that has been discovered, filtered, and designated to meet a specific intelligence objective within context. This can include information uncovered through metadata searches, code searches, phone number searches, geospatial research, and the like. OSINT is the most popular category of open-source information and the main tool utilized in sex trafficking cases, highlighted within this report.

Lastly, validated open-source intelligence (OSINT-V) refers to intelligence with a firm conviction of certainty. This data has been checked, double checked, and confirmed by multiple sources, other than OSINT. It must be verifiable, credible, and reliable without question. This can include live interviews, discussions, or debates broadcasted through mainstream media.

*Open-Source Intelligence and the Third-Party Doctrine*

The Fourth Amendment of the United States Constitution protects citizens from unreasonable searches and seizures by the government. This includes searches and seizures conducted in both the physical and the digital worlds, ensuring places where individuals have reasonable expectations of privacy remain private and secure (Barney 2018). The third-party doctrine helps law enforcement in cases where people voluntarily and knowingly give up their expectation of privacy, where a warrant might otherwise be required. This legal doctrine specifically deals with those who intentionally give their information and data to third parties (Thompson 2014). Third parties include banks, telephone providers, e-mail servers, and internet service providers (ISPs). All of these entities are of interest to law enforcement but specifically, internet service providers, as traffickers use online classified advertisement websites to conduct their crimes voluntarily. That said, a distinction must be made between publishers and providers. Through the third-party doctrine, law enforcement agencies are not required to obtain a legal warrant to obtain information from these parties (Packard 2013), which saves time, which is of the essence, in sex trafficking cases. They may, however, need to secure a subpoena or court order, or perhaps obtain consent from the account holder.

*The Use of Open-Source Intelligence for Investigation Purposes*

The interview with Agent Desy (2020) revealed that law enforcement utilize much of the information that is publicly available to them to figure out who is responsible for these crimes. Government agencies, like the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI), work together with federal, state, and local law enforcement departments in an effort to proactively identify and end sex trafficking across the nation. Agent Desy noted the United States Marshalls have even begun assisting in the fight. Several of these agencies

have gone as far as developing child exploitation and human trafficking task forces to hone in on this deadly problem.

Law enforcement begin their investigation by filtering through classified advertisement websites that are known for facilitating sex trafficking and promoting commercial sex. Utilizing their knowledge of keywords/phrases and certain indicators of trafficking, advertisements that appear suspicious or skeptical are flagged for further analysis. The images and descriptions are analyzed and all phone numbers, email addresses, and usernames are saved for open-source intelligence purposes. It is essential to the investigation to find out where else on the Internet these same phone numbers, email addresses, and usernames appear to make connections to other commercial sex advertisements. Figure 3 below shows an example of an open-source intelligence framework tool that allows investigators to plug in countless pieces of information.


*Figure 3: OSINT Framework*

Figure 4 below shows the unlimited possibilities and opportunities available publicly to find those same phone numbers, email addresses, and usernames elsewhere on the Internet. This does not include the dozens of other pieces of information that can be investigated using this tool, including public records, business records, and archives. The OSINT Framework even includes the dark web, which Agent Desy commented about in the interview (2020), stating its use is slim in sex trafficking cases, as minors are unaware of its existence and would not have the capabilities of finding it.

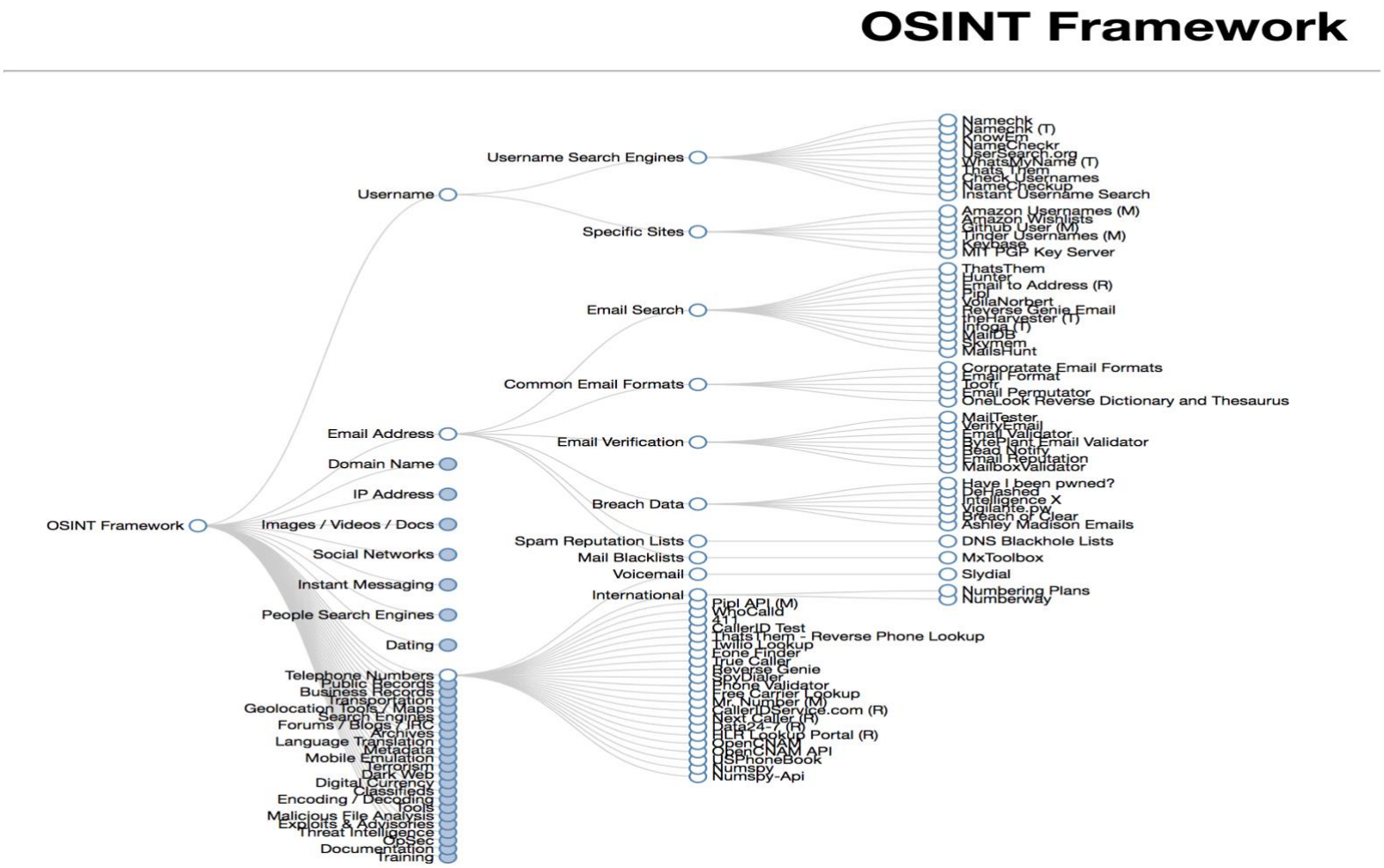


*Figure 4: OSINT Framework Extended*

Being able to piece together the identities of those behind the screen using the information within the description portion of these advertisements is principal in sex trafficking cases. Connections are what solidify the evidence, as advertising across multiple sites is common in these types of situations. A 2012 study confirmed the same phone numbers were used to advertise different individuals of different ages in different locations (Latonero et al.). Thus, there may be one individual responsible for hundreds or even thousands of advertisements. The use of the OSINT framework gives investigators a better chance at locating that individual in other spaces within the digital world, making it easier to reveal their true identities. The next step, after analyzing the descriptions of advertisements, is the analysis of the images themselves. As previously mentioned, investigators will look at the height, weight, and health status to determine if the individual in the image is a minor and will consider any blurred or censored depictions. Investigators must find where else on the Internet these images are located, and the OSINT framework has the ability to do just that. A reverse image search can be used to find similar or related images to the ones investigators are analyzing. Figure 5 below shows the countless search options for reverse imaging available in the OSINT framework.

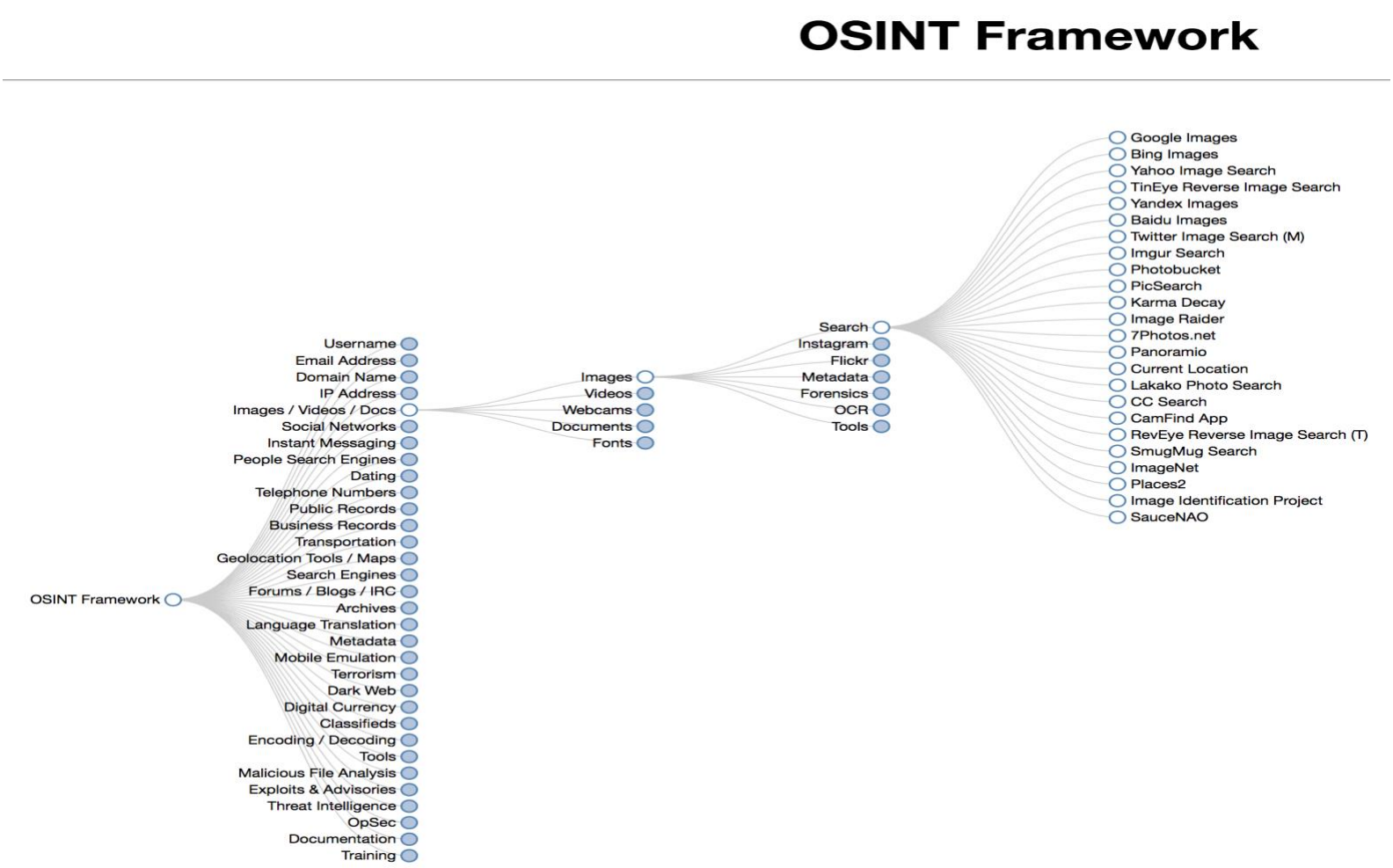


*Figure 5: OSINT Framework Reverse Imaging Options*

Reverse imaging can help connect advertisements on different platforms using the same pictures. Additionally, if a trafficking victim's family has reported them missing, their image might come up in a missing persons advertisement or post, which can further the investigation along, putting a name to a face. Agencies will often put out pictures to the public of the victims in these advertisements to see if anyone recognizes them or knows who they might be. Unfortunately, most of these victims go missing or leave on ill-fated circumstances and do not have family or friends that care enough about their disappearances, making the investigator's job harder. In these cases, biometric facial recognition can be beneficial to make matches across platforms.

### *Biometric Facial Recognition and Hashing*

Hashing, the production of a number generated from a string of text, is another cybersecurity technique that is utilized in sex trafficking cases, as it can be used to facilitate quicker comparisons of files. The three most common hashing algorithms are MD5, SHA1, and SHA 256. Hashing produces unique values for pieces of data, assigning a number to a file or a message of some sort. Agencies, like the Internet Watch Foundation, create hashes of child exploitation images and make an all-encompassing list of the hashes to share with other agencies. The list is put into a forensic software that has the ability to scan the hard drives of suspects and compare the data. Hashing saves law enforcement a lot of time, money, and resources that may otherwise be unavailable to them in sex trafficking cases.

## THE DIGITAL WORLD MEETS THE PHYSICAL WORLD

Once sex trafficking advertisements have been located, analyzed, and verified, law enforcement move onto the next step, which brings together the physical and digital worlds. Using the information they have collected in the digital world about the trafficker and the trafficked victim, law enforcement attempt to set up meetings in the physical world with these individuals.

### *Honey Trapping*

Honey trapping is commonly used in cases involving sex trafficking but is not to be confused with entrapment. If buyers click on an ad for a young minor with all the indications that the person in the images is a child, they are well aware of their actions. This is enough to prove a predisposition to commit child exploitation, which is illegal. Law enforcement officials will then consider an undercover operation, in which they represent themselves as the individual in the images and develop a romantic or sexual connection with the buyer in hopes of setting up a

meeting, otherwise known as a sting. Law enforcement can also mimic the buyer, when attempting to target and uncover the trafficker. Agent Desy (2020) further explained these undercover operations, as he was previously a member of the Special Weapons and Tactics (SWAT) team. He noted that during the meetup, there are agents watching activity on both the inside and the outside. If they are meeting a buyer, they take note of anyone else in the car. If they are meeting a seller, they take note of who is dropping off the trafficked victim, as well as who is hanging around the premise during the drop-off, which could indicate an accomplice. Undercover operations, like honey traps, are one of the most effective ways in combatting the facilitation of sex trafficking, on both the buyer and the seller's part. Policing operations, like these, ensure that justice is served for victims of human trafficking.

## CURRENT SOLUTIONS TO THE PROBLEM

The United States government, and particularly the Federal Bureau of Investigation, has taken great strides to initiate projects and programs that are aimed at ending the sexual exploitation of human beings throughout the country. A description and explanation of three of initiatives, arguably the most successful, will be discussed below.

### *Operation Innocent Images*

The United States Congress appropriates money to the FBI annually to fund Operation Innocent Images. Recent annual allocations have been roughly $10 million. This is an undercover operation that dismantles online communities and organizations that seek out children for sexual exploitation and child pornography. Similar to honey traps, agents represent themselves as children and engage in conversation with suspected pedophiles online (Federal Bureau of Investigation 2020b). Operation Innocent Images works directly with the National

Center for Missing and Exploited Children, whose main goal is to end the abduction, abuse, and exploitation of children everywhere.

### *Endangered Child Alert Program*

The FBI initiated the Endangered Child Alert Program (ECAP) in 2005 to disrupt the production of child pornography on the Internet. This program releases photos of unknown individuals, known as John/Jane Does, who have been seen in child pornographic videos and images. Their faces are plastered on the FBI website in hopes that someone will recognize and report them to the authorities. Many of the images display distinguishing features and characteristics that would make these individuals easily identifiable (Federal Bureau of Investigation 2020a). The Endangered Child Alert Program works directly with the National Center for Missing and Exploited Children, as well. The photos can be found at fbi.gov/wanted/ecap.

### *Operation Peer Pressure*

The FBI initiated Operation Peer Pressure in 2003 to attack individuals using peer-to-peer (P2P) networks to share files of child pornography. P2P networks facilitate the collection and distribution of child pornography online. Undercover agents download images of child exploitation from offenders' computers to stop the victimization of innocent children (Federal Bureau of Investigation 2014).

## CONCLUSION

The United States has become one of the most technologically advanced nations in world. For the majority of users, technology serves a means of communication, intelligence, and innovation. Unfortunately, there are users who do choose to use technology and the digital world for the wrong reasons at the expense of innocence people. The intricacies of technology allow

users to perform acts online that do not leave the same paper trail of evidence as they would in the physical world. That said, it is easier to commit wrongful acts online, and thus, easier to get away with it. Sex traffickers around the world have become experts on how to maneuver the digital community, and particularly, how to use classified ad websites to gain access to the supply and demand of commercial sex. The increase in sexual exploitation and crime on the Internet parallels the increase of technologic dependency and overreliance of its users.

Agencies like the FBI and DHS have worked endlessly to match the energy and knowledge put out by sex traffickers daily. With the use of open-source intelligence (OSINT) and hashing, they have been successful in apprehending and charging many traffickers and saving the lives of many victims, now coined as survivors. With iniatives like Operation Innocent Images, the Endangered Child Alert Program, and Operation Peer Pressure, the future of sex trafficking online does not look promising. Not only do law enforcement agencies need to stay updated and educated on digital literacy, but also children and adults around the world. This is a joint effort that needs all hands-on deck. All suspicions can be reported to the Cyber Tipline at 1-800-843-5678. In a worldwide effort to combat the widespread issue of human trafficking on the Internet, prevention, awareness, and detection are key to being on the right end of the sword.

REFERENCES

Barney, David. 2018. "Trafficking Technology: A Look at Different Approaches to Ending Technology-Facilitated Human Trafficking." *Pepperdine Law Review* 45:747-784.

Desy, David. 2020, September. Interview with FBI Agent David Desy.

Federal Bureau of Investigation. 2014. "Departments of Justice, Homeland Security Announce Child Pornography File-Sharing Crackdown." *United States Department of Justice*. Retrieved October 25, 2020. (https://archives.fbi.gov/archives/news/pressrel/press-releases/departments-of-justice-homeland-security-announce-child-pornography-file-sharing-crackdown).

Federal Bureau of Investigation. 2020a. "Endangered Child Alert Program." *United States Department of Justice*. Retrieved October 25, 2020. (https://www.fbi.gov/wanted/ecap).

Federal Bureau of Investigation. 2020b. "Operation Innocent Images." *United States Department of Justice*. Retrieved October 25, 2020. (https://www.fbi.gov/history/famous-cases/operation-innocent-images).

Hassan, Nihad and Rami Hijazi. 2018. Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence. 1st Edition. New York City, NY: Apress Media LLC.

Internet Safety 101. 2020. "Sex Trafficking." *Enough Is Enough.* Retrieved October 25, 2020. (https://internetsafety101.org/trafficking).

Latonero, Mark, Jennifer Musto, Zahleh Boyd, Ev Boyle, Amber Bissel, Karli Gibson, and Joanne Kim. 2012. "The Rise of Mobile and the Diffusion of Technology-Facilitated Trafficking." *University of Southern California, Center on Communication Leadership & Policy*.

Musto, Jennifer Lynne and Danah Boyd. 2014. "The Trafficking-Technology Nexus." *Social Politics* 21(3):461-483.

National Human Trafficking Hotline. 2020. "Federal Law. Federal Anti-Trafficking Laws." *Polaris Project*. Retrieved October 25, 2020. (https://humantraffickinghotline.org/what-human-trafficking/federal-law).

Packard, Ashley. 2013. Digital Media Law. 2nd edition. West Sussex, UK: Wiley-Blackwell.

Polaris. 2019. "2019 Data Report. The U.S. National Human Trafficking Hotline. More Victims and Survivors Speaking for Themselves." *Polaris Project*. Retrieved October 25, 2020. (https://polarisproject.org/wp-content/uploads/2019/09/Polaris-2019-US-National-Human-Trafficking-Hotline-Data-Report.pdf).

Portman, Rob and Claire McCaskill. 2017. "Backpage.com's Knowing Facilitation of Online Sex Trafficking." *United States Senate Committee on Homeland Security and Governmental Affairs*. Retrieved October 25, 2020. (https://www.hsgac.senate.gov/imo/media/doc/Backpage%20Report%202017.01.10%20FINAL.pdf).

Romano, Aja. 2018. "A New Law Intended to Curb Sex Trafficking Threatens the Future of the Tnternet as We Know It." *Vox Media, LLC.* Retrieved October 25, 2020. (https://www.vox.com/culture/2018/4/13/17172762/fosta-sesta-backpage-230-internet-freedom).

Thompson II, Richard M. 2014. "The Fourth Amendment Third-Party Doctrine." *Congressional Research Service of the United States Congress*. Retrieved October 25, 2020. (https://fas.org/sgp/crs/misc/R43586.pdf).

Vosler, Chase A. 2020. “Identifying Sex Trafficking in a Digital Environment Through Open Source Intelligence.” Master’s Thesis, Department of Cybersecurity, Old Dominion University.

Whitney, Jessica, Murray Jennex, and Aaron Elkins. 2018. “Don’t Want to Get Caught? Don’t Say It: The Use of Emojis in Online Human Sex Trafficking Ads.” Paper presented at the Hawaii International Conference on System Sciences. January 3-6, Waikōloa Village, HI.