From the Street Corner to the Digital World: How the Digital Age Impacts Sex Trafficking Detection and Data Collection

Jennifer Middleton

Contents

Abstract

Although sex trafficking has been a social issue long before the conception of the Internet, the arrival of a worldwide network has increased sex traffickers' reach and anonymity, potential victims' vulnerability, and buyers' selection, driving an explosion in sex trafficking and exploitation. Via the Internet, sex traffickers can advertise trafficking victims anywhere in the world. However, data mining initiatives allow law enforcement agencies and researchers to gather and analyze data from web pages that potentially contain sex trafficking information. Addressing the need for public security in this domain requires the use of these technologies via data aggregation, analytics, and computational forensics. For example, DARPA created the Memex program in order to index the data from web pages on the deep web. The Memex program shares similarities with popular search engines, which index the web pages that most users access every day. Gathering and analyzing data in new ways will allow for a greater understanding of how sex trafficking is being performed in the digital world by providing insight into the modus operandi of sex traffickers and providing valuable information

J. Middleton (✉)
Human Trafficking Research Initiative, Kent School of Social Work, University of Louisville,
Louisville, KY, USA
e-mail: jennifer.s.middleton@gmail.com

J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, https://doi.org/10.1007/978-3-319-63192-9_23-1

about the victims themselves. This, in turn, will inform more effective public security responses and victim aid to these crimes.

Keywords
Human trafficking · Sex trafficking · Labor trafficking · Information and communications technology (ICT) · Cybercrime · Data mining · Memex · Deep web

Introduction

Trafficking existed before the conception of the Internet, but the arrival of a worldwide network increased traffickers' reach and anonymity, potential victims' vulnerability, and buyers' selection. This chapter examines how the digital age has affected human trafficking in general – and sex trafficking in particular – as well as the actions being taken to prevent sex trafficking in the United States and abroad. First, the chapter discusses the victims of trafficking. Understanding the targeted individuals and what risks they face is crucial to understanding the process of being trafficked for sexual exploitation. Next, the focus shifts to traffickers and how they operate in the digital world. Traffickers use a variety of digital tools to lure victims and attract buyers. Following that, the chapter discusses how traffickers leverage technology for their benefit. Finally, the chapter analyzes current and upcoming prevention methods. There are many programs and initiatives in place that focus specifically on combatting sex trafficking. Understanding how they address the challenges inherent in investigating sex trafficking provides a more comprehensive understanding of all types of trafficking in the digital world.

Victims

The Victims of Trafficking and Violence Protection Act of 2000, enacted by the US Congress, defines labor trafficking and other types of trafficking for services as "the recruitment, harboring, transportation, provision, or obtaining of a person for labor or services, through the use of force, fraud, or coercion for the purpose of subjection to involuntary servitude, peonage, debt bondage, or slavery" (U.S. Congress 2000). It goes on to discuss sex trafficking as one of the "severe forms of trafficking in persons" where "a commercial sex act is induced by force, fraud, or coercion, or, in which the person induced to perform should an act has not attained 18 years yet" (U.S. Congress 2000). With all the information of the Internet at their fingertips, it is easier than ever before for traffickers to recruit victims from social media like Facebook and Twitter. Similarly, due to the information available on the Internet – such as location check-ins on social media – traffickers can potentially locate and transport the victim via coercion or force. However, the trafficker does not have to utilize force, fraud, or coercion in order to be guilty for trafficking a minor. If the victim is under 18 years old, the trafficker is guilty simply by persuading a minor to engage in a sexual act (U.S. Congress 2000).

The United Nations Global Initiative to Fight Human Trafficking (UN-GIFT) found that trafficking victims are used in a variety of industries, such as: "construction, manufacturing (e.g., textile, metal, wood), industrial fishing and fisheries, agriculture, domestic servitude, mining, quarrying, food processing, forestry, leather and tanning, carpet-weaving, [and] livestock" (International Organization for Migration 2009). Due to the ease of communication, traffickers can promise opportunities of gainful employment in other regions or countries. However, when the victims arrive, the traffickers force them to do jobs such as those mentioned above. The victims may be forced to work without pay or may have their identification papers taken from them which prevents them from escaping the trafficker.

In their white paper, Chawki and Wahab (2005) included an account of a trafficking victim from Mali. The authors discuss how information and communication technologies, or ICTs, are often used for criminal means such as trafficking. The victim, Seba, was contacted in chat room; the traffickers promised Seba could live with their family in Paris, France, and get a French education. Instead she was made to cook, clean, and care for the traffickers' children:

> One day I told her that I wanted to go to school. She replied that she had not brought me to France to go to school, but to work for her and for her child.
>
> I was so tired and run down. I had problems with my teeth; some my *[*sic*]* cheek would swell and the pain would be terrible. Sometimes I had stomachaches, but when I was ill I still had to work. Sometimes when I was pain *[*sic*]* I would cry, but my mistress would beat me.
>
> I slept on the floor, my food was her leftovers. I was not allowed to take food from the refrigerator like them, if I would take food, she would slap me. She beat me with the broom, with kitchen tools, or whipped with electric cable. Sometimes I would bleed; I still have marks on my body.

Seba described how at one point the traffickers threw her out, but she did "understand anything" and simply wandered the streets until her traffickers found her and took her back to their house. She was then tied up, beaten, and had chili peppers rubbed into her wounds (Chawki and Wahab 2005). Seba's experience illustrates not only how trafficking victims are often lured but also the hopelessness they face when they are trafficked. Even if they are able to escape, or let go in Seba's case, trafficking victims often find themselves in unfamiliar countries or regions where they do not know the language or culture. Victims are removed from their support systems and abused and may not know where to go for help.

In cases of transnational trafficking, victims may not even feel they can go to the authorities for help because they are in the country illegally. In the United States, the department of Immigration and Customs Enforcement (ICE) routinely raids companies that may have undocumented migrants. Some local laws stipulate that when law enforcement officers stop individuals to check their immigration status, they can also check to see whether the individual has other violations (Brennan 2010; Gardner 2015; Weitzer 2014). Migrant workers could be victims of trafficking, but due to government policies, they may not come forward for fear of jail time or the risk of being deported. Even if the victim entered the country legally, all the trafficker has to do to coerce the victim is to hold their travel documentation hostage (Landesman 2004). This tactic can affect all victims of transnational trafficking.

In regard to the issue of sex trafficking, it is important to note the difference between sex trafficking and commercial sexual exploitation (CSE). Human rights organization Love146 differentiates sex trafficking from commercial sexual exploitation by the presence of a third party: “CSE is defined as the abuse of power differentials or the exploitation of a person’s vulnerabilities in order to exchange a sexual act(s) in exchange for something of value” (Kim et al. 2015). Commercial sexual exploitation involves the trafficker providing something the victim needs such as a place to stay in exchange for sexual acts. Sex trafficking involves a third party, the buyer, benefiting from the victim. In exchange, the buyer pays the trafficker for the time spent with the victim.

Although researchers are aware of the types of victims that traffickers target online, as well as the potential risks victims face while browsing the Internet, very little empirical research exists on the prevalence of child sex trafficking on the Internet (Mitchell and Boyd 2014). A study conducted in 2009 concluded that 5% of youth, between the ages of 1 and 17, experienced sexual victimization within their lifetime (Finkelhor et al. 2009). The same year, the National Crime Victimization Survey found that teenagers, between the ages of 12 and 15, experience violent crime victimization at a rate more than double the national average (Truman and Rand 2009). Online sex trafficking represents a subset of these statistics.

Victims of sex trafficking tend to be young women originating from all over the world. A report from the Human Trafficking Data Collection and Reporting Center found that 70% of all sex trafficking victims are under the age of 24, and 30% are under the age of 18 (Farrell et al. 2008). The same report found that an overwhelming majority of those victims were young adult women and juvenile girls, 98% and 94%, respectively (Farrell et al. 2008). The report documented victims who originated primarily from within the United States and developing countries such as Mexico, China, and South Korea. Traffickers also target juvenile boys and young men, but their primary victims are young women and underage girls. While the research to examine online victims of sex trafficking is still nascent, it is safe to say that the number of victims is significant. Furthermore, the number of victims is likely to rise in the coming years as it becomes easier and easier to connect and communicate on the Internet.

Traffickers

Before the advent of the Internet, traffickers and sexual predators needed to have physical access to their potential victims. However, with the popularity of chat rooms in the 1990s, and the rise of social media in the 2000s, traffickers can electronically connect with victims regardless of physical distance. Traffickers are able to advertise opportunities to work and live abroad and can attract victims across international borders (Sciadas 2005). Sexual predators utilize the Internet to exchange child pornography, attempt to lure victims and engage them in sexual acts, encourage juveniles and young adult victims to send pornographic photos, and exploit women and children for sexual tourism (Taylor et al. 2015). Sexual tourism can be defined as traveling "with the intent to engage in sexual behavior for commercial gain and/or personal gratification" (Taylor et al. 2015). The clients are often wealthy men who travel to a developing or third-world country to engage in sexual acts that are either illegal or viewed as deviant in their own country; they usually seek out adolescents and children (Taylor et al. 2015). The risks to victims online are myriad.

Organized crime groups can easily extend their reach internationally by harnessing the technology available to them. The United Nations Convention against transnational organized crime declared that transnational organized crime is a critical security issue for the world's nations to address (Lavorgna 2003). Transnational groups advertise the opportunity to travel to a new country or region and promise the victims they will help secure travel plans, living accommodations, and visa documentation once they arrive (Sciadas 2005).

Typical examples for job opportunities include positions such as dancers or servers at a restaurant (Stoecker 2000). After luring the victim, the trafficker offering the position may coerce the victim into slave-like working conditions, become the victim's pimp, or may only be the bottom rung in a human trafficking chain. The trafficker might only be serving as a local representative of the criminal group, whose responsibility it is to send the victim to an intermediary contact in another city or country (Stoecker 2000). Once the victim has been transported, the local trafficker or intermediary contact establishes a connection with a buyer, and the victim's services are sold. As opposed to the drugs and firearms, a criminal group may also sell; they "can sell a human over and over again" (Gardner 2015).

Traffickers utilize many electronic venues in order to lure and sell their victims. Websites such as Craigslist and Backpage easily allow the trafficker to advertise the victim as an escort, masseuse, or companion. The use of classified advertisement websites has allowed traffickers to continue to advertise in the physical world but has also established "'virtual red light districts' [to] provide a low risk environment for buyers to connect with sellers" (Ibanez and Suthers 2014). Victims are advertised ubiquitously for the ease of potential clients. One law enforcement investigator said, "Almost everyone being prostituted is advertised on some type of advertising or social media site" (Mitchell and Boyd 2014).

The process for luring a younger victim is different than those that can feasibly travel by themselves for the promise of a job. Generally, when attempting to lure a child or young teenager, the trafficker attempts to gain the victim's trust and build a relationship. Traffickers use many different tactics to engage their victims. The trafficker may begin indirectly, by sending a link to a pornographic site or engaging in a sexual conversation. The trafficker may also try to normalize sex acts, such as juveniles having sex with adults (Taylor et al. 2015). As the relationship progresses, the trafficker will attempt to isolate the victim – to alienate them from their support network of family and friends – and establish reliance on the trafficker (Finkelhor et al. 2009). Older children and teenagers seem to be the most at risk for these interactions. Young people in this age range often have Internet access, but a parent or guardian may not be monitoring their activity. Traffickers attempt to establish trust and dependency by physically meeting up with the victim and then presenting the victim with gifts, food, or money. Eventually these seemingly kind acts lead to the trafficker asking them for sexual acts in exchange. Once the trafficker has the victim in their possession, the offender may utilize any combination of attempts to ensure the victim's captivity and dependency. The offender may physically punish or threaten the victim or their family in order to ensure the victim's submission (Dixon 2013).

Mitchell and Boyd reported that over half of the law enforcement investigators included in the study found technology to be nearly inseparable from their sex trafficking cases (Mitchell and Boyd 2014). The law enforcement officials noted that between 76% and 100% of their cases involved technology in some way (Mitchell and Boyd 2014). When technology was a part of the case, it played a "very important role" in 33% of cases and an "extremely important role" in 60% of the cases (Mitchell and Boyd 2014). One law enforcement official explained the value of technology in relation to sex trafficking: "The crime is the same, the way they communicate to commit the crime has changed" (Mitchell and Boyd 2014). The Internet is invaluable to traffickers and buyers because it allows them to expand their habits to the digital world with slight modification and significant benefit: perceived safety and anonymity and a much greater pool of potential clients and victims.

Technology Used for Trafficking

Due in part to their relative anonymity, traffickers have routinely utilized digital classified websites, such as Backpage, Craigslist, and social media sites, in order to advertise their victims. Traffickers also utilize everything from niche websites to smartphone apps to advertise to and communicate with clients (Mitchell and Boyd 2014). The ubiquitous nature of technology allows traffickers and buyers to communicate seamlessly. Buyers can access the advertisements as easily as they can look for a used television. They can peruse the ads from their phone, tablet, or computer while they are at work, school, or home. With the aid of classified websites and social media, traffickers have attempted to normalize the process of buying or renting a victim, so that the buyer is more detached from the trafficker, the victim, and the act. The virtual experience allows the buyer to perform their research to decide which victim to contact and make a decision in a low-risk environment. They can do everything, except for the physical act, from the comfort of their normal surroundings (e.g., their own home, their office).

Prepaid, or burner, phones have helped to increase traffickers' accessibility and anonymity. Many traffickers have prepaid phones set up to link themselves to their advertisements. Traffickers often link multiple advertisements to their prepaid phone number. Prepaid phones are convenient because in several countries, purchase of a prepaid phone does not currently require personal information or a service contract to set up. Law enforcement cannot link the prepaid phone back to the trafficker unless there is identifying information linked to the prepaid account. The only information that law enforcement can obtain is the original location of the prepaid phone's purchase (Ibanez and Suthers 2014). A content analysis of the Louisville, Kentucky, Backpage website found that adult advertisements had contact area codes from all over the United States (Hayden 2014).

A significant portion of sex trafficking occurs via "adult classified" advertisements. Sex traffickers utilize classified advertisements to promote trafficked victims. Adult classifieds, and similar posts promoting prostitution or sexual tourism, appear on both the surface web and the deep web. The surface web, in this context, can be defined as sites indexed by search engines such as Google, Yahoo, and Bing. Conversely, the deep web is the majority of the Internet that is not indexed by search engines. Therefore, the user needs specific software, configurations, or information in order to access a given website or web page. On the surface web, Backpage.com has been the most common location to find adult classifieds over the past several years (Goldman 2016).

In the past, both Craigslist and Backpage were accused of facilitating sex trafficking (Dixon 2013; Hayden 2014). However, Craigslist removed its adult services in 2010. Since that time, Backpage became the dominant force in the commercial sex advertising market (Goldman 2016). The company's total sales are more than $150 million; $100 million comes from adult classified advertisements (Goldman 2016). There are other niche sites that offer adult classifieds such as: Myredbook.com, TheEroticReview.com, CityVibe.com, and NaughtyReviews.com. However, the Backpage competitors have a stigma associated with them (Ibanez and Suthers 2014). Backpage is more commonplace and thus is not considered merely a site that a "John" or sexual tourist would visit (Ibanez and Suthers 2014).

Special events, namely, sporting events, have been found to increase online sex trafficking sales. Hayden (2014) analyzed Backpage adult advertisements in Louisville, Kentucky, for 15 months. The study concluded that on average, there were 53 adult ads posted per day. During major events such as the Kentucky Derby, the number of postings per day increased (Hayden 2014). As mentioned above, Hayden (2014) also found that area codes from across the United States were included in the local sex ads. Ibanez and Suthers (2014) found that traffickers frequently change locations along circuits or routes. It is possible that the distant area codes recorded by Hayden were contacts for traffickers who were staying in Louisville, Kentucky, temporarily as part of their trafficking circuit.

Senators Rob Portman and Claire McCaskill have led the Permanent Subcommittee on Investigations' attempts to gather information regarding the adult ads on Backpage. Carl Ferrer, CEO of Backpage, has been uncooperative with the subcommittee (Everett 2016). In addition to reportedly stalling Portman and McCaskill's efforts, Ferrer failed to comply with a subpoena (Everett 2016). The Senate subcommittee examined Backpage's current policies for processing adult classifieds. The National Center for Missing and Exploited Children testified, "71% of all reports of suspected child sex trafficking" were found to be linked to Backpage (Goldman 2016). The subcommittee found that Backpage edits the content of advertisements to remove potentially illegal references to prostitution before publishing the post:

> . . .we find substantial evidence that Backpage edits the content of some ads, including by deleting words and images, before publication. The record indicates that in some cases, these deletions likely served to remove evidence of the illegality of the underlying transaction. Specifically, as part of its moderation process, it appears that Backpage will delete particular words or images from an advertisement before posting it to the web *[*sic*]*, if those words or images violate its terms of service. . . The Subcommittee attempted to take the testimony of two Backpage employees in charge of its moderation practices, but they refused to testify on the grounds that it might incriminate them. The Subcommittee, however, obtained evidence demonstrating that, from 2010 to 2012, when Backpage outsourced its moderation work to India, it did delete certain images, words, or phrases from "adult" advertisements. The Subcommittee's subpoena seeks to understand whether Backpage's current practices have the purpose or effect of removing images or text that could alert law enforcement to the nature and extent of the transaction being offered. Backpage refuses to produce that information. (Portman and McCaskill 2016)

The subcommittee's assertion is that by editing the text or image associated with an adult classified, Backpage obfuscated classified posts that may have been directly linked to sex trafficking. By removing information from the post, law enforcement officials are not as readily able to investigate potential sex trafficking cases. Furthermore, by editing the classified advertisement, rather than simply not publishing it or reporting it to law enforcement authorities, Backpage may have aided sex traffickers.

Additionally, the subcommittee found that Backpage removed the metadata from images on its website (Portman and McCaskill 2016). Metadata in photographs often contains identifying information such as who owns the file, what camera took the photo, and keywords to make the image searchable. Removing the metadata from a file provides a layer of privacy for the owner of the file. In e-commerce sites such as Backpage or Craigslist, removing the metadata serves to protect the user from potential cybercriminals who might use that information to identify and exploit the user. Therefore, it is beneficial for Backpage's users that the website removes the metadata. However, in a potentially illegal classified advertisement, it would be very beneficial to law enforcement for the metadata to be available for their investigations.

In March 2016, the Senate subcommittee declared Backpage in contempt of Congress. Officially designating Backpage as being in contempt is an important step toward determining Backpage's guilt or innocence concerning its affiliation with sex trafficking. The designation of contempt allows the Senate Legal Counsel to file a lawsuit (Goldman 2016). Backpage stated that the company would welcome a lawsuit so that the courts can determine if Backpage's practices are illegal or if the First Amendment protects the company's current operating procedure (Goldman 2016). The courts ruled that Backpage.com was legally protected by Section 230 of the Communications Decency Act, so citizens, victim rights advocates, and policy makers demanded a change to the current laws protecting websites such as Backpage.com.

As a result of bipartisan efforts at the federal level in the Unites States, on April 11, 2018, President Donald Trump signed a combination of bills into law to better protect victims of online sex trafficking. The bills include the Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA) and the Stop Enabling Sex Traffickers Act (SESTA). The legislation opens more avenues for victims of online sex trafficking to legally pursue websites that facilitate trafficking by amending Section 230, making it easier for federal and state prosecutors and private citizens to go after platforms whose sites have been used by traffickers.

Technology Used Against Trafficking

Although sex traffickers and buyers are difficult to identify on the Internet, evidence of their criminal acts will become more visible as sex trafficking continues to shift into the digital world (Ibanez and Suthers 2014). Researchers and law enforcement agencies are using new technologies and various methods to identify trafficking and stem its spread. Utilizing data mining in order to collect and analyze aggregate data appears to be the most promising approach at this time. Researchers using data mining employ strategies to group, classify, and analyze data. Examining aggregated data allows patterns to emerge.

The more data that is gathered and analyzed, the more effective these investigative efforts will become. On the surface web, researchers gather data from suspected sex trafficking posts on websites and social media apps, in order to identify and analyze sex trafficking patterns. As noted above, Ibanez and Suthers (2014) tracked traffickers' movements across the country and concluded that traffickers often travel in circuits, advertising their victims. Similarly, Hayden (2014) marked suspected traffickers' approximate locations based on the telephone information the traffickers listed for their Backpage.com advertisements.

In 2015, Thorn, a nonprofit organization that focuses on the prevention of child sexual exploitation, launched the Spotlight program to help law enforcement officials identify and solve child sex trafficking cases. Spotlight is being used in 48 states, has helped identify more than 360 victims, and lead to the arrests of more than 60 traffickers (Thorn 2015). The program utilizes machine-learning algorithms in order to prioritize leads (Thorn 2016). Law enforcement agencies can access Spotlight for free in order to investigate sex trafficking in their area (Thorn 2016). Spotlight serves as an example of initiatives that organizations are harnessing, utilizing data mining to categorize and analyze potential sex trafficking cases.

To data mine potential sex trafficking cases on the deep web, Defense Advanced Research Projects Agency (DARPA) developed the Memex program. DARPA is an agency of the US Department of Defense whose goal is to develop greater technologies for improving national security. The name and concept behind "Memex" refers to a hypothetical device pioneered by Vannevar Bush that stores vast amounts of information and records and also possesses supplementary functions for its stored data (Shen n.d.). Memex focuses on identifying fraudulent advertisements and job postings used to lure potential victims, so traffickers can abduct them (Greenemeier 2015). The goal of Memex is “to invent better methods for interacting with and sharing information, so users can quickly and thoroughly organize and search subsets of information relevant to their individual interests” (Shen n.d.).

Memex will strive to meet its goals by utilizing domain-specific indexing, domain-specific search, and Department of Defense (DoD)-specified applications (Shen n.d). Sex trafficking is difficult to track in part because sex traffickers utilize temporary advertisements, as well as peer-to-peer connections, both of which reside in the deep web and, thus, are not indexed by traditional search engines (Greenemeier 2015). Researchers and law enforcement officials will be able to utilize Memex’s search capabilities to identify potential sex trafficking sources which they would have had no way of accessing on the surface web.

In addition to its search features, Memex also boasts the ability to link together data found within search results (Greenemeier 2015). When key patterns, similarities, and discoveries are detected, certain algorithms within Memex will generate a statistical score for significance. An important example is the Tika-Jaccard Similarity algorithm. This algorithm attempts to capture statistical similarities from image or video metadata, by weighing this metadata against a “golden feature set.” The golden feature set is a known set of metadata which represents sex trafficking activity. The metadata often includes exchangeable image file format (EXIF), Flash, RGB, Color Space, Camera Make, and Camera Model Serial Number. Mattman (2016) provides the following pseudocode of the Tika-Jaccard Similarity algorithm:

```
input: directory of files d
output: scores s for all files in d

goldSet:= {}
allMetadata:= {}
scores:= {}

for file in d:
text, metadata:= tika.parse(file)
  goldSet:= goldSet $\bigcup$ metadata.keys
  allMetadata[file]:= metadata

 goldenSetSize:= |goldSet|

  for file in allMetadata.keys:
  overlap:=|allMetadata[file]$\bigcap$ goldSet|
  score:= overlap / goldenSetSize
  scores[file]:= score

 return scores
```

In the above algorithm, lines 1–2 initialize the input and output variables. Next, lines 4–6 initialize the “goldSet,” “allMetadata,” and “scores” variables as arrays to organize the input and output data. Lines 8–11 creates a “for loop” to gather the metadata from a known human trafficking data set. This loop will run until it has processed all the files within the data set. Line 13 sets the size of “goldSet” array, which will be used to calculate the statistical score of the suspected human trafficking data set. Lines 15–18 compare the suspected human trafficking data to the known human trafficking data. Line 20 returns the scores for each file in the suspected human trafficking data set. The researcher can then analyze the scores of the suspected human trafficking data to determine if the data set is likely to be linked to trafficking.

The data can be displayed visually in order to identify spatial and temporal maps in real time (Daire 2015). Memex is already being used to a limited extent. The New York District Attorney’s Office stated that Memex has aided over 20 active sex trafficking investigations, as well as 9 open indictments (Daire 2015). Traditional search engines merely display various search results, ranked by algorithms that prioritize the links the engine estimates will be the most helpful. Each search result is isolated to itself; there is no connection between the sources of data. Memex’s ability to link data points will present patterns that were not clear before, on both the deep web and surface web.

Although Memex is primarily being applied to sex trafficking cases at this time, its associative ability to index, organize, and link data has innumerable applications. Law enforcement agencies can utilize Memex to investigate similar crimes, such as firearm and drug trafficking (Greenemeier 2015). The domain-specific searching lends itself to investigating other major issues such as terrorism and disease tracking and response (Greenemeier 2015). Although the primary goal of Memex is to combat human trafficking, other organizations are also interested in using Memex to search and link data not related to crime at all. For example, NASA JPL is interested in utilizing Memex to catalog spacecraft data, a hefty task that is usually daunting for scientists (Churgwin 2015). Additionally, Memex also has capabilities of crawling and linking data from the surface web. One of the most important Memex utilities that perform this function is TJBatchExtractor. Specifically designed to harvest adult classifieds and female escort information from Backpage, TJBatchExtractor performs data collection and analysis on all available data across multiple advertisements. Specifically, TJBatchExtractor harvests data such as age, physical measurements, ethnicity, eye and hair color, phone numbers, and emails. The data is then linked together, and the same analyses can be performed as though the information had been gathered from the deep web.

The Memex team is creating a “dark web crawler” in order to index the dark web, the region of the Internet accessible only via Tor or peer-to-peer software (Greenemeier 2015). This is currently being accomplished by utilizing multiple web crawlers with specific guidance. The major web crawlers listed in the DARPA open catalog each serve a distinct purpose: ACHE enables focused crawling; Arachnado allows for deep crawling; Distributed Frontera integrates decision-making for logic and policies to be used when crawling; Frontera can be used when storage and priorities are needed; HSProbe (The Tor Hidden Service Prober) can extract hidden content; SourcePin assists with new website discovery (Shen n.d.). Memex even has the capability to crawl web pages that require log-ins. Using a utility called "Autologin," Memex can crawl any given web page of any given website, when provided with proper user credentials (Hyperion Gray 2014). Additionally, Memex also includes tools which provide machine learning, infrastructure, visualization, security, analytics, statistics, experimentation support, processing, distributed programming, and application program interface(API) (Shen n.d.). The complexity of Memex is an astounding achievement that has arisen from combating human and sex trafficking. Indexing the dark web will provide a greater understanding of the scope of activity that takes place in one of the most inaccessible parts of the Internet. While not all activity on the dark web is criminal in nature, advertisements for criminal activity do exist. Identifying locations on the dark web is a significant step toward tracking the cybercrime that is facilitated there.

The prospect of such a powerful data mining tool raises questions about the privacy of innocent users on the Internet. Data collection is one of the primary functions of Memex, and in the wrong hands, it seems as though it has the capabilities to gather sensitive user information, such as bank account information. The DARPA Open Catalogue currently lists 12 projects whose primary purpose is data collection (Shen n.d.). These data collection projects include web crawlers and tools that supplement and interpret the gathered data. Memex program manager Christopher White made a conscious decision for Memex to avoid password-protected content (Greenemeier 2015). The Memex program is not interested in "deanonymizing or attributing identity to servers or IP addresses, or accessing information not intended to be publicly available" (Shen n.d.). Significantly, the Memex project is mostly composed of open-source tools, all available on Github through the DARPA Open Catalogue (Greenemeier 2015). One of the most fascinating characteristics of the Memex program is the enormous amount of collaboration behind it. Memex has received aid from academia, government, industry, and open-source development. Some of the major contributors include the US Naval Research Laboratory, Georgetown University, Columbia University, Carnegie Mellon University, NASA Jet Propulsion Laboratories (JPL), Kitware, and Continuum Analytics (Shen n.d.). The open-source nature of the code will provide unbiased information about how the Memex team built the tools and how researchers and law enforcement agencies use those tools. The prevention of crimes such as sex trafficking is an objectively positive goal, but innocent users' personal information need not be sacrificed in order to prevent those crimes.

Conclusion

The conception of the Internet has increased the scope of trafficking. Due to our interconnected world, victims can be targeted from any location around the world, traffickers can advertise to potential buyers with a sense of anonymity, and buyers can rent or buy victims from the comfort of their home. Although we know the demographics and groups traffickers target, there is dearth of prevalence data to speak to how many victims are affected by trafficking. However, traffickers will continue to utilize technology to their advantage, and as their methods are analyzed, researchers will gain a better understanding of how to prevent trafficking.

Programs such as Spotlight and Memex will allow researchers and law enforcement agencies to organize data in new ways in order to find patterns and draw conclusions. As data is collected, and these technological approaches mature, researchers will have more evidence regarding how trafficking is conducted in the digital world. While traffickers are able to obfuscate their identities online, the tools discussed above provide an advantage to law enforcement officials in their efforts to track and prevent trafficking. Technology has initially negatively impacted anti-trafficking efforts by enhancing traffickers' ability to recruit and sell victims for sex trafficking, but emerging programs such as those discussed in this chapter are narrowing the gap between traffickers and law enforcement responses to address the issue.

References

106th Congress. (2000). Victims of trafficking and violence protection act of 2000, public law 106–386. Retrieved from http://www.state.gov/j/tip/laws/61124.htm

Brennan, D. (2010). Thoughts on finding an assisting individuals in forced labor in the USA. *Sexualities,* 13(2), p139–152.

Chirgwin, R. (2015). JPL joins DARPA's Memex project. The Register. Retrieved from: http://www.theregister.co.uk/2015/05/27/jpl_joins_darpas_memex_project/

Chawki, M. & Wahab, M. (2005). Technology is a Double-Edged Sword: Illegal Human Trafficking in the Information Age. *Computer Crime Research Center.*

Daire, S. (2015). Memex helps find human trafficking cases online. Human Trafficking Center. Retrieved from http://humantraffickingcenter.org/posts-by-htc-associates/memex-helps-find-human-trafficking-cases-online/

Dixon, Jr. Judge H. B. (2013). Human trafficking and the internet* (*and other technologies, too). *The Judges' Journal,* Vol. 52 (1).

Everett, B. (March 11, 2016). Senate set to hold classified ads website in contempt: The standoff is over its alleged role in facilitating sex trafficking, which backpage.com has denied. *Politico*. Retrieved from http://www.politico.com/story/2016/03/senate-accuses-backpage-sex-trafficking-220646

Farrell, A., McDevitt, J. & Fahy, S. (June 2008). Understanding and improving law enforcement responses to human trafficking, final report. *Human Trafficking Data Collection and Reporting Center Research and Technical Reports,* Paper 1, pp.71–73.

Finkelhor, D., Turner, R. K. & Turner, H. A. (2009). Lifetime assessment of poly-victimization in a national sample of children and youth. *Child Abuse & Neglect*, Vol. 33 (7), pp.403–411.

Gardner, S (2015). TraffickACTS.Org: Turning Advocacy to Action to Combat Human Trafficking Through the Public. *MA IDS Thesis Projects.* Paper 16.

Greenemeier, L. (February 8, 2015). Human traffickers caught on hidden Internet: a new set of search tools called Memex, developed by DARPA, peers into the "deep Web" to reveal illegal activity. *Scientific American*. Retrieved from http://www.scientificamerican.com/article/human-traffickers- caught-on-hidden-internet/

Goldman, D. (March 17, 2016). Senate hold backpage.com in contempt, sparking likely free speech fight. *CNN Money.* Retrieved from http://money.cnn.com/2016/03/17/technology/backpage-contempt/

Hyperion Gray. (2014). *Autologin*. [Computer program]. Retrieved from: https://github.com/TeamHG-Memex/autologin/blob/master/docs/intro.rst

Hayden, T. C. (2014). A content analysis of backpage.com advertisements in Louisville, Kentucky. *Sixth Annual Interdisciplinary Conference on Human Trafficking, Paper 10.*

Ibanez M., & Suthers, D. D. (2014). Detection of domestic human trafficking indicators and movement trends using content available on open internet sources. *47th Hawaii International Conference on System Science*. Waikoloa, HI, pp.1556–1565.

International Organization for Migration (2009). Caring for Trafficked Persons: Guidance for Health Care Providers.

Kim, E., MacLaughlin, J., & Fuentes, C. (2015). Not a number: Resources to support a whole-school or entire-system response. New Haven, CT: Love146.