Published In International Journal of Cyber Warfare and Terrorism (IJCWT) Vol. 12, Issue 2, p. 41-49. First published, International Conference on Information Warfare and Security, Denver, Colorado, March 24-26.

The Emergence of Cyber Activity as a Gateway to Human Trafficking

V Greiman[1, 2], C Bain[2]

[1]*Boston University, Boston, USA*

E-mail: ggreiman@bu.edu

[2]*Harvard Kennedy School, Carr Center for Human Rights Policy*

Program on Human Trafficking and Modern Slavery, Cambridge, USA

E-mail: ggreiman@law.harvard.edu

E-mail: Christina_Bain@Harvard.edu

Abstract: *Today, according to the U.S. Department of State's 2012 Trafficking in Persons Report it is estimated as many as 27 million people around the world are victims of trafficking into the sex trade and other forms of servitude known as modern slavery or trafficking in persons. This paper will assist in creating a deeper understanding of the impact of cyber activity on the human trafficking industry in the effort to find greater solutions for the prevention and prosecution of, as well as the protection of the innocent from the growing incidence of cyber activity as it relates to human trafficking around the globe.*

Introduction to Human Trafficking and Modern Slavery

The United States' *Trafficking Victims Protection ACT (TVPA) of 2000*, as amended, and the United Nations' *Palermo Protocol to Prevent, Suppress, and Punish Trafficking in Persons* describe human trafficking using a number of different terms. Under United States federal law, 'severe forms of trafficking in persons' includes both sex trafficking and labor trafficking as defined below:

> Sex trafficking is the recruitment, harboring, transportation, provision, or obtaining of a person for the purposes of a commercial sex act, in which the commercial sex act is induced by force, fraud, or coercion, or in which the person induced to perform such an act has not attained 18 years of age. (22 USC § 7102; 8 CFR § 214.11(a))
>
> Labor trafficking is the recruitment, harboring, transportation, provision, or obtaining of a person for labor or services, through the use of force, fraud, or coercion for the purposes of subjection to involuntary servitude, peonage, debt bondage, or slavery. (22 USC § 7102)

On the international level, the *Palermo Protocol*, defines trafficking in persons as

> The recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs or other types of exploitation. (Article 3, para.(a))

Table 1 shows that on the basis of the definition given in the Trafficking in Persons Protocol, it is evident that trafficking in persons has three major elements: (1) The Act (what is done); (2) The Means (how it is done); and (3) The Purpose (why it is done).

Table 1: Elements of Human Trafficking

Act of Trafficking	Means of Trafficking	Purpose of Trafficking
Recruitment	Threat or use of force	Sexual Exploitation
Transport	Abduction	Prostitution of Others
Transfer	Coercion	Forced Labour or Services
Harbouring	Deception	Modern Slavery
Receipt of Persons	Fraud	Servitude
	Abuse of Power	Removal of Organs
	Vulnerability	Other Types of Exploitation
	Payments or Benefits to Person in Control of Another Person to Achieve Consent for the Purpose of Exploitation	

Criminalization of Human Trafficking

The definition contained in article 3 of the *Trafficking in Persons Protocol* is meant to provide consistency and consensus around the world with regard to the phenomenon of trafficking in persons. Article 5, therefore, requires that the conduct set out in article 3 be criminalized in domestic legislation. In addition to the criminalization of trafficking, the Trafficking in Persons Protocol also requires criminalization of

- attempting to commit a trafficking offence,
- participating as an accomplice in such an offence, and
- organizing or directing others to commit trafficking.

The *Protocol* further requires that domestic legislation should adopt the broad definition of trafficking prescribed in the *Protocol*. The legislative definition should be dynamic and flexible so as to empower the legislative framework to respond effectively to trafficking that (1) occurs both across borders and within a country (not just cross-border); (2) is for a range of exploitative purposes (not just sexual exploitation); (3) victimizes children, women, and men; and (4) takes place with or without the involvement of organized crime groups.

In the United States, sex trafficking was criminalized under 18 U.S.C. para. 1591, "Sex trafficking of children or by force, fraud, or coercion," which makes it illegal to recruit, entice, provide, harbor, maintain, or transport a person or to benefit from involvement in causing the person to engage in a commercial sex act, knowing that force, fraud, or coercion was used or that the person was under the age of 18.

Definition and Scope of Cybertrafficking

While the traditional means of human trafficking remain in place, cyber technologies give traffickers the unprecedented ability to exploit a greater number of victims and advertise their service across geographic boundaries (Latonero 2011). Importantly, the extent to which these technologies are used in both sex and labor trafficking is unclear and is the subject of emerging research.

In recent years, the term 'cyber' has been used to describe anything that has to do with computers, networks, and the Internet, particularly in the security field. However, the contours and meaning of 'cybertrafficking' have not yet been constructed to any substantial degree in legal or trafficking literature or in practice. Similar definitional development has occurred around the more well-established umbrella term 'cybercrime' over the last few years, and yet considerable debate persists over both the validity of cybercrime as a separate category and the most appropriate scope of the term.

Drawing upon several definitions of human trafficking utilized under the *Trafficking Victims Protection Act of 2000 (TVPA)*,[1] the European *Convention on Cyber Crime*,[2] the Council of Europe *Convention on Trafficking in Human Beings*,[3] The United Nations *Convention against Transnational Organized Crime Protocol on Human Trafficking*,[4] and various state statutory schemes,[5] some commonality among the provisions was identified. A review of cases on the websites of the U.S. Department of Justice Computer Crime and Intellectual Property Section (CCIPS), Harvard Law School's Berkman Center for Internet and Society, and Interpol also revealed no existing definition of cybertrafficking but a diversity of definitions for cybercrimes and trafficking in humans.[6]

Because there is no consensus on the meaning of 'cybertrafficking,' we have developed the following working definition of the term to describe the potential reach of 'trafficking on the Internet' (however, we should note that a precise definition of the term, while useful for some purposes, is not necessary to understand the importance of the Internet as a gateway to human trafficking and how this activity is being dealt with in selected jurisdictions):

> 'Cybertrafficking' is the 'transport of persons,' by means of a computer system, Internet service, mobile device, local bulletin board service, or any device capable of electronic data storage or transmission to coerce, deceive, or consent for the purpose of 'exploitation'. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labor or services, slavery or practices similar to slavery and servitude. 'Transport in persons' shall mean the recruitment, advertisement, enticement, transportation, sale, purchase, transfer,

---

[1] *The Trafficking Victims Protection Act of 2000 (TVPA)* defines trafficking in persons as "(a) sex trafficking in which a commercial sex act is induced by force, fraud or coercion, or in which the person induced to perform such act has not attained 18 years of age."

[2]Chapter 1, Article 1 (d) of the *Convention on Cybercrime* defines "traffic data" as "any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service." Budapest, 23.XI.2001 Council of Europe, *Convention on Cybercrime*, opened for signature Nov. 23, 2001, E.E.T.S. no. 185.

[3] Council of Europe - Council of Europe *Convention on Action against Trafficking in Human Beings* (CETS No. 197) defines human trafficking as follows:

> 'Trafficking in human beings' shall mean "the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation."

[4] The United Nations *Convention against Transnational Organized Crime*, adopted by General Assembly resolution 55/25 of 15 November 2000 *Protocol on Human Trafficking*.

[5] See generally, Polaris Project for a World Without Slavery, (listing state and federal human trafficking laws) available at: <http://www.polarisproject.org/resources/state-and-federal-laws>.

[6] U.S. DOJ/CCIP available at <www.justice.gov/criminal/cybercrime/intl.html>; Harvard Law School Berkman Center for Internet and Society available at <http://cyber.law.harvard.edu/vaw02/module3.html>; Interpol available at <http://www.interpol.int/Public/Children/Default.asp>.

harbouring or receipt of persons, for the purpose of exploitation with or without the consent of the victim.

The Use of Technology in Trafficking

The use of technology in trafficking—cybertrafficking—takes many forms, but all these forms can be roughly grouped into three major categories. The first is the use of the Internet, text messaging, digital cameras, and mobile devices/smartphones to offer, advertise, and sell sex services, some of which are provided by trafficked victims. There has been a dramatic shift in the advertising of commercial sex, moving from the streets, sidewalks and printed ads to online classified advertising sites such as backpage.com, (until recently) Craigslist, and a range of more specialized sites.[7] On September 4, 2010, Craigslist removed its 'Adult Services' after a campaign launched by 17 attorneys general and several prominent national and international anti-trafficking organizations and replaced the link to the section with one word: 'censored' (Miller 2010).

A variety of cases and prosecutions has revealed how traffickers make sophisticated use of mobile technology to photograph their victims, place and change online ads quickly when they transport their victims to new cities, send photographs of and other information about victims to potential customers in real time to arrange transactions, etc. While empirical data is not available, anecdotal evidence suggests that a substantial majority of sex trafficking in the United States may now be advertised and arranged on the Internet.

The second main category of the use of technology in trafficking is identifying, locating, enticing, and recruiting new victims into trafficking and then helping to control the victims once they have been trafficked. This may take the form of using social networking sites, such as Facebook, MySpace, and others, or using direct communications tools like email, instant messaging, and text messages. Evidence exists that this recruiting function is being used both for sex trafficking and for labor trafficking. Examples of the latter category include creating fictitious employment, immigration assistance, and 'online bride' websites to lure potential victims into contact with the traffickers. One specific case analyzed involved a trafficking enterprise that used phony immigration advice and counseling websites to 'solicit and recruit alien workers from both abroad and within the United States and to obtain information about these aliens.'[8] Although Internet classified sites already have come under intense scrutiny, the role of social networking sites and online classifieds has yet to be fully researched.

---

[7] For a number of years, Craigslist and its 'erotic services' and then 'adult services' categories were one of the major locations for commercial sex ads. In 2010, under heavy pressure from U.S. state attorneys general, Craigslist eliminated the specific 'adult services' category of ads. Since then, much of the most blatant and explicit advertising for commercial sex has shifted to other sites, particularly backpage.com and certain, more-specialized 'fetish' sites.

[8] *United States v. Askarkhodjaev, et al*. (W.D. Mo.), Indictment, May 6, 2009, Case 4:09-cr-00143-SOW, Doc. 1. Available at http://blogs.kansascity.com/files/traffick.pdf (last viewed July 5, 2013)

A third category involves both the advertising *and* the delivery of coerced sex services over the Internet. One case of coerced 'cybersex' involved victims offered to customers over the Internet and then forced to perform sex acts for those customers not in person but via Internet webcams and chat technologies. Similarly, the U.S. Department of State *Trafficking in persons report* (2010) reveals that, in China, many North Korean trafficking victims are subjected to forced prostitution in Internet sex businesses.

In November 2012, the USC Annenberg Center on Communication Leadership and Policy (CCLP) issued an important research report on *The rise of mobile and the diffusion of technology-facilitated trafficking*. The report contained the following two key findings on the role of technology in domestic minor sex trafficking: (1) technology-facilitated trafficking is far more diffuse than initially thought, spreading across multiple online sites and digital platforms; and (2) mobile devices and networks play an increasingly important role that can potentially transform the trafficking landscape. Moreover, the authors noted that the centrality of mobile phones has major implications for counter-trafficking efforts and may represent a powerful new tool in identifying, tracking, and prosecuting traffickers (Latonero 2012, p. 36).

Cybertrafficking Legislation

The importance of legislative frameworks in combatting human trafficking has been notably recognized by Secretary of State Hillary Rodham Clinton:

> The problem of modern trafficking may be entrenched, and it may seem like there is no end in sight. But if we act on the laws that have been passed and the commitments that have been made, it is solvable. (Lee 2011)
> *- U.S. Secretary of State Hillary Rodham Clinton, June 28, 2011*

The *2012 Trafficking in persons report* highlights the importance not only of the passage of domestic laws consistent with international standards, but also the importance of training the law enforcement and justice officials likely to encounter these individuals violating the laws. Such laws must provide a victim-centered framework for fighting modern slavery in which everyone victimized by trafficking, whether for labor or commercial sexual exploitation, whether a citizen or immigrant, whether a man, woman, or child, is considered a victim under the law (p. 14).

In the United States, many states have passed statutes on trafficking and victim protection; however, these laws have only been passed recently, and many do not go far enough in imposing criminal penalties on perpetrators. Significantly, the State Department's *2011 Trafficking in persons report*, noted that 'while state prosecutions continue to increase, one study found that less than 10% of state and local law enforcement agencies surveyed had protocols or policies on human trafficking (p. 373)'.

In 2003, Texas was one of the first states in the nation to criminalize human trafficking. Though the law provides for (1) a statewide task force on trafficking; (2) a four-hour police training program; (3) victim defense to prostitution; and (4) a simplified burden of proof for prosecutors, the law noticeably does not address the unique aspects of the use of technology in trafficking.

On November 21, 2011, Massachusetts also passed a tough new law, *An Act Relative to the Commercial Exploitation of People*, which strengthens protections for victims of human trafficking and prostitution and increases the punishment for offenders by carrying a potential life sentence for traffickers of children. As part of this anti-human trafficking law, the legislature created an interagency task force to address all aspects of human trafficking through policy changes. The task force is charged with addressing Human Trafficking through service development, demand reduction, system change, public awareness, and training.

As noted above, the protections available to trafficking victims vary among states, and minor victims of sex trafficking can even face prostitution charges in some state courts *(In the Matter of BW* 2010). New York was the first state to pass legislation addressing this issue in 2010, with the passage of the *Safe Harbor for Exploited Children Act*. Several states have since passed similar acts.

Emerging Issues in Cybertrafficking Prosecutions

An emerging issue with regard to cybertrafficking prosecutions seems to be the lack of case law which fleshes out the various elements of federal and state statutes. Human trafficking prosecutions themselves seem to be limited in comparison to other areas of criminal law, and many cases appear to be pleaded out before reaching a judge or jury to determine factual issues. As a result, many unknowns exist around the scope of proof and requisite evidentiary needs.

The cases that do exist often view the Internet suspiciously as lacking in authenticity or trustworthiness. In one Texas case involving human trafficking through the use of the Internet, the court held that Plaintiff's electronic 'evidence' is totally insufficient to withstand defendant's motion to dismiss: 'While some look to the Internet as an innovative vehicle for communication, the Court continues to warily and wearily view it largely as one large catalyst for rumor, innuendo, and misinformation' (*St. Clair* 1999). The court went on to say that

> . . . there is no way Plaintiff can overcome the presumption that the information he discovered on the Internet is inherently untrustworthy. Anyone can put anything on the Internet. No web-site is monitored for accuracy and nothing contained therein is under oath or even subject to independent verification absent underlying documentation.

Authenticity and admissibility arose in another case involving control over an Internet account. The court in *Commonwealth v. Williams* held printouts of MySpace messages sent from Defendant's brother's MySpace account to witness were not properly authenticated in absence of proof of who accessed the account and sent the messages (2010).

Despite the concerns of authenticity by some courts in prosecuting these cases, the following cases suggest that there are ways of overcoming these concerns. For example, the use of Internet advertising was the key to a successful human trafficking prosecution in the case of *Iowa v. Russell*. In this case, the defendant was convicted of human trafficking under Iowa Code § 710A.1(1). The defendant met two teenaged girls (age 15 and 16) who had run away from a juvenile home in Nebraska through a woman named 'Jazzie.' The victims agreed to go on a road trip and were later told they would have to work at strip clubs and as prostitutes. The legal element of 'continuing basis' in the human trafficking statute was met because there was evidence advertising the victims' sexual services, with photos of the victims on the Internet.

In another on-going matter, a defendant in Florida and four others were indicted by a federal grand jury for conspiracy to traffic in persons under the age of 18 for purposes of causing such persons to engage in a commercial sexual act under 18 U.S.C. §1594(c) (*U.S. v. Wilson* 2010). This particular defendant sought to sever his trial from the other alleged co-conspirators. In response, the United States cited evidence of the conspiracy, which included Internet ads on backpage.com. The United States alleges that the co-conspirators helped each other with Internet advertising of adult and minor females, such as sharing computers to advertise the sexual services.

In addition to the lack of specific legislation governing trafficking through the use of the Internet, critical forensic issues continue to arise in human trafficking cases. These issues include (1) the ability of law enforcement to access stored communications; (2) whether an interception includes stored communications; (3) the definition of electronic storage; (4) admissibility of electronic evidence; (5) preservation of computer data; and (6) cross-border searches and seizures. As technology evolves, law enforcement must always stay on the cutting edge of technological change and continually invest money and resources for new training and equipment.

Cybertrafficking Research and Collaboration

The increasing international focus on trafficking in persons has started to be reflected in the surprising amount of research on the issue of human trafficking. Since 2000, the International Organization for Migration has tracked the rapid increase in publications on the subject. However, as noted by the U.S. Department of Justice, the research is limited in the number of reported cases due to enormous difficulty in tracking a global criminal enterprise (2011). In the *2011 Trafficking in*

Persons Report, the U.S. Department of State stressed the increased need for information and understanding of the role of technology in trafficking.

In the course of the research thus far in the Program on Human Trafficking and Modern Slavery at Harvard's Kennedy School of Government, the authors have spoken with various trafficking experts, consulted with investigators and prosecutors, and collected filed indictments and other charging documents as well as press accounts of trafficking cases where technology was alleged to have played a role in the selection or recruiting or grooming or control of the victim. The goal of the research is to identify as many case studies of cybertrafficking as possible. Simultaneously, the authors have sought to interview specific law enforcement officials and prosecutors involved in many of the cases identified to gather details on the nature of the technologies used and the role they played in the offenses *and* to collect and analyze actual case evidence relating to technology. Consulting with leading trafficking prosecutors and investigators nationwide to glean their knowledge of the scope and nature of technology use and the adequacy of existing laws to address that use, the authors will continue targeted legal research and analysis to identify emerging case law and best practices surrounding evidentiary issues relating to electronic evidence, particularly from social networking sites and other Internet sources. Due to the unavailability of empirical research, the possibility of developing empirical data with potential governmental or private sector partners for use in mitigating or preventing the use of electronic devices for the commission of human trafficking continues to be explored.

The Harvard Cyberlaw Clinic at the Berkman Center for Internet & Society has been instrumental in providing valuable insight into the evidentiary issues faced in trafficking prosecution. In addition, its research team has been forging valuable collaboration links with a number of other researchers working in this space including danah boyd, a prominent technology and youth-safety advocate, Fellow at Harvard's Berkman Center for Internet & Society, and now a senior researcher at Microsoft Research.[9] The authors and the rest of the Kennedy research team have also shared information and approaches with a promising research and advocacy program, the Technology and Trafficking in Persons Research Project at USC's Annenberg Center on Communication Leadership and Policy.[10] Highlighted in table 2 below is a summary of the key objectives and questions raised by the Kennedy School program's research to date.

Table 2: Key Areas of Research

Research Objectives	Research Question
Ensure a victim-centric focus to understanding the	Are the international, federal, and state laws

[9] See biography available at http://www.danah.org/

[10] http://communicationleadership.usc.edu/projects/technology_trafficking_in_persons.html

trafficking problems and their impacts.	effective in preventing and resolving human trafficking on the Internet?
Analyze trafficking forensics and evidentiary issues in prosecution and the role of the Internet prosecutor.	What typical and unique evidence-gathering techniques are being used successfully by law enforcement and prosecutors?
Survey the impact of digital evidence in the courtroom.	Do the case decisions uphold the use of digital evidence, and how do the rules and procedures impact these decisions?

Conclusions

As recognized by the U.S. Department of State, while human trafficking problems are being resolved on the international level through the passage of domestic legislation under the *Palermo Protocol*, emerging technologies give rise to new challenges in fighting human trafficking. Though the Internet offers new ways of conducting human trafficking, it also offers opportunities to campaign against trafficking and to provide knowledge about the dangers of trafficking as it impacts the victims. It also offers the ability to proactively monitor and prevent these events before targets become victims. The information-security implications of these technologies are areas of active research, and methodologies for protecting victims from cybertrafficking are still evolving. In the interim, collaborative research is critical to the development of security models that protect victims of trafficking, while at the same time developing electronic evidence of trafficking activity that will withstand motions to dismiss in the legal tribunals around the world.

References

Commonwealth v. Williams (2010) 456 Mass. 857, 926 N.E. 2d 1162.

Council of Europe, Convention on Cybercrime, Budapest 23.XI.2001, opened for signature Nov. 23, 2001,CETS No. 185, *S. Treaty Doc. No. 108-11, 2001 WL 34368783, 41 I.L.M. 282, Convention on Cybercrime explanatory report*, p. 6.

Council of Europe *Convention on Action against trafficking in human beings*, Warsaw, opened for signature May 16, 2005, CETS No. 197.

Council of Europe 2009, *Cybercrime training for judges and prosecutors: a concept, project on cybercrime*, <www.coe.int/cybercrime> and the Lisbon Network, Strasbourg, France.

Craigslist, Inc. v. McMaster (2009) No. 2:2009cv01308 (D.S.C.).

In the Matter of BW (2010) 313 S.W.3d 818, 826 (Tex. 2010). (This case involved a 13 year old who was arrested and convicted in Texas for offering to perform an illegal sex act on an undercover officer, despite a state law that persons under 14 cannot consent to sex. The Texas Supreme Court reversed the decision on appeal, noting, 'Children are the victims, not the perpetrators, of child prostitution.')

Iowa v. Russell (2010) no.9-906/08-2034, 2010 Iowa App. LEXIS 145 (Iowa Ct. App. 2010), *aff'd*, 781 N.W.2d 303.

Latonero, M (2011) *Human trafficking online: the role of social networking sites and online classifieds*, Research Series on Technology and Human Trafficking, Annenberg School for Communication & Journalism, Center on Communication Leadership & Policy, University of Southern California, Los Angeles.

Latonero, M (2012) *The rise of mobile and the diffusion of technology-facilitated trafficking*, Research Series on Technology and Human Trafficking, Annenberg School for Communication & Journalism, Center on Communication Leadership & Policy, University of Southern California, Los Angeles.

Lee, M (2011) Remarks of Secretary of State, Hilary Rodham Clinton in presenting the 2011 Trafficking in Persons Report, June 28, Associated Press, Globe Newspaper Company.

Miller, CC (2010) 'Craigslist blocks access to 'adult services' pages', *New York Times*, Technology Business Daily, 4 September, <http://www.nytimes.com/2010/09/05/technology/05craigs.html (last accessed on 8 July 2013).

St. Clair v. Johnny's Oyster & Shrimp, Inc. (1999) 76 F. Supp.2d 773 (S.D. Tex. 1999).

United Nations (2000) The United Nations Convention against Transnational Organized Crime, adopted by General Assembly Resolution 55/25 of 15 November, Palermo, opened for signature on 12-15 December 2000 and entered into force on 29 September 2003, supplemented by the United Nations Convention Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, was adopted by General Assembly Resolution 55/25 and entered into force on 25 December 2003.

U.S. Department of Justice Literature Review 2011, *Data and Research on Human Trafficking: Bibliography of Research-Based Literature* Prepared by EM Gozdziak and MN Bump.

United States, *Trafficking Victims Protection ACT (TVPA) of 2000* (Pub. L. 106-386).

United States v. Askarkhodjaev, et al. (2009) (W.D. Mo.), Indictment, May 6, 2009, Case 4:09-cr-00143-SOW, Doc. 1. Available at http://blogs.kansascity.com/files/traffick.pdf (last accessed on 8 July 2013).

U.S. Department of State June 2009 - June 2012, *Trafficking in Persons Reports*.

U.S. v. Wilson (2010) No. 10-60102-CR, 2010 WL 2609429 (S.D. Fla. 2010).

U.S. v. Wong, (2003) 334 F.3d 831, 838 (9th Cir.).