An Inquiry into Privacy Concerns: Memex, the Deep Web, and Sex Trafficking

Jeffery Hammonds

East Carolina University

ICTN 6885

March 17, 2015

Abstract

This research study will examine how large scale data mining may negatively affect privacy as it helps solve national and international sex trafficking crimes. The data mining tool researched here is the Memex Project; created, implemented, and managed by the United States Defense Advanced Research Projects Agency (DARPA). The Memex Project senses patterns in large amounts of data and makes connections. Memex was created to assist the federal government in cracking down on human trafficking. It may also be used by national governments in the fight against terrorism in the near future. While the Memex Project's purpose is admirable, it could be used as a tool to intrude on the privacy of law-abiding citizens. As part of this research study, a breakdown of how data mining is defined and regulated by United States law will also be examined.

An Inquiry into Privacy Concerns: Memex, the Deep Web, and Sex Trafficking

Introduction

As humankind designs and creates digital forensics tools such as the Memex Project to protect the people of many different nations, the public and private sectors must decide how many personal freedoms must be sacrificed to keep children, women, and men out of the hands of international sex and human slavery traffickers. Loss of Internet privacy may lead to the difference between life and death for victims of human trafficking; how much privacy invasion is worth this result, and how many personal freedoms must be violated in order to reach the goal of reducing or eliminating these horrendous crimes? The goal of this paper is to highlight the benefits and risks concerning the Memex Project data mining tool in particular. In pursuit of this goal, the Defense Advanced Research Projects Agency (DARPA), the history of the Memex Project and data mining, the atrocities of human trafficking, and the security concerns surrounding implementation and use of the Memex Project and programs similar to it will be examined in depth. Finally, conclusions will be drawn about the Memex Project, determining ways in which national laws regulate or fail to regulate Internet privacy.

The Defense Advanced Research Projects Agency (DARPA)

To understand the significance of data mining, The Defense Advanced Research Projects Agency (DARPA), and the Memex Project in the world of human trafficking, DARPA itself must be examined. DARPA was established in 1958 to "prevent strategic surprise from negatively impacting United States national security and create a strategic surprise for U.S. adversaries by maintaining the technological superiority of the U.S. military (DARPA, "Our work," 2015). In essence, DARPA is a division of the United States Department of Defense (DoD) which develops emerging technologies for use by the military and the federal government

in order to prevent and track Internet usage and international and national crimes through digital forensics and other methods. DARPA's technological security focuses are: 1) technology, adaptability, & transfer; 2) biology, technology, & complexity, 3) discovery, modeling, design, & assembly; 4) information, innovation, & cyber; 5) decentralization, EM spectrum, globalization, & information microsystems; 6) networks, cost leverage, & adaptability, and 7) weapons, platforms, & space (2015).

DARPA's mission is to "apply multi-disciplinary approaches to both advance knowledge through basic research and create innovation technologies that address current practical problems through applied research…the creation of full-scale technology demonstrations in the fields of biology, medicine, computer science, chemistry, physics, engineering, mathematics, material sciences, social sciences, neurosciences," etc. are included in the DoD's main source of technological innovation (DARPA, "Our work," 2015). The Information Innovation Office, also known as I2O, currently consists of thirty-nine programs devoted to the process of "anticipating new modes of warfare…and developing the concepts and tools necessary to provide decisive advantage for the U.S. and its allies" ("About I2O," 2015). The focus of I2O is to use heterogeneity, formal methods proofs, secure code generation, and automation to prevent vulnerabilities in cyberspace and information networks, including military systems, enterprise networks, secure communication, and industrial systems (2015). The influence of "Big Data" on the abilities of computers to store, network, and measure information such as the "online correlation for societal unrest."

The question asked by I2O is, how can new computing power be leveraged in order to glean defining information about the human condition; how can this information be applied in order to better society and prevent terrorism and human trafficking crimes; and how can

computing be used to improve current computing abilities in the long-run. The Memex Project was developed to enhance the ability of "search technologies and revolutionize the discovery, organization, and presentation of search results," and was named for hypothetical device from a 1945 *The Atlantic Monthly* article written by Vannevar Bush, the acting director of the United States office of Scientific Research and Development (OSRD) during World War II (DARPA, 2014).

The Memex Project: A History

Vannevar Bush was an American electrical engineer and administrator responsible for the development of the Differential Analyzer and government scientific research during World War II. Among Bush's many computer and electrical engineering successes were the Rockefeller Differential Analyzer which produced ballistics tables for the military; the establishment of the Raytheon Company which manufactured electronic parts; and the National Defense Research Committee (NDRC), the basis for today's DARPA, and what is today known as the military-industrial complex, or the Pentagon (n.d.). Bush was responsible for the "marriage of government funding and scientific research," and the OSRD's annual budget by the end of World War II was over $500 billion (n.d.). Radar and the atomic bomb were OSRD inventions, but the defeat of Bush's National Research Foundation (NSF) in 1949 confirmed Bush's fears that "the militarization of American science would harm the development of the economy" (n.d.). Despite Bush's attempts to dissuade the world from allowing military control and innovation of computer science, the military is now the "major patron" of American scientific research. Bush's article "As We May Think" proposed a device called the Memex, "an indexed, archival, microfilm machine for cross-referencing and retrieving information;" the first machine that defined, introduced, and led to the design and creation of hypertext and the implementation

of the World Wide Web (n.d.). The purpose of the Memex machine was to "help people sort through the enormous amount of published information available through the world" and was meant to be "an enlarged intimate supplement" to the human memory (Lemelson-MIT, n.d.). Bush's idea included viewing screens and a keyboard on a desk, and the precursor for hypertext. Although the device was never created, Bush's proposal helped others create the Internet as we know it today.

Most web-searching tools today use centralized approaches to search the Internet; these include identical sets of tools for all queries, and has been commercially successful. This method of searching, however, does not "work well for many government use cases"; its issues include: no saving of sessions; one-at-a-time entry and almost exact input; and no aggregation of search results (DARPA, 2014). The Memex Program was created in order to "revolutionize the discovery, organization, and presentation" of Internet search results to be more helpful in military projects (2014). Users of Memex must be able to increase the reach of search capabilities quickly and in a more organized manner. Other goals of Memex are to improve military, government, and commercial enterprise ability to "find and organize mission-critical publically available information on the Internet" (2014). Essentially Memex seeks to reverse the Internet search paradigm so that individual users' specific subject areas are the focus of the search system. Memex is being developed for "non-programmers" down the line, but is currently being used for a much more humanitarian mission: human trafficking (2014).

According to DARPA, human trafficking greatly affects law enforcement, intelligence investigations, and military missions through its "significant" presence on the Internet. Forums, chats, advertisements, hidden services, and fictional job postings are all important sources for

information that could lead to the prevention of human trafficking crimes through curating by the Memex Project (2014).

Data Mining: A History

Furnas (2012) stated, "Without data mining, when you give someone access to information about you, all they know is what you have told them. With data mining, they know what you have told them and can guess a great deal more…data mining allows companies and governments to use the information you provide online to reveal more than you think" they would be able to. Furnas notes that although "data mining algorithms [are] quite complex," data mining is not difficult to understand (2012). Data mining organizes and sorts large, complex data sets; so many data sets that attempting to make sense of them is so complex and overwhelming that data mining evaluation methods became the only way to interpret the immense amounts of digital information (2012). Description and prediction are the main types of data mining, and they do exactly what their descriptors entail; in addition, there are a few main types of organization which help people interpret and use the data in valuable ways.

Data mining strategies include anomaly detection, association learning, cluster detection, classification, and regression. Anomoly detection allows detection of notable differences in typicality in a large data set. Association learning is most familiar to the general public through the behavior of retail sites such as Amazon, which use previous purchase information to predict and suggest possible future purchases. Cluster detection algorithms recognize sub-categories within data instead of using human-imposed sub-categories that may fail to capture needed information due to human error. Classification uses existing structures to classify new incidences of pre-determined categories; this is useful for comparing differences between two large systems or data sets (an example is spam email filters). Regression is used to create predictive models

based on different variables. Facebook is the example Furnas uses, indicating that usage data gathered from the application such as amount and type of personal information shared over the user lifetime may inform future incarnations (2012). Data mining, then, is a powerful tool that can be used either for good or evil, depending on the desired outcome. Hackers increasingly use data mining techniques in order to recognize patterns within monetary and financial organizations and users, and to penetrate user email and social media accounts with more impunity (Smith, 2009). As we have seen, data mining can provide insight into large sets of data, such as the individual time spent and visits made to a particular website. This information can be extremely helpful to law enforcement and military agencies attempting to locate and apprehend international human trafficking suspects and criminals involved with, or benefiting from this inhumane industry.

Human Trafficking

Human trafficking is a difficult subject to discuss in any situation, but the high rates recorded by the United Nations in its latest report are disheartening and heartrending. Humantrafficking.org noted that across the globe in 2012, 2.4 million people are victims of human trafficking, and 80 percent of those are considered sexual slaves to the perpetrators of these horrendous crimes against men, women, and children. The website noted that the industry rakes in $32 billion for criminal perpetrators, and two-thirds of its victims are women. The United Nations Office on Drugs and Crime noted that “only one out of 100 victims of human trafficking is ever rescued” (2012). In the United States 10 percent of police stations are have protocol for human trafficking, and it is one of the “fastest growing and lucrative crimes” in the world currently, moving victims along the same international routes as arms and drug smuggling criminals use (2012).

One of the main barriers to the prevention of human trafficking the world over is the persistent categorization of prostitutes as criminals, and lack of criminal persecution or protocol for the perpetrators of human trafficking crimes. This mindset prevents the addressing of the real crimes in favor of victim criminalization. The main countries for *origin* of human trafficking victims in 2012 were Ukraine, Haiti, Yemen, Laos, Uzbekistan, Cambodia, Kyrgyzstan, Afghanistan, Belarus, and Ethiopia (2012). The majority of these victims were destined for the Russian Federation, Haiti, Yemen, Thailand, Kazakhstan, Afghanistan, Indonesia, Poland, Egypt, and Turkey (2012). Unfortunately, victims of human trafficking are not often kept apprised of their captors' future plans, and the destinations listed above may not encompass the final destination of many of these victims, or inform the people who ultimately benefit from the services or labor victims are ultimately forced to perform. In other words, these destinations may only be stops on the way to more affluent countries and "customers" in locations such as the United States or Europe.

Human traffickers use force, fraud, or coercion in order to force victims to provide commercial sex or labor services against their will (Polaris, 2015). Violence, threats, deception, and debt bondage are additional tactics employed by perpetrators, and victims have been found in online escort services, brothels disguised as legitimate businesses, prostitution, sales crews, large firms, restaurants, and carnivals to name a few (2015). According to Polaris and the International Labor Organization, a Washington, D.C. organization which works to disrupt the conditions that allows human trafficking in society, high profits and low risk drive the criminal industry and 20.9 million victims are trafficking globally, over half of which are women and girls (as cited in Polaris, "Human Trafficking," 2015). Victims are promised jobs, stability, education, or a "loving relationship" in most cases, and homeless youth and victims of sexual

assault, domestic violence, war or conflict, and social discrimination are targeted (2015). Leverage of non-portability of work visas and lack of victim familiarity with their surroundings (including laws, rights, language, and cultural understanding) are used by traffickers to indebt foreign nationals who have paid fees for travel or recruitment into fictional programs (2015). Traffickers steal personal identification and prevent victim knowledge of surroundings through frequent moves to various locations which are not conducive to victims' language or culture knowledge.

H.R. 181, the Justice for Victims of Human Trafficking Act was passed unanimously by the United States House of Representatives in February, 2015 (Taibi, 2015). The Hyde Amendment, which is included, prevents the use of taxpayer money to fund abortions and other health services for victims of human trafficking, and is currently causing friction and resistance in the Senate. Human trafficking needs to be addressed by laws such as this; it is time to help prevent these horrible crimes in whatever ways are available to national and international governments.

Prevention of Human Trafficking Through Data Mining and the Memex Project

The Memex Project seeks to prevent human trafficking through domain-specific indexing, domain-specific search, and DoD-specified applications. DARPA stated that "the program is specifically not interested in proposals for the following: attributing anonymous services, deanonymizing or attributing identity to servers or IP addresses, or accessing information not intended to be publicly available;" and will use open source technology and architecture in order to pursue its goals of preventing human trafficking crimes (2014). In other words, DARPA does not intend to invade the general public's privacy through the use of its new technology, but is this possible, and is this the real issue that people need to be concerned with?

Chris White is the inventor of Memex, and explained that "The Internet is much, much bigger than people think…by some estimates Google, Microsoft Bing, and Yahoo only give us access to around 5% of the content on the Web" meaning that there is plenty of unseen, illegal and black market weapons and sex trafficking trades conducted that most people are completely unaware of (CBSNews.com, 2015). Dan Kaufman, Director of DARPA's Information Innovation Office, states "there are parasites that live on [the Internet], and we take away their ability to use the Internet against us – and make the world a better place" (2015). According to Kumar (2015), the Deep Web is not indexed by commercial search engines, and "is a heap of illegal activity, pervaded with child pornography, drug deals, Cyber crime and human trafficking." Memex' goal is to extend the reach of search capabilities and "organize subsets of information" that can then be used to track down or expel illegal activities such as these from the web (2015). Beta testing for Memex is occurring now in two district attorneys' offices, one law enforcement agency, and one NGO (non-governmental organization). More testing will be done after this initial group is finished, according to Kumar (2015).

An important article in *Scientific American* details the use of "an experimental set of Internet search tools" (Memex) in a recent case of sex trafficking in New York City (Greenemeier, 2015). A woman who was held captive and sexually abused by a group of men jumped out of a window in order to escape; many of her bones were broken, but she survived (2015). Using Memex, Benjamin Gaston (of the New York District Attorney's Office) obtained a sentence for one of the abusers in prison: 50 years to life (2015). A central piece of prosecution such as this case is using "Memex to scour the Internet in search of information about human trafficking, in particular advertisements used to lure victims into servitude and to promote their sexual exploitation" (2015).

Understanding the Deep Web information that Memex has the ability to search requires knowledge of the "unstructured data" which is compiled using devices that are not included in databases that are scanned by search engines (Greenemeier, 2015). Other information is only on temporary internet pages, and are removed before search engines take note of their presence; many illegal and sexual services are offered in this manner on the Internet (2015). Specially-designed software like the Tor Onion Router allows anonymous peer-to-peer connections which avoid centralized computer servers and illicit services offerings to interested parties; I2P is a similar open source software designed for Mac, Windows, and Linux (2015). Memex's design consists of "eight open-sources, browser-based search, analysis and data-visualization programs as well as back-end server software that perform complex computations and data analysis," as noted by Greenmeier in *Scientific American* (2015).

Kevin Bales, a member of the Wilberforce Institute for the Study of Slavery and Emancipation, noted that "Slavery is the possession or control of a person in such a way as to significantly deprive that person of his or her individual liberty, with the intent of exploiting that person through their use, management, profit, transfer, or disposal. Usually…achieved through…violence or threats of violence, deception and/or coercion" (as cited in Datta, 2014). Datta noted that slavery can include sex trafficking, adult labor in mines, child slavery, or forced domestic servitude (2014). Legislation at the federal level concerning human sex trafficking has been ongoing since 2000 in the United States under the title of the Trafficking Victims Protection Act (Franklin, 2014). The act has been criticized for its lack of accurate and useful language that prosecutors can use to obtain justice for victims. Under the act, prosecutors must prove that "victims were forced, defrauded, or coerced into the sex trade," subtly implying that these victims might be there by choice, which is not likely (2014). This language views victims

as offenders instead of victims; the act does contain exceptional provisions for those under the age of 18, however (2014). To understand the gravity of the situation, Franklin details the "consequences of victimization" in the sex trafficking industry in her Human Trafficking Series at the Crime Victims' Institute in Sam Houston State University College of Criminal Justice.

The physical health of sex trafficking victims are ruthlessly and horribly impacted by their enslavement at the hands of traffickers, and common risks include victim rates of 70 to 95 percent for physical abuse (contusions, broken bones, and head trauma resulting in neurological dysfunction); 88 percent for verbal abuse, which contributes to feelings of helplessness and inescapability of their situations; and 60 to 75 percent rape by *both* traffickers and sex services buyers. If these statistics were not enough to highlight the horrific and inhumane treatment of sex trafficking victims, they are at high risk for the following problems, as well: mental health issues, chemical dependency and addiction, sexually transmitted infections, unwanted pregnancies, forced abortions, and incredible rates of physical and mental trauma (2014). Post-traumatic stress disorder, suicide, depression, and anxiety affect over 68 percent of sex trafficking victims (2014).

Memex is a new technology, and is currently being used in a very limited capacity; yet it already has a proven track record of success in persecution of sex traffickers in the United States (Greenemeier, 2015). Datta (2014) noted that "the U.S. government is also using big data to mine private information networks, not on the World Wide Web" but only on the Deep Web; thus fears about government data mining of non-offender information is unfounded and a bit paranoid (p. 23). Datta also indicated that the use of quantitative methods to estimate enslaved people in the world has led to "discussion among the media and policy community on how to mitigate modern day slavery, with an eye toward its eradication" (p. 32). The importance of this

future eradication and the steps being taken toward it are immeasureable, and will affect the lives of thousands or millions of slaves in the world.

Big Data Privacy Concerns Not Associated with Sex Trafficking

The world is worried about privacy; this is clear from headlines splashed across the internet and across media internationally. Big Data's incredible reach has been criticized, lauded, and condemned by various institutions and people. Grimmelmann (2014) noted that Big Data "tends to inevitably…convert its users into its subjects," and that "every visitor to the Land of Data leaves a little of herself behind" (p. 5). Grimmelmann stated that restrictions on use of Big Data was originally dealt with through "deidentification," or removing names, ranks, and serial numbers from an individual dataset (p. 6). However, personal information expresses a singularity, Grimmelmann stated, which cannot be erased. The overzealous scrutiny of personal information by marketing companies and hedge-fund traders is driving the privacy argument against tools like Memex to an extreme, and naturally the public is in fear of a big brother who analyzes and stores every bit of data a person views on a device screen (p. 6). Grimmelmann argues that allowing a small group of people the ability to comb through user data a will is paramount to playing God with people's lives. Although it depends upon what data is being analyzed, the recent black hat hacker information thefts across many large organizations have led to a general need for restructuring of privacy policies on the Internet.

The Deep Web and the Internet must be policed by some government entity; in any society or group there are a minority of ne'er-do-wells and a majority of good, behaving human beings. The fear of the population in general is that Big Data represents the kind of control a dictatorship has over its people; this includes regulation of all activities, forbidden actions which may result in imprisonment or penalties, and public discrediting if the lines between acceptable

behavior are crossed. Grimmelmann stated that "centralizing data disempowers both subjects and users…both now subject to the policies…of whatever entity controls the dataset" (p. 8). The policies of the situation are the key to understanding and solving this data dilemma. There must be control put in place to prevent the abuse of power that is possible due to information trawlers like Memex, and policies put into place regarding the privacy of Internet users, as well. Policies and laws are the foundation of the judicial system in the United States and internationally; if privacy is breached, new laws must be made in order to prevent future breaches.

United States Privacy Laws

According to the American Civil Liberties Union, "surveillance – whether by government or corporations – chills free speech and association, undermines a free media, and threatens the free exercise of religion (ACLU, n.d.). The ACLU also noted that "we shouldn't have to choose between using new technologies and keeping our personal information private. Technology can be implemented in ways that protect civil liberties, limit the collection of personal information, and ensure that individuals have control over their private data" (n.d.). The Electronic Communications Privacy Act (ECPA) needs to be updated, and works with national and state legislators to institute laws that prevent invasion of privacy via the Internet. The ACLU works specifically on law enforcement access to electronic communications content, location tracking, domestic surveillance drones, and automatic license plate readers, and provides a map that details state Internet and surveillance security laws (n.d.). ACLU pointed to mobile phone cell tower location registration which does not require a warrant from a judge to obtain. Privacy laws for businesses are defined on the United States Small Business Government website SBA.gov, and include prohibition of deceptive use of customer information by the Federal Trade Commission; protection of children's online privacy; usage and disposal of consumer and

employee credit reports; a sound security plan in order to enforce data security and identity theft; and a safeguarding plan or sensitive financial data in accordance with information sharing practices already in place (SBA, n.d.).

In *U.S. v. Jones* in the Supreme Court, it was ruled that a GPS tracking device attached to a car is considered a government search under the Fourth Amendment, but did not decide whether or not a warrant is required to do so (n.d.). This ruling should be applicable to cell phone information tracking, as well, but it is not clear how. Police warrants for using cell phone information from cell service companies is also being considered. Goldman (2014) noted that among the most important Internet laws passed in 2013 are the Gmail Electronic Communications Privacy Act (ECPA) decision of Judge Lucy Koh concerning Google's ad triggering methods in Gmail; Internet crackdowns via the Federal Trade Commission concerning "native ads," inauthentic blog posts, online ads aimed at kids as defined by the Children's Online Privacy Protection Rule (COPPA); data security; and new state laws aimed at regulating privacy which include requiring websites to disclose whether or not they are honoring "do-not-track" signals sent by browsers (2014). States have also proposed privacy laws limiting student data collection by schools as of late. The "stalemate" at the Federal level concerning privacy laws and the controversial National Security Association's widespread civilian monitoring has forced state legislatures' hands in this instance, which may be a positive thing as states decide on their own privacy laws (Segupta, 2013).

Conclusion

Privacy is and must be a concern in the world, especially the world of the Internet; however, using Memex to help eradicate one of the most destructive and merciless crimes that exists is not a privacy concern. Instead it is one of human understanding, compassion, and caring

which cannot be simulated by any computer, software program, or app. The victims of human trafficking suffer much more than an Internet user will if a Google search in Justin Bieber is revealed. The question of privacy on the Internet is an important one, but it is more perilous to those who are committing crimes and seeking profit from human suffering. If a user has nothing to hide, then that user has little to fear from data mining beyond identity and financial theft. The amount of available personal information is so vast that it cannot all be catalogued and organized, much less read and understood. Still, personal privacy is a concern because criminals will always seek to invade and exploit it.

From a personal vantage point, data mining is irritating; ads for things searched while waiting in line at the supermarket persist daily. The difference between typical data mining and Memex is that Memex has been expressly created and executed to track and convict sex trafficking criminals, not to find out which brand of toothpaste a consumer prefers. Keeping this distinction clear prevents panicky mental processes which may blind us to the reality of sex trafficking and the solution presented by Memex and DARPA. DARPA's Memex invention is striving to solve crimes. The millions of sex trafficking victims in the world include millions who suffer through the knowledge that their mothers, daughters, brothers, sons, parents, grandparents, or other close relatives are beaten, verbally abused, raped, or sexually assaulted for profit each and every day. When looked at from this viewpoint, DARPA's Memex Deep Web searcher does not seem so much like a privacy concern for individual, non-offending people, but more like a saving grace for those who are mistreated and victimized throughout the world.

References

American Civil Liberties Union (n.d.). Internet privacy. *ACLU.org.* Retrieved from https://www.aclu.org/technology-and-liberty/internet-privacy

CBS News.com (2015). New search engine exposes the "dark web." *CBSNews.com.* Retrieved from http://www.cbsnews.com/news/new-search-engine-exposes-the-dark-web/

DARPA (2014). Memex aims to create a new paradigm for domain-specific search. *DARPA.mil*. Retrieved from http://www.darpa.mil/newsevents/releases/2014/02/09.aspx

DARPA (2015). About I2O. *DARPA.mil*. Retrieved from http://www.darpa.mil/Our_Work/I2O/About.aspx

DARPA (2015). Our work. *DARPA.mil.* Retrieved from http://www.darpa.mil/our_work/

Datta, M. N. (2014). Using big data and quantitative methods to estimate and fight modern day slavery. *School of Advanced International Studies Review, 34*(1), 21-33.

Franklin, C. (2014). Human sex trafficking: An overview. PDF. *Dev.cjcenter.org.* Retrieved from http://dev.cjcenter.org/_files/cvi/Human%20Trafficking%2010.14.14forpdf.pdf

Furnas, A. (2012). Everything you wanted to know about data mining but were afraid to ask. *Atlantic Monthly.com.* Retrieved from http://www.theatlantic.com/technology/archive/2012/04/everything-you-wanted-to-know-about-data-mining-but-were-afraid-to-ask/255388/

Goldman, E. (2014). Top ten Internet law developments of 2013. *Forbes.com.* Retrieved from http://www.forbes.com/sites/ericgoldman/2014/01/09/top-ten-internet-law-developments-of-2013/

Greenemeier, L. (2015). Human traffickers caught on hidden internet. *Scientificamerican.com.* Retrieved from http://www.scientificamerican.com/article/human-traffickers-caught-on-hidden-internet/

Grimmelmann, J. (2014). Big data's other privacy problem. *Big Data and the Law.* Saint Paul, MN: West Academic.

Humantrafficking.org (2012). Recent Updates. *Humantrafficking.org.* Retrieved from http://www.humantrafficking.org/

Kumar, M. (2015). U.S. government builds "Memex Deep Web Search Engine" to track criminals. *Thehackernews.com.* Retrieved from http://thehackernews.com/2015/02/memex-deep-web-search-engine.html

Lemelson-MIT Program (n.d.). Vannevar Bush. *Lemelson.mit.edu*. Retrieved from http://lemelson.mit.edu/resources/vannevar-bush

Polaris (2015). Human Trafficking. *Polarisproject.org*. Retrieved from http://www.polarisproject.org/human-trafficking/overview

Segupta, S. (2013). No U.S. action, so states move on privacy law. *NYTimes.com*. Retrieved from http://www.nytimes.com/2013/10/31/technology/no-us-action-so-states-move-on-privacy-law.html

Smith, G. (2009). Data mining: How hackers steal sensitive electronic information. *The Journal of Corporate Accounting & Finance, 20*(4), 23-26.

Taibi, C. (2015). Fox News' Dana Perino thinks 'democrats are jerks' for blocking human trafficking bill. *Huffingtonpost.com*. Retrieved from http://www.huffingtonpost.com/2015/03/13/dana-perino-democrats-jerks-human-trafficking-bill_n_6864256.html

United States Small Business Administration (n.d.). Privacy law. *SBA.gov*. Retrieved from https://www.sba.gov/content/privacy-law