# THE EFFECTIVENESS OF DIGITAL FORENSICS AND SECURITY STRATEGIES IN USING AI AND MACHINE LEARNING TO PROTECT CHILDREN ONLINE

By

Edwin Giovanni De Jesús Cruz

A Thesis Submitted in Partial Fulfillment

of the Requirements for the Degree of

Master of Science

In

Computer Science

POLYTECHNIC UNIVESITY OF PUERTO RICO
SAN JUAN, PUERTO RICO

2019

Approved as to style and content:

_____
Jeffrey Duffany, Ph.D.
Chairperson, Graduate Committee

_____
Alfredo Cruz, Ph.D.
Member, Graduate Committee

_____
Nelliud Torres, DBA
Member, Graduate Committee

_____
Miriam Pabón, Ph.D.
Dean Graduate School

## ACKNOWLEDGMENTS

I want to thank my family for encouraging me to strive for greatness and for teaching me that the sky is the limit if you're willing to put in the work. I am extremely grateful to my partner in life, Barbara, for helping me to be the version of myself that I am today and for giving me constant love, inspiration, and constructive criticism on the development of this thesis and in all aspects of life; without her, I definitely would have taken a lot longer to finish this degree. A big thank you to my in-laws for always being there and lending a helping hand and advice when I need it the most. Thanks to the friends that in one way or another sent me a positive word to give me an extra boost of motivation. I would also like to thank the excellent professor, Dr. Jeffrey Duffany for being my thesis advisor and for showing me that just because something is heavily encrypted doesn't mean it can't also be fun. I would also like to thank Dr. Alfredo Cruz and Professor Nelliud Torres for being part of my thesis committee and providing valuable feedback on my work. This thesis is the product of people with great minds and even greater hearts. Without all of you, I would not be writing this right now and I definitely would not be the person I am today. Thank you.

**ABSTRACT**

THE EFFECTIVENESS OF DIGITAL FORENSICS AND SECURITY STRATEGIES IN USING AI AND MACHINE LEARNING TO PROTECT CHILDREN ONLINE

2019

EDWIN GIOVANNI DE JESÚS CRUZ, B.S.C.S

INTERAMERICAN UNIVERSITY OF PUERTO RICO

METROPOLITAN CAMPUS

M.S.C.S, POLYTECHNIC UNIVERSITY OF PUERTO RICO

Directed by: Prof. Jeffrey Duffany

In the past few years, social media platform and video game use has increased massively. Even people who were once opposed to the idea of playing video games or using social media websites have now integrated such activities into their daily lives. This includes children, and while it could be argued that parents should not be allowing their kids to get online and interact with strangers, one thing is certain: Wherever children gather, virtually or otherwise, sexual predators may potentially follow as well. In this research various tests are conducted, utilizing different tools, to examine the accuracy with which they could approximate users' ages, based on their written texts. The findings of the tests showed that there is still work to be done to reach the level of accuracy and effectiveness that is necessary for the protection of children online. A Visual Basic program and Crystal Reports were utilized to display the results of these tests and to provide a proof of concept for the future of online security.

## TABLE OF CONTENTS

Page

## LIST OF FIGURES

## LIST OF ABBREVIATIONS

| | |
|---|---|
| AI | Artificial Intelligence |
| ANN | Artificial Neural Networks |
| CS | Computer Science |
| DM | Data Mining |
| DF | Digital Forensics |
| HART | Harm Assessment Risk Tool |
| LSTM | Long Short Term Memory |
| NCMEC | National Center for Missing & Exploited Children |
| IP | Intellectual Property |
| ML | Machine Learning |
| NLP | Natural Language Processing |
| URL | Uniform Resource Locator |
| Wi-Fi | Wireless Fidelity |

# CHAPTER 1

# INTRODUCTION

Technology has been on a continuous rise since the computer appeared on the cover of Time Magazine in January 1983. Since then, more and more ways to facilitate every aspect of life, like waking up, driving, working, and relaxing, have been created and seamlessly integrated. Future generations will surely continue this constant stream of innovation. Today, the world is connected through the power of the Internet. Everyday appliances come with computers inside them, TV's can easily connect to Wi-Fi Internet, and self-driving cars are no longer something only found in cartoons or Science Fiction novels. However, with all this progress, criminals also have been finding ways to adapt to changes. Digital forensics is an answer to that adaptation.

## 1.1 Purpose

Digital forensics is defined as a process "uncovering and interpreting electronic data with the goal of processing and preserving any evidence in its most original form while performing a structured investigation by collecting, identifying and validating the digital information for the purpose of reconstructing past events." (Techopedia, 2018). Today, there is a need for digital forensics due to the high number of criminal cases where computers or smartphones have been used to commit crimes. As long as crimes are being committed virtually, digital forensics and cybersecurity firms must be alert and up to date on criminal tactics. Part of the purpose of this research is to answer the question: What tools and techniques are being used to stop these virtual crimes from happening, and how effective are they

currently?

The goal of this research is to provide a clear picture of the present status of our digital environment and society. It seeks to reach an educated conclusion based on factual evidence and statistics where it is expressed and illustrated whether digital forensics and other cybersecurity branches are currently representing a stopping force against virtual crimes and to determine if users, specifically children, are being protected online. How many kids come into contact with a sexual predator? On what platforms? How many reach contacts in the real world? Are parents aware of these online interactions? How are parents setting boundaries to avoid this type of exposure? These matters will be subsequently discussed in the following chapters.

### 1.2 Background of the Study

Criminals are constantly finding ways to adapt to the advances in technology, exploiting the novelty of these changes to commit crimes in different ways. In the past, it was very difficult to catch criminals because there was less surveillance and ways to identify them, as the United States saw with the infamous case of Ted Bundy. This series of events transpired in a decade where law enforcement could only interact with other jurisdictions through landlines, physical mail, and - in most cases - not at all. This is particularly what enabled criminals to commit crimes and avoid capture for longer periods of time than what is considered to be the norm today.

Now, everything is connected through the Internet and it is much easier for some criminals to make mistakes and for authorities to detect and stop crime from

happening than it was a few decades ago. However, this access can also be used as a gateway for other criminals to infiltrate everything from finance to online games like Fortnite. Interactive online games that promote connecting with other players across the globe tend to be a common scenario for criminals to exploit its unsuspecting player base, particularly children. An article written by Robinson (2018) states that, “Given that around 125 million people actually play Fortnite, it has the potential to become a new breeding ground for predatory behavior.” Moreover, he goes on to say that during a raid made in New Jersey to arrest people using this popular game to attract children, a total of twenty-four individuals were arrested and among them were a police sergeant and a firefighter. Many social media websites and applications have policies against criminals utilizing their services, yet this does not appear to be working either by lack of enforcement or simply by lack of an effective means to detect criminals.

Fortunately, law enforcement authorities in cooperation with university researchers and digital forensics experts have been attempting to identify and bring criminals to justice with the use of state-of-the-art technology such as artificial intelligence (AI) using natural language processing. On the importance of artificial intelligence, Matt Coatney (2017) states:

> AI technologies have already made their way into digital forensics, even if they were not marketed as such. Sophisticated algorithms are used today for DNA sequence matching, e-discovery document review, and cyber-crime detection, and more use cases are in the works. Some researchers are exploring how AI can facilitate improved collaboration when it comes to

> the analysis of cyber-crimes around the world. Others are experimenting with how AI can assist with recognizing patterns in the programming signatures of suspected criminals or wayward employees. (para. 5)

With the use of natural language processing (NLP), artificial intelligence is becoming more and more effective in detecting specific patterns and human speech every day. This is because natural language processing attempts to bridge natural human communication and computer processing and understanding, which may be the key for accurately detecting criminals on the web before they act.

In a recent article, two researchers at Purdue Polytechnic Institute, Rayz & Seigfried-Spellar (2018) showcased an effective utilization of AI in the pursuit of providing a safer environment for adult users and children alike. They analyzed many different conversations between predators and minors in different countries to obtain data to pass to their artificial intelligence, with the goal of teaching it many techniques and speech patterns that predators use around the world, so that the AI can flag these types of patterns when it sees it in chatrooms or other social sites. They hypothesized that, by analyzing many conversations with NLP and employing statistical discourse analysis, the AI could possibly tell the difference between an innocent person and a criminal just by the way predators communicate. Rayz & Seigfried-Spellar (2018) also state that one in twenty-five children are sexually solicited online, which presents the importance of having a way to flag and expose these criminals before they can act and hurt others online and in the real world.

This type of technology's impact could possibly be implemented to detect all types of online crimes, and that is where future technology and cybersecurity solutions could be moving towards. The key is to make artificial intelligence tools and algorithms as accurate as possible, because incorrectly flagging individuals as potential criminals is not acceptable. Additionally, determining what type of data to collect on suspicious individuals before or after they raise a red flag can let the artificial intelligence know if those people are in fact engaging in criminal behavior or not. And if the threat is confirmed to have been detected correctly, what actions should be taken next.

## CHAPTER 2

## DIGITAL FORENSICS AND DIGITAL CRIME

Digital forensics, also known as cyber forensics, is defined as: “the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law.” (Rouse, 2014). Digital forensics began as a branch of forensic science that specialized in crimes perpetrated with the use of computers (known as cybercrime) but has since become its own area of knowledge and expertise. Most of the same principles of forensics apply to digital forensics (DF) as well. For example, “Locard’s Principle of Transference” which states that “one cannot interact in any environment without leaving something behind.” (Easttom, 2014, P.79). This principle applies to both criminals and forensic investigators alike because keeping this principle in mind during an investigation guarantees that a crime scene is not altered or tampered with, as this could compromise the entire investigation’s legal standing. Digital forensics has been instrumental in the apprehension of many criminals in recent years, and courts have become more aware of the processes and the legality that is involved in cases involving cybercrime.

Furthermore, digital forensics follows the same rules for evidence acquisition that apply to regular law enforcement procedures. Failure to follow these rules during investigations could lead to cases being dismissed in a court of law. To this end, digital forensics has two main goals. The first is to find out what happened and what data or entity was affected. The second is to collect the

evidence in a manner that is recognized as acceptable to be presented in a court of law. All digital forensics investigators must possess knowledge of all components and underlying functions of computers, mobile devices, and any medium in which information can be stored and accessed. For example, a digital forensics investigator should be aware of common tactics used by criminals such as steganography, which is the art of hiding objects of importance inside other objects. A simple use of steganography used by criminals is the act of changing the file extension of the file they intend to protect, because this effectively hides it in plain sight. The investigators should also have essential knowledge about the laws and processes of crime scene investigations.

### 2.1 Digital Evidence Procedures

The procedures for collecting evidence during a digital forensics' investigation are just as important as anything else related to a given case. All digital forensics personnel must ensure that no human rights are violated in their proceedings. According to the Fourth Amendment of the United States Constitution (U.S. Const. amend. IV), which reads:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

It can be stated that a seizure is any interruption in a person's accessibility to any of their property; therefore, evidence must never be collected illegally. After

probable cause has been determined and a warrant is issued by a court, the first step is to secure the crime scene by allowing no unauthorized access to the devices that have been seized, this includes remote connections to the devices. A common technique is to place the devices in Faraday bags. These bags cancel out any outgoing or incoming signals from and to the suspect device. Once the evidence has been collected and properly secured, chain of custody must be maintained at all times; this could determine if the case holds up in court. To this end, forensic investigators must keep an updated log of where the evidence is, who has handled it, and at what times.

Given the sensitive nature of digital evidence, all seized devices must be transported to a digital forensic laboratory. This specialized facility is where analysts will create a copy or “image” of the evidence to be analyzed, so as to preserve its integrity. Criminals have methods and tricks for hiding illegal data so forensic analysts must be aware of all the places data could be stored. Once the forensics analysis team have concluded their investigation on the data that was recovered, it is then prepared to be presented during trial by a forensic investigator acting as an expert witness.

The forensic tools utilized during the analysis of the evidence must be thoroughly explained by the expert so that the process can be fully comprehended by all parties in court. This is why experts must adhere to the Daubert standard with regards to the tools and techniques used in this phase of the investigation. The Daubert standard states that “any scientific evidence presented in trial has to have been reviewed and tested by the relevant scientific community.” (Easttom,

2014, p.46). Ultimately, the designated forensics expert must be knowledgeable in all the stages of a digital forensics investigation, adhere to the code of ethics in place, and have an unimpeachable background because opposing counsel could question their methods and character with the motive of having the case and its evidence dismissed.

### 2.2 Cybercrime

Cybercrime are the crimes that digital forensics usually investigates. These crimes can be of a variety of natures. Cybercrime can be defined as:

> …any type of illegal scheme that uses one or more components of the Internet (chat rooms, email, message boards, websites, and auctions) to conduct fraudulent transactions or transmit the proceeds of fraud to financial institutions or to others connected with the scheme. Cybercrime also applies to generating spam emails, downloading viruses or spyware to computer, harassing another through the Internet, child pornography, and solicitation of prostitution online. Perhaps the most prominent form of cybercrime is identity theft, in which criminals use the Internet to steal personal information from other users. (US Legal, 2018)

This means that essentially every online or offline crime or attack that is perpetrated with the use of a computer, phone, or any other electronic device can therefore be considered a cybercrime. There is no shortage of ways for criminals to commit a cybercrime; the more technology advances, more and more ways to commit crimes emerge, affecting the forensic process as well.

Right now, the internet is a free space and for some people the anonymity that comes with it is an emboldening factor. Apart from identity theft, one the most commonly known types of cyberattacks are viruses. In recent years, viruses have been known to come in the form of a fake antivirus that installs itself on a computer without the user's consent and prevents the user from downloading a real antivirus tool. Other types of cyberattacks include spyware, which monitors a user's computer actions, and ransomware, which takes the computer's operating system hostage and demands a monetary amount for its release back to the user. Ransomware has become one of the most popular forms of attacks used by hackers and cybercriminals to date, and it has been documented that during a ransomware attack, monetary payment to the attackers usually do not result, after all, in the victim's system being released.

With the advent of social media platforms and the increased acceptance towards video game culture, cybercrimes and attacks have become more personal in nature. A big part of cybersecurity today falls upon educating the user on the best practices of computer and Internet use. To illustrate, on September 5, 2018, NBC5 News reported that a naked 21-year-old man broke into a girl's home after he stalked her through her Instagram posts. The girl had uploaded to her account pictures with her location information (also known as geotagging) which the man used to find out where she lived. The report states: "Ward found out where girls lived based on their social media posts, according to police, and they believe Ward broke into the girl's home previously, since he was caught on indoor surveillance cameras." (NBC, 2018). This is of relevance because Instagram's policy

specifically states that sexual offenders are not allowed to use their platform, yet this is not stopping offenders from accessing this and other websites.

### 2.2.1 Commonwealth vs. Emanuele

An example of a cybercrime and its resulting digital forensics investigation can be found in *Commonwealth vs. Emanuele*. On March 2012, authorities in Charlottesville Virginia, received a cybertip from the National Center for Missing & Exploited Children (NCMEC) stating that a certain email address was soliciting illegal images in a website that was known for hosting that kind of content. Soon afterwards, authorities contacted a digital forensics investigator to handle the case. Not having probable cause or a warrant, they arrive at Emanuele's home hoping he will cooperate on his own. Mr. Emanuele, a two-time sex offender, allowed the investigators to seize and investigate any equipment of interest, even agreeing to let them take the devices to be forensically analyzed. It did not take long for the digital forensics team, using the forensic software tool, EnCase, to find hundreds of child pornography files on Mr. Emanuele's hard drive . The digital forensics team – now having probable cause – requested and received a search warrant for the computer on which they found the files so that Mr. Emanuele's consent could not be retracted, which he later tried to do.

Following this initial discovery, the forensics team requested and obtained two more search warrants; one for Mr. Emanuele's house and another for his previous one. This was because they left many CD's and storage media behind on their first visit to Mr. Emanuele's house containing more potential evidence. Next, the digital forensics team arrived at the next location, now belonging to Mr.

Emanuele's ex-wife, for their second investigation. This time they found more child pornography on old storage media stored in a junk shed. Finally, the Prosecutor on the case tasked the forensics team with determining the top ten worst evidence files to indict Mr. Emanuele. On April 2013 Mr. Emanuele pleaded guilty to multiple counts of possession of child pornography and is serving fifteen years in prison and lifetime probation.

The mentioned case is only one of millions found in The United States. According to the National Center for Missing & Exploited Children's Key Facts statistics for 2018, the FBI determined that a total of 424,066 missing children entries were made by the end of the year. Furthermore, a total of 18 million reports of exploited and abused children were made to the NCME Cybertip line. The issues of the reports made to the tip line were related to:

- Apparent child sexual abuse images
- Online enticement, including sextortion
- Child sex trafficking
- Child sexual molestation

Criminals will utilize any advantages they are given, and in this technological era, they no longer have a need to go outside and expose their identity in order to commit crimes or establish contact with minors.

### 2.2.2 Video Games and Crimes Therein

For decades, video games have been brought into family's homes as a means of entertainment. While they once were an offline experience, players are now able to connect to play and chat together across the globe. To illustrate, a

total of 90 billion US dollars are expected to be made in 2020, from the 78.6 billion dollars made in 2017 (WePC, 2018). Today, there is an estimated amount of 2.5 billion people who play video games worldwide, and with many of this population being children it is a clear grooming ground of choice for criminals and sexual predators to attempt to find unsuspecting people to victimize. During 2018, an online multiplayer game called Fortnite became one of the top 3 most played video games in the world, but it didn't take long for news outlets to report that sexual predators were using the game's voice chat and on-screen text capabilities to reach and exploit children. Figures 1, 2 and 3 illustrate the results of WePC (2018) research *2018 Video Game Industry Statistics, Trends & Data - The Ultimate List*.

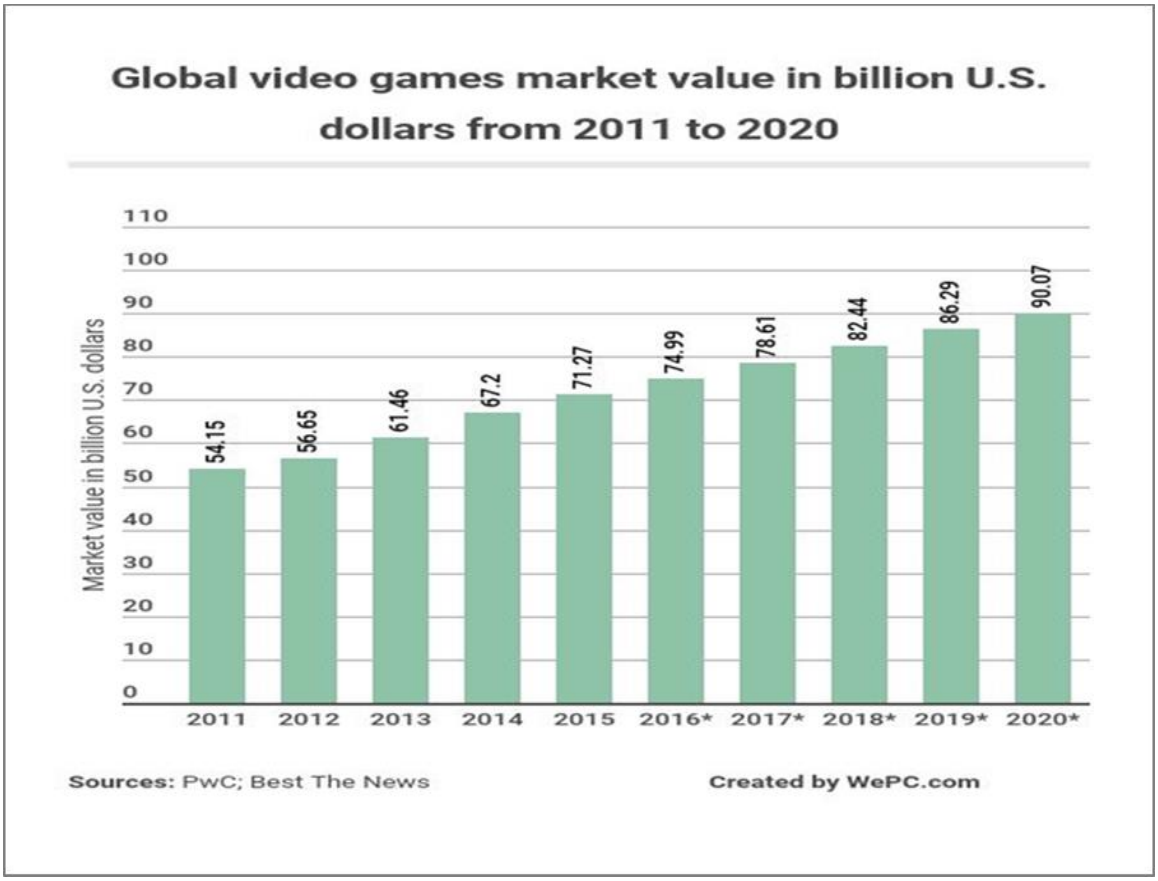



Figure 1. Market Value in Billions, Showing a Steady Increase

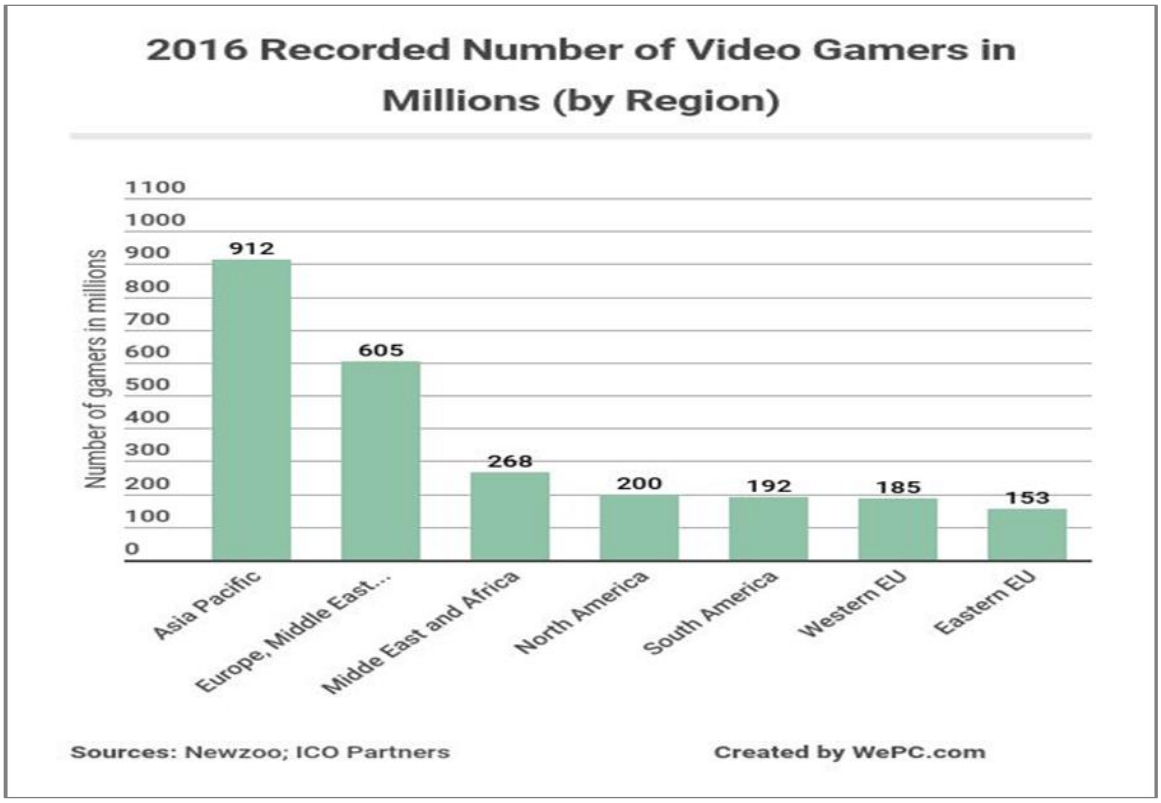



Figure 2. Population of Video Gamers by Region

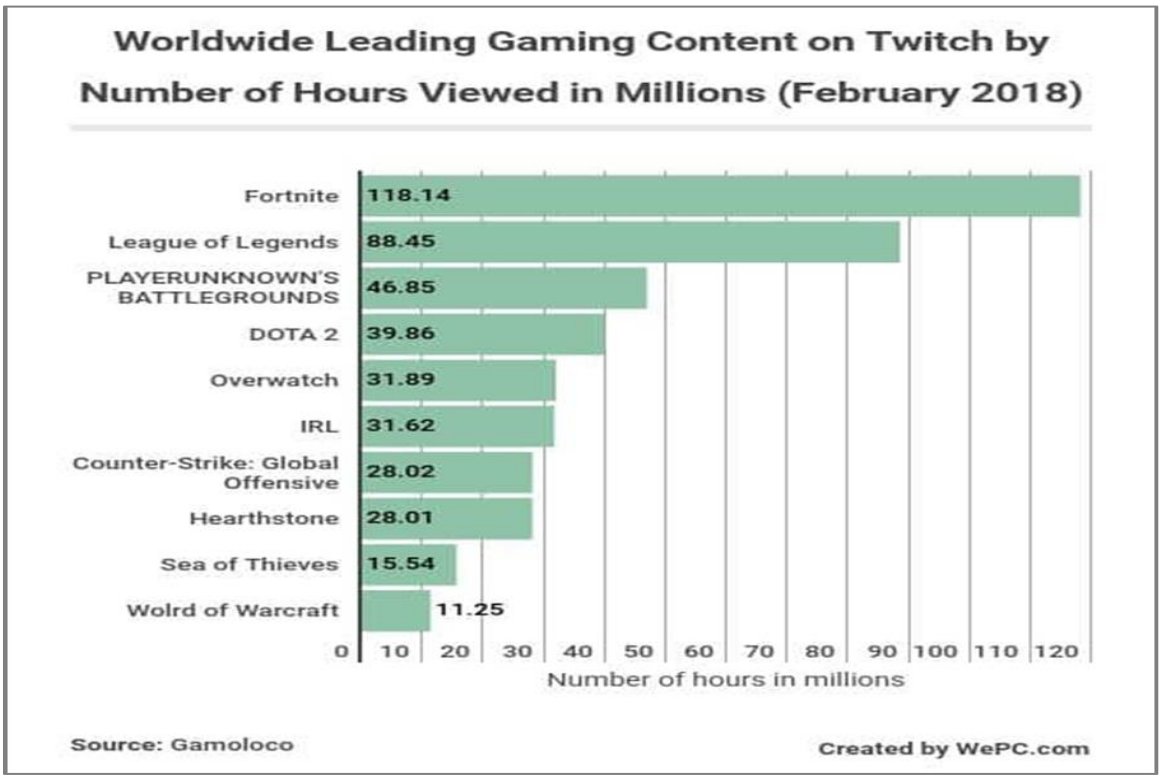



Figure 3. Video Game Statistic for Most Viewed Game on Twitch (in millions of hours)

It is projected that video games will only continue its revenue trend, generating billions of dollars to the economy, which is directly proportional to video game use. For 2019, the approximate revenue given is 86.29 billion and for 2020 the statistics showed a projected increase to 90.07 billion dollars in revenue. In the second figure, we can see the population of gamers across the globe. The leading region in terms of population in millions is Asia with 912 million, followed by Europe, the Middle-East, Africa, and the North America. This clearly shows the number of people that play video games around the world, which is a number that is expected to increase as the years go on. Figure 3 shows statistics for the number of hours viewed in millions. To provide background, Twitch is a streaming platform for gamers and artists alike where they can play or create for an audience. Users decide who they want to follow and filter by the game they want to watch. In February, the most viewed game on this platform was Fortnite, leading with 118.14 million hours viewed.

Consequently, on September 2018, David Nath wrote a report for Fox News containing the FBI's recommendations on the Fortnite predator issue after a sting operation they conducted, that reads:

> "Operation Open House" saw law enforcement agents posing as underage players in order to snare online predators soliciting kids for sex through "Fortnite," believed to be the world's most-played video game at the moment. FBI Special Agent Kevin Kauffman is now warning parents to get more involved in their kids' game-playing world, sooner rather than later. "This is a tool that the predators are using to go out and get after your kids,"

> Kauffman said, adding "I would say that a good percentage of them are not who they say they are." (2018)

The FBI suggests that parents being more involved in their kids' play time and disabling the in-game chat functionalities could be a key factor in keeping them from being exploited by criminals. Another report by British newspaper The Telegraph, stated that a mother became aware of Fortnite when she overheard her 12-year-old son was being offered money to perform sexual acts for a man grooming him through the game. Once more, the recommendation was that education and, in this case, communication between parent and child play a big role in online security. Evidently, cases such as these are not exclusive to the United States, they can happen anywhere in the world.

WBTB News 13 released an article on November 2018 in which it was reported that the South Carolina Horry County Sheriff's office receives referrals from social media apps or video games such as Fortnite several times a month and sometimes on a weekly basis. A Lieutenant working at the Sheriff's office stated that they've also had cases of money laundering and others where the criminals scammed children for money, convincing them to reveal their parent's credit card information. The referrals that are received by the department are sent to the National Center for Missing and Exploited Children. The article also provides statistics for these types of incidents stating:

> Statistics from the Crimes Against Children Research Center said, one in five children between ten and seventeen years of age reported receiving unwanted sexual solicitation online. The Horry County Sheriff's Office said

a lot of the time it goes unreported. That same study showed only a quarter of those who encountered sexual solicitation told a parent. (Calhoun, 2018) This shows that most of the cases happening around the world of similar criminal nature are not being reported to the pertinent authorities and are not followed up on in meaningful ways. In fact, Epic Games' Fortnite Policy states that no one can use their game to harm others or for any illegal activities, but this is not stopping anyone.

Conversely, the cases that have been reported by news outlets all seem to suggest that the solution to these cases is to educate children on proper Internet use and to be more present and aware of the people they talk to. Another incident of sexual harassment where a predator utilized Fortnite is the case of Anthony Gene Thomas. Thomas is a 41-year-old man from Florida that first established contact with his victim through the game voice chat and eventually met the victim in person for sex. When the police arrested Mr. Thomas, his phone contained pornographic images of the minor. The author of the article, David Neal (2018), states that, Ashley Moody, the attorney general reviewing the case said: "This case is disturbing not only because it involves child pornography, but also because a popular online game was used to communicate with the victim.", urging parents once more to be aware of their children's online actions.

Finally, in Montreal, police received similar reports of four children that were victims of sexual extortion. According to the article *Police Investigate Sexual Extortion Case Involving Game Fortnite* written by The Canadian Press (2018), the characteristics were the same: young males contacted through Instagram's chat

feature –violating Instagram's policy on sex offenders– promising reward codes for reaching a higher level in Fortnite in exchange for explicit pictures. The article stated that when the child predator received the images from the kids, he proceeded to threaten and blackmail them for more explicit images. The takeaway given by local authorities being that, users should never share personal information with strangers. Moreover, how do social media platforms such as Instagram detect whether or not a criminal is indeed using their service in violation of their policies and what detection methods and technologies are currently being used to detect crime in general?

## CHAPTER 3

## THE IMPLEMENTATION OF ARTIFICIAL INTELLIGENCE

In this technological era, computers are being programmatically trained to understand human behavioral patterns and even the context of speech used in conversations. With companies like IBM and Google developing their own, artificial intelligence is slowly moving away from being something only found in science fiction. In an article titled *What Is Artificial Intelligence? Examples and News in 2019*, Sraders (2019) defined artificial intelligence as "the use of computer science programming to imitate human thought and action by analyzing data and surroundings, solving or anticipating problems and learning or self-teaching to adapt to a variety of tasks." These are complex algorithms used for application in a seemingly boundless variety of fields.

There are three main divisions of artificial intelligence: neural networks, machine learning, and deep learning. In the aforementioned article, Sraders explains these divisions as:

> Neural networks (often called artificial neural networks) essentially mimic biological neural networks by "modeling and processing nonlinear relationships between inputs and outputs in parallel." Machine learning generally uses statistics and data to help improve machine functions, while deep learning computes multi-layer neural networks for more advanced learning. (2019, para. 5)

Artificial intelligence is further divided into two other classifications depending on its purpose and design. Weak AI is characterized with having the need for

supervision and the responses generated by the AI are mostly programmed into it. Examples of weak AI are Amazon's Alexa or Apple's Siri, because they are programmed to return certain responses depending on the keywords that they receive from the user. Unlike weak AI, strong AI, for the most part, requires no supervision and the responses are not programmed; this type of artificial intelligence is known for being able to teach itself things based on the data it receives.

In the same fashion, yet another distinction between artificial intelligence has been defined and created, and these are now classified as specialized artificial intelligence and generalized artificial intelligence. What separates these two types of AI's is their proposed area for application. This division is defined as:

> Specialized AI is AI that is programmed to perform a specific task. Its programming is meant to be able to learn to perform a certain task - not multiple. For example, from self-driving cars to predictive news feeds, specialized AI has been the dominant form of AI since its inception (although this is rapidly changing). On the other hand, general AI isn't limited to one specific task - it is able to learn and complete numerous different tasks and functions. In general, much of the cutting-edge, boundary-pushing AI developments of recent years have been general AI - which are focused on learning and using unsupervised programming to solve problems for a variety of tasks and circumstances. (Sraders, 2019)

As presented, generalized artificial intelligence has the capacity to be applied to any kind of situation regardless of the nature involved, rather than only

being able to handle a specific problem, as is the case of specialized artificial intelligence. The excitement around artificial intelligence for the future is typically attributed to generalized artificial intelligence because of its versatility and flexibility to be applied to any industry field.

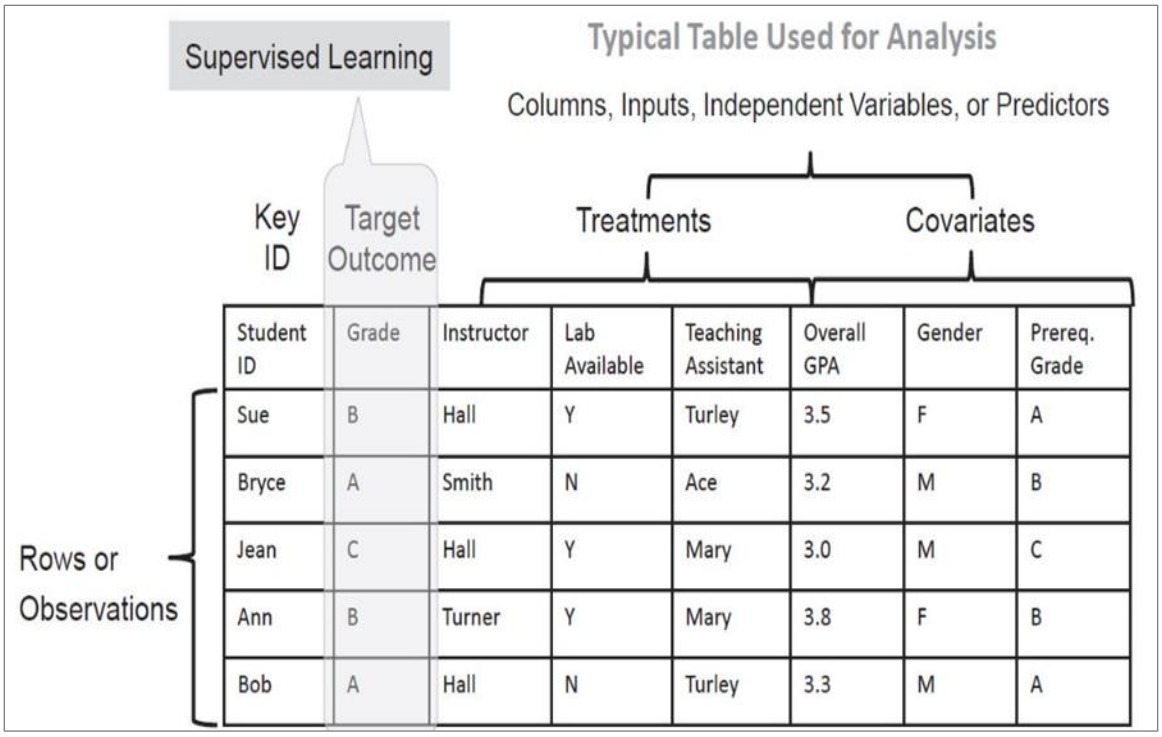
Correspondingly, between specialized and generalized AI, the world has been coming into contact with artificial intelligence more and more every day. For example, users of the video streaming service Netflix come into a subtle contact with AI when they watch a movie or TV series because the AI will base suggestions for the users based on their previously watched content. Another example of AI that is already being tested and applied in society is Facebook. Facebook has implemented an AI to push the content it thinks you want to see even higher, filtering content based on the user and its built-in algorithm. Finally, despite having publicly expressed his reservations regarding AI, Tesla and SpaceX's Elon Musk has been researching artificial intelligence and applying it in the world today as well. Tesla has been implementing various artificial intelligence and crowd-sourced data for their self-driving vehicles to improve their navigation and system. This is all made possible through the machine learning applied to create these advanced algorithms.

### 3.1 Machine Learning

To further explain the learning process within an artificial intelligence, we will focus on strong artificial intelligence. Machine learning and deep learning are two elements that are instrumental in helping an AI understand information of any nature. In fact, as AI continues to grow and adapt itself to different types of

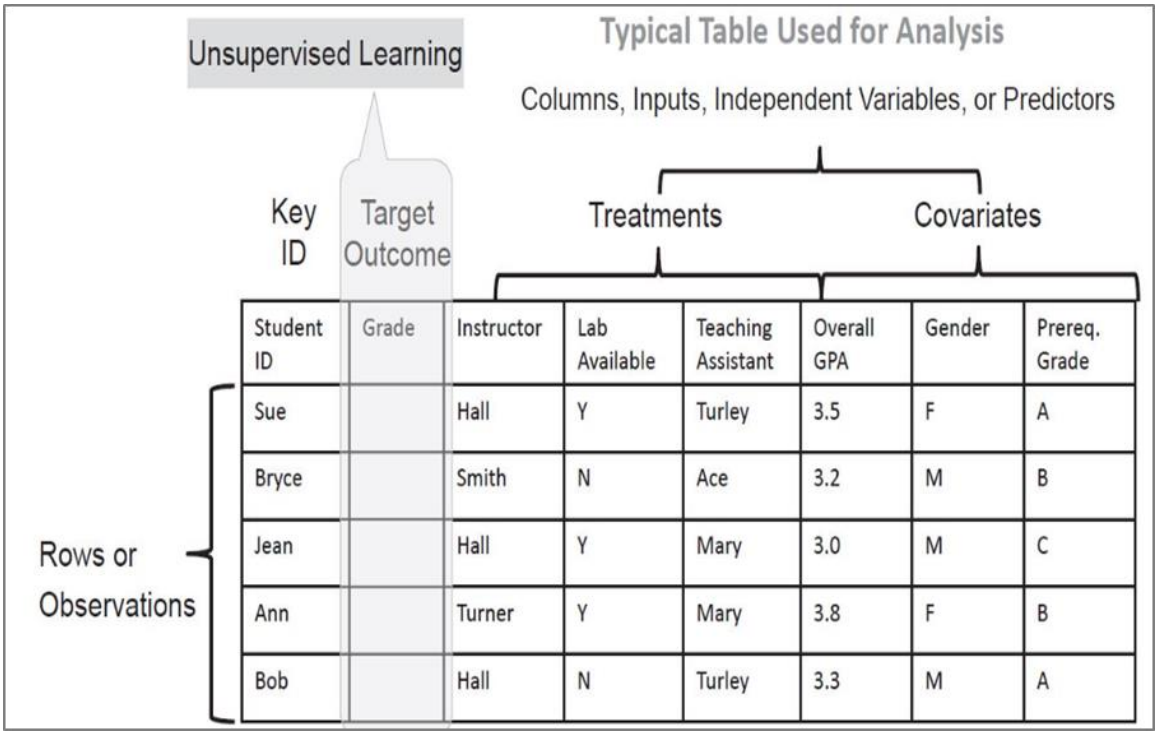
businesses, it is faced with a diverse plethora of problems that it then learns how to solve. Here is where the multiple learning processes take place. First, there are two kinds of machine learning. These are classified as supervised and unsupervised learning.

Supervised learning is similar to an instructor teaching a student about a given subject and the concepts within that subject. According to Marr (2017), in a *Forbes* article, supervised learning is the most common type of machine learning used in industries for a wide array of purposes. Additionally, the output or results of this type of learning is known to the programmer because they operate in a fashion similar to other programs where the programmer can adjust the algorithms as necessary to guide it towards the desired output. On the other hand, unsupervised learning for artificial intelligence connotes a more complex process. Furthermore, according to Pilcher (2019) in his article for elderresearch.com, unsupervised learning is similar. But the key difference is found in that the target outcome is not dictated to the system. In supervised and unsupervised learning, the same input data is given to the system to be processed, but the target outcome is not given in the latter. Studies show that both types of learning do yield similar results, albeit through different processes and logic. Figures 4 and 5 illustrate the difference between these two types of machine learning.




| Student ID | Grade | Instructor | Lab Available | Teaching Assistant | Overall GPA | Gender | Prereq. Grade |
|---|---|---|---|---|---|---|---|
| Sue | B | Hall | Y | Turley | 3.5 | F | A |
| Bryce | A | Smith | N | Ace | 3.2 | M | B |
| Jean | C | Hall | Y | Mary | 3.0 | M | C |
| Ann | B | Turner | Y | Mary | 3.8 | F | B |
| Bob | A | Hall | N | Turley | 3.3 | M | A |

Figure 4. Example of Supervised Learning, Where Target Outcome is Given




| Student ID | Grade | Instructor | Lab Available | Teaching Assistant | Overall GPA | Gender | Prereq. Grade |
|---|---|---|---|---|---|---|---|
| Sue | | Hall | Y | Turley | 3.5 | F | A |
| Bryce | | Smith | N | Ace | 3.2 | M | B |
| Jean | | Hall | Y | Mary | 3.0 | M | C |
| Ann | | Turner | Y | Mary | 3.8 | F | B |
| Bob | | Hall | N | Turley | 3.3 | M | A |

Figure 5. Example of Unsupervised Learning, Where Target Outcome is not Given

Pilcher (2019) also connects with this research in a meaningful manner:

> Unsupervised learning is technically more challenging than supervised learning, but in the real world of data analytics, it is very often the only option. For example, to create enough labeled cases when building a model to detect fraud, it's usually impractical to investigate (and thereby label) enough cases in a sample of data to see whether fraud exists. Without definitive historical information about target outcomes, the data scientist must use unsupervised learning techniques to build a model, and then look for anomalies (unusual cases) as a good place to start investigations. (para.8)

This quote is of particular interest, because it states that if an artificial intelligence were to be developed for the security of online use, unsupervised learning would be an ideal starting point. This is due to the way that unsupervised learning utilizes given input data, as well as the nature of the data that is being proposed as input. For a system to understand what suspicious activity and criminal predatory behavior looks like, it must take in many conversations and chatroom encounters as data, while also having the freedom to make its own conclusions about what is to be understood as a threat or crime. This does not mean that researchers should ignore supervised learning entirely; tests must be conducted to decide which model of learning works best for the desired results.

This is the type of AI that is referenced when people talk about machines that are teaching themselves without the need of a human supervising their actions

or guiding them. The outcomes of the AI are unknown because it attempts to solve an elaborate problem – in any field of study – without any previous related data to guide it, using only the logic they were programmed with initially. For example, in supervised learning a human would have to explain the problem at hand to the AI, while in unsupervised learning, the AI would be capable of figuring it out on its own. Companies and their research teams such as Google's Deep Mind, and IBM's Watson division, have been hard at work at further developing more independent AIs that are capable of being applied to any scenario in any industry or field. Artificial Intelligence attempts to think like a human brain using a process called artificial neural networks", which has the ability to create human language models; however, how can an artificial intelligence understand human conversations and the underlying context therein? This all connects with our current research in that, an implemented artificial intelligence for the detection of online crime must fully understand that crimes have many ways of being committed, so it must also adapt to the different scenarios and conversations which could be presented at any moment. If developed successfully, machine learning will lead to a precise, accurate detection tool for stronger cyber security.

### 3.2 Natural Language Processing

While machine learning in all its forms has helped create models for the use of human language, what truly allows an artificial intelligence to understand and analyze what is being said in conversation, including the context under which the conversation is being said, is the use of natural language processing (NLP). The study of natural language processing has been around for quite some time, but it

is now that it has gained an increased amount of attention because of the value and functionality it brings to human-computer interactions, and – consequently – to artificial intelligence. Analytics Software and Solutions Group SAS Institute defines this component of artificial intelligence as:

> Natural language processing (NLP) is a branch of artificial intelligence that helps computers understand, interpret and manipulate human language. NLP draws from many disciplines, including computer science and computational linguistics, in its pursuit to fill the gap between human communication and computer understanding. (2018)

Large datasets comprised of text can be analyzed with the use of natural language processing, making it possible for machines to read, hear, and recognize what parts of speech are important. To no surprise, machines can analyze these datasets with an ease and consistency that humans are unable to match. Understanding syntax and the correct context of a conversation is crucial for AI's ability to distinguish between different types of intent.

With the purpose of understanding intent within speech recognition, natural language processing has developed various techniques over the years. These techniques have been made possible through the combination of natural language processing with deep neural networks. Long short term memory (LSTM) is one of these techniques, which Harper (2019) of AI Business described as "a type of deep neural network designed for time-series analysis. When applied to NLP, it helps remember the various words - and their significance - for different parts of longer sentences or paragraphs." LSTM is very useful for optical character recognition,

which aids an artificial intelligence in translating languages, by increasing the speed of its text and speech recognition.

Further enhancing natural language processing, memory augmented networks are essentially deep neural networks that build upon long short term memory's text analysis functionality by elevating the latter's comprehensive capabilities. A memory bank that can be consistently read and written to and over is what helps memory augmented networks operate because they are able to store the context of a conversation and learn to create relationships between those contexts. This functionality within natural language processing could present a cornerstone on which strong artificial intelligence can stand for detecting online criminal activities. If natural language processing could enable an AI to store context and compare it to real-time conversations using a robust dataset of past instances and environments where a similar context was used, then artificial intelligence could potentially act as an accurate and effective deterrent against cybercrime.

## CHAPTER 4

## THE DETECTION OF ONLINE CRIME

Cybercrime has been growing consistently in number, and the nature of the threats they present has consistently transformed and adapted with the advances in technology. These cybercrimes can result in the loss of data and currency, which has even brought about bankruptcy for some companies around the world, not to mention physical harm to users. Many companies have been trying to detect criminals within their networks using a variety of methods, and Microsoft has stated that hackers can be within a network for up to 146 days before being detected. This is an extensive amount of time for a threat to be infiltrated in a system. This is also true for websites and chatrooms where criminals can plan their attacks and target others without repercussions. However, to understand the detection of online crime it is essential to comprehend the basics for detection of offline crime as well.

To illustrate, crime has been around for centuries with no signs of stopping and as a result, countermeasures have been developing along with it. This is why criminal profiling was created; to better understand the motives of criminals in the hopes of stopping them before they are able to harm another person. One of the most prominent of these methods is that of profiling. Offender or criminal profiling is defined by Turvey:

> The identification of specific characteristics of an individual committing a particular crime by a thorough systematic observational process and an analysis of the crime scene, the victim, the forensic evidence, and the

known facts of the crime. The profiling technique has been used by behavioral scientists and criminologists to examine criminal behavior, and to evaluate as well as possibly predict the future actions of criminals. (2017)

In his article the author states that the analysis of the psychology of criminals is a determining factor in the process of predicting future attacks of the same kind. This process involves building a big enough body of data consisting of common patterns and behaviors in order to build a general description for these types of suspects. Offender profiling has helped to capture many criminals throughout decades, but in order for it to continue to do so, it must be applied to cybersecurity. Establishing a digital means for criminal profiling could prove to be the key for a more secure future for generations to come. However, for artificial intelligence to understand what separates a sexual predator from an innocent person, the AI must receive the necessary data based on previous cases and predatory behavior including repeated speech patterns, tactics, and tells or giveaways. This will help the artificial intelligence to define what a predator talks, acts, and maybe even thinks like, to identify them successfully and without making mistakes in this identification process. This is why it is important for the correct information to be passed to the AI, because the algorithm's output will only be as efficient as its input.

To provide an example, on the topic of child predators, Easttom (2014) describes the process of adults who prey on children stating that predators tend to initiate contact via social media which, as aforementioned, has crossed over into video games as well. First, these predators will attempt to determine if the child is

a likely target by looking for signs that the child feels he or she is not getting enough attention, doesn't feel accepted, or is going through something emotional like a divorce. Second, predators will present themselves to be empathetic towards the child and provide a means of conversation in a platform where they feel is more advantageous for them. Next, the criminal will begin to initiate flattery and convince the child to integrate sexual content into the conversations, being careful as to not causing the child to feel scared. Finally, once the criminal feels comfortable enough for a physical meeting, they will suggest something like watching a movie together.

This process varies from predator to predator, and some avoid sexual conversations altogether. But this kind of information, collected and amassed through techniques such as data mining (DM), can prove instrumental for building a *Modus Operandi* that can be possibly fed into an artificial intelligence (or another form of a strong detection system) as test data with the objective of aiding in the detection of these criminals and to, ultimately, keep these crimes from taking place. Artificial intelligence could provide a means to eliminate the need for detectives to go undercover into chatrooms where criminals lurk in attempts to bait them into getting caught. Instead, the artificial intelligence could be guided to monitor such chatrooms and determine if a criminal is actually there, report the information to the necessary authorities, and facilitate the way to take the required actions.

Additionally, on February 2019, yet another incident involving sexual predators harming children occurred on the popular video platform, YouTube. According to an article written by Alexander (2019), a user of the platform brought attention to the matter showing that by searching for videos of females trying on

new clothes, videos of minors would also come up as recommendations. The problem was not in the videos themselves as they were not pornographic, but rather in the comments section of the videos, which featured predators sexualizing the children in the videos and commenting on how attractive they found the minors. Subsequently, YouTube acted swiftly on the matter by disabling the comments on the videos that contained that type of content and deleting the accounts associated with the comments of predatory nature. In the end, a total of over 400 YouTube accounts were terminated and over tens of millions of comments were deleted in the attempt to rid the platform of predatory content. Moreover, advertisements from companies such as Disney, McDonald's, and Epic Games (Fortnite's creator) have been pulled from the video streaming platform as a form of protest against this controversial issue. YouTube also received criticism for the reliance on the current algorithms they have in place to take down videos against their policy, because several inoffensive videos were wrongly taken down as a result of the explicit comments that were left in their comments section during this scandal; hence, exposing an area where YouTube could improve in the future.

However, YouTube's preventive actions have not stopped predators and scandals from surfacing, and they are attempting to approach the problem from different angles. It appears this is something that will simply prove insurmountable by human action, which is where an artificial intelligence tasked with the detection of criminal behavior and the eradication of accounts exhibiting predatory behavior could take center stage. Ideally, this artificial intelligence would be capable of sifting through large volumes of content at a speed unparalleled by its human

counterpart. This scandal should serve as a warning and a call to action for artificial intelligence creators to focus their efforts on protecting minors as well as providing security to other users on the Internet, wherever they may be browsing. The question of what data should be fed into an artificial intelligence to ensure that its detection accuracy rate is high enough so that false positives don't occur within its algorithm on this front still exists. To this end, the algorithms of these AI must be as robust as possible, if they are to yield the maximum amount of efficiency and security to the children that are involved in attacks such as this YouTube scandal.

### 4.1 Current Applications

All different elements of a crime are indeed important for determining if an online user is a predator or not. Previous data on what actual predators behave and act like would play a critical role in this analytical process, especially for the future implementation of artificial intelligence and natural language processing for crime detection. Recurrent behavior such as speech patterns, manipulative tactics, the types of people that are typically targeted by criminals, and perhaps even demographics would all have to be observed and considered before an artificial intelligence can formulate a true and accurate determination. It is imperative that an extremely robust and accurate system would have to be in place to ensure that innocent people are not falsely identified as a criminal, generating what are known as false positives.

Moreover, if high resolution cameras and surveillance systems are normally all around cities and establishments, it should be expected for the online security to be of an equivalent standard and caliber. These systems are instrumental in helping law enforcement identify criminals and can even record crimes being committed in real time as evidence. Surveillance systems are current examples of the technology and innovation that have been crucial in adapting to changes in criminal methods online as well as offline. But whereas cameras aid in the detection of crimes in the physical world, this kind of security seems to be missing in online websites and applications. Furthermore, are all these tactics being applied for online services? And, to what degree can artificial intelligence be utilized in the detection of offline and online crime to this date?

Currently, artificial intelligence serving as detection systems have been applied in some countries, in a variety of ways, to reduce crime. Law enforcement has used AI in the surveilling of gun detonations. ShotSpotter gunfire detection system has been implemented in the states of California, Illinois, Florida, Ohio, Louisiana, Indiana, and Connecticut to help determine the origin of gunshots by triangulating the position of the shooters. ShotSpotter identifies the source of the shots using built-in sensors that can hear the sound of the detonation and determine its distance based on how the sound bounced off of nearby buildings. As presented on ShotSpotter's website, the presence of this detection system has helped reduce gun violence significantly in the aforementioned states and has also aided police officers in the capture of many criminals.

Another artificial intelligence-powered detection system is Hikvision. It is similar to regular surveillance cameras found in cities. Hikvision has been running tasks such as face recognition, license plate scanning, and other analytics remotely or in the cloud, but with the power of AI, Hikvision can now run deep neural networks right on the camera's board. To explain what this means, Faggela, an expert on the competitive strategies of artificial intelligence, said about Hikvision:

> By performing the processing within the cameras themselves, they are making the process faster and cheaper. It can also reduce the need for using significant bandwidth since only relevant information needs to be transmitted. Among the successes of Hikvision cites is a 65% drop in crime in Sea Point, South Africa following the introduction of their cameras system. (2019, para.14)

This is yet another artificial intelligence that has had a direct impact on the crime rates of the cities that have integrated AI to their security infrastructure. Other systems using artificial intelligence, such as Predpol and Cloud Walk, use previous criminal data to determine and predict where crimes usually happen and at what times. This is an example of the machine learning and neural network processes that take place within artificial intelligence which help maximize the efficiency of these systems.

On a similar front, artificial intelligence has been applied to the legal system inside courts in Durham, in the United Kingdoms. Before this, judges had to determine, in a short amount of time, if a criminal should be allowed back into

society or not, including the amount of money to set their bail at. Now this process is delegated to artificial intelligence. The Harm Assessment Risk Tool (HART), an AI with five years input of case data on criminal proceedings, can now determine an individual's risk level based on said data. On the success of this artificial intelligence, Faggela said:

> The city has been testing the system since 2013 and comparing it's estimates to real world results. The city claims Hart's predictions that an individual would be low risk were accurate 98 percent of the time, and predictions that an individual would be high risk were accurate 88 percent. (2019, para.26)

This is a significant improvement upon other systems found in the United States such as COMPAS, which generates risk assessments for criminals and has been used for decades. These older systems were proven to contain the racial bias of the police officers providing the data fed into the artificial intelligence, hence altering the integrity of the results.

With the current systems and different applications of artificial intelligence that are currently in use, the detection of crime through an AI has been made a reality soon to be asserted as a stopping force against crime. Artificial intelligence can detect crime much faster than humans and in cooperation with other kinds of artificial intelligence called Intelligent Agents, the effectivity of the detection algorithms for cybercrime could prove even greater. On Intelligent Agents, K. Tatera of *The Science Explorer* explains their use:

> Intelligent Agents are autonomous computer-generated forces that communicate with each other. By cooperating and sharing data, intelligent agents plan and implement appropriate responses in case of unexpected events. Intelligent agent technology is collaborative by nature and able to adapt to the environments in which it is deployed, making it a powerful weapon against cybercrime. (2015, para. 8)

Regardless, this level of detection in a consistently effective form has not yet been fully integrated for online security for users and children. While Purdue University's research on AI has been successful in the detection of online predators and criminals based on what is known about these types of crimes, there is still a need for a more present artificial intelligence system to monitor and accurately prevent crimes committed online. The number of scandals involving sexual predators continues to grow every day, and the platforms on which they take place are more and more public each time as well. This means, that these criminals either aren't afraid of getting caught or they know that there isn't a security entity or strategy that can stop them from carrying out these attacks. Artificial intelligence could change the way security operates on the internet and may become a new normal for the way cybercriminals are brought to justice. However, if this type of AI cybersecurity agent is successful in its implementation, the ensuing trials for cybercriminals and the legal procedures that follow must be assessed.

## CHAPTER 5

## DISCLOSURE OF AI TECHNOLOGIES IN COURT

The key for the successful, future implementation of a strong artificial intelligence for the detection and prevention of online crime is the assurance that the legal steps involved in regular court proceedings are also maintained by the artificial intelligence. It goes without saying that people accused of crime have constitutional and human rights, and for an artificial intelligence to detect criminals based on previous data or any other element, it must be very aware of the laws that exist to protect the privacy of each individual, criminal or not. Therefore, in the event that a criminal is apprehended with the help of an artificial intelligence, an expert must be able to explain the methods and processes undertaken for the capture of said criminal.

Explaining an artificial intelligence and the processes within its algorithm that leads to the capture of a criminal might prove a bit challenging, even for an expert. For example, the expert must be able to show – beyond a shadow of a doubt – that the chain of custody for evidence collection was maintained and that every digital forensic procedure and law has been carried out infallibly. Could this exposure and disclosure of the technology in court endanger the effectiveness of the artificial intelligence in future scenarios, due to the possibility that criminals would then be made aware of the exact data that is collected to identify them? Do they legally have a right to know?

### 5.1 The Case of Apple vs. FBI

In 2016, the FBI entered a legal battle with Apple after the FBI retrieved a phone from one of the men responsible for the San Bernardino Shooting. This dispute stemmed from Apple's refusal to create a special operating system for the FBI to allow them to bypass the functionality that erases all of the iPhone's data after 10 failed password attempts. The FBI argued that they required the help of Apple and that without them they would not be able to access the shooter's device. Apple's reason for refusing to aid the government is because not only would it have undermined the security of their devices, but it would also have set a precedent for future cases involving technology for the government to force technology companies to comply in government investigations. However, the case was soon dismissed because the FBI found a third-party tool that gained them access to the device's information.

Additionally, *Apple v. FBI* gained popularity because of the apparent controversy involved and this helped bring new issues regarding technology to light. Rianna Pfefferkorn wrote an article for the Center for Internet and Society at Stanford Law School that pinpointed some outstanding details of the *Apple vs. FBI* case:

> The Sixth Amendment guarantees criminal defendants the right to a fair trial, and per *Brady v. Maryland*, the Fourteenth Amendment's Due Process Clause requires the prosecution in a criminal case to turn over all exculpatory evidence to the defendant. That means that when criminal investigators use technological techniques to surveil a suspect and gather

digital evidence against him, they should have to disclose the technique to him in the prosecution. (2018)

This disclosure of the technology tools within the process to the criminals that it helped catch doesn't happen as often as the law would like. However, compared to several years ago judges are becoming more and more aware of the workings of technology, so now they know what details to ask for in cases. Regardless, Pfefferkorn (2019) also stated that during a case where the government managed to arrest a wanted sexual predator, when asked to reveal the methods used to capture the sex offender the government opted for dropping the case against the criminal rather than reveal and expose their technology's inner workings. This is where intellectual property laws clash with the laws for the prosecuting of criminals.

The case of *Apple v. FBI* and the laws related to intellectual property bring an essential aspect that cannot be overlooked for the future of artificial intelligence, digital forensics, and other security strategies for the detection of online crime. This aspect is the proprietary nature of intellectual properties. The digital forensic procedures for the collection and preservation of evidence are in place for this exact reason; to ensure that the methods that make the evidence admissible in a court of law are upheld by the forensics personnel, up to the moment the evidence is presented in front of a judge. The defining factor for the success of forensic, technological tools and actions utilized to prevent cybercrime and to bring criminals

such as sexual predators to justice is that they must find common ground within the judicial system in their integration into the current legal landscape.

### 5.2 The Case of State vs. Eric Loomis

If technology companies continue to choose to uphold the secrecy of their methods rather than to enlighten the courts on how their products did not cut any legal corners, then it could be argued that they are effectively denying people their due process. In 2013, the wheelman of a drive-by shooting, Eric Loomis, was brought to trial in the State of Wisconsin. This trail gained interest because an artificial intelligence, COMPAS, was used to assess the risk Mr. Loomis had of committing another crime if he were to be released, which the AI determined to be high. Edwards (2017) in an article on Loomis' case stated that:

> The Wisconsin Supreme Court ruled against Mr. Loomis holding he would have gotten the same sentence using the usual factors. However, the Court did seem to express concern about the use of a secret algorithm to sentence an individual to prison. (para. 2)

Eric Loomis was sentenced to six years in prison, based on the information the artificial intelligence had on him and its previously input case data.

Furthermore, Mr. Loomis' case had some important elements involved. The first is that neither the report generated by the artificial intelligence nor the information used to determine the results of the report were shown to Mr. Loomis because the private company who owns COMPAS claimed those were trade secrets. On this element, in an article for *The Globe and the Mail*, David Butt (2017) affirms:

> The court that sentenced Mr. Loomis used a commercial risk-assessment tool. So the algorithm at its heart was proprietary: meaning it was secret. As the Wisconsin Supreme Court observed, "The proprietary nature of [the tool] has been invoked to prevent disclosure of information relating to how factors are weighed or how risk scores are to be determined." (para. 7)

This is the part of a trial where a forensic expert goes through the evidence gathered and explains the processes taken to collect said evidence. And then to present beyond a shadow of a doubt that the facts and truth of the case implicate the defendant, which leaves some room for the defendant to challenge the findings.

The second point of interest is that, after further inspection it was determined that the initial data that was put into the AI's algorithm was based on police reports that contained the racial bias of those police officers. This, in turn, compromised the integrity and impartialness of the artificial intelligence's assessment. However, this could not be perceived at the time that the sentenced was passed, because the company who owned COMPAS invoked the proprietary nature of the artificial intelligence.

In an article written for *phys.org* by Georgia State University on the topic of using AI to convict criminals, district attorney Vic Reynolds declared:

> "We're talking about an area of law where there is very little precedent," Reynolds said. "If we commit to a system where AI is being used to help formulate a criminal sentence, we do in fact have an ethical obligation to

share the foundation of that system with the very people whose lives are affected." (2018, para. 10)

Based on these statements it can be understood that cases such as this one, serve as an example of the compromise that must be made when introducing AI into the legal system; which is, to make law-oriented AI inherently transparent.

Lastly, Eric Loomis could not challenge or argue with the artificial intelligence that assessed his recidivism risk percentage because of the implicit secrecy of the intellectual property. It is standard for private companies to protect their investments in their software and property by refusing to disclose their trade secrets, but when these creations are putting people behind bars, the justice system has an indisputable expectation of transparency and due process. On the question of whether this means that AI and the judicial system are at an impasse, Butt (2017) declared:

> No. We can pursue the revolutionary potential of AI to enhance justice processes without undermining essential justice safeguards. Justice is a core public service and in economic terms, a public good. It is not just another playground for profit-maximizing economic activity. Therefore, it is incumbent on the public, not private, sector to fund and develop AI tools to enhance justice processes. Since the public sector has no business need to keep commercial secrets, the inner working of those AI tools can be disclosed, and thus fully and independently challenged in court. The result will be more comprehensible and thus more acceptable AI-aided verdicts. (para.12)

Indeed, giving the court an artificial intelligence whose inner workings they can analyze and understand will result in a more just and forthright trial. This is even more effective by combining this kind of AI with the appropriate human interaction and guidance, because there are some things AI is not currently suited for more than experienced humans. This is not to say that artificial intelligence is infallible, but moving past the battle between protecting intellectual properties and providing a fair trial is the first step in fully setting AI up to be an indispensable forensic instrument for preventing crime and protecting adults and minors online.

# CHAPTER 6

# METHODOLOGY AND RESULTS

This chapter will present and describe the research methodology used for exploring the viability of utilizing a software tool to determine the age of a person who has written a given text. This research experiment complements the technologies of current applications in the detection of online crime and suspicious activities mentioned in Chapter 4. The subsequent results of the research methodology will also be described in this chapter.

## 6.1 Research Approach

The research approach taken stemmed from the research questions and topics explored in previous chapters. Of these topics, the matter of detection was chosen as the focal point, specifically the detection of age differences and distinctions between a child and an adult. In a research paper titled *Aggression and Anxiety in Rapists and Child Molesters*, the authors of the article, Mally Shechory and Sarah Ben-David (2005", p.653), on the differences between child molesters and rapists stated, "child molesters had more emotional disturbances, low levels of self-esteem, a lack of self-confidence, a lack of emotional maturity, and high levels of emotional pressure and anxiety." The authors also found that child molesters and sex offenders generally lack social skills when compared to rapists. Hence, it could be inferred that child molesters are more likely to behave in a manner that would not be considered normal, adult behavior, perhaps even to the point of behaving as a child would behave when attempting to engage in social interactions.

Based on these findings the methodology approach in this section was undertaken assuming that the average pedophile will express themselves utilizing a lower level of writing, similar to that of a child's, rather than the level of writing that would normally come from an average functioning adult. Therefore, the Flesch-Kincaid Method was investigated. The Flesch-Kincaid method is a process used to measure the readability and reading difficulty of any given text, and is used by newspapers and the military to determine the varying grade levels in which their articles and manuals are written. The actual formula utilized in this method is defined as:

$$0.39 \times (\text{words/sentences}) + 11.8 \times (\text{syllables/words}) - 15.59 \quad (1)$$

This equation considers the number of words used divided by the number of sentences written in the text in the first term, and in the second term, the number of syllables is divided by the number of words used in the text. The resulting number is the Flesch-Kincaid grade level index, which is then used to determine the grade level and age of the person for whom the text is written for, and perhaps it can be hypothesized that it would return an age close to that of the person who wrote it, as well.

### 6.2 Method and Results

A readability tool which utilizes the Flesch-Kincaid grade level assessment, created and hosted by *WebFX.com,* was used. The test by direct input option was selected for testing, but the tool also allows for a URL's to be entered if the text is found on a web page. This readability tool considers many other grade level indexes and models along with Flesch-Kincaid. But the focus of this methodology

will be on the Flesch-Kincaid only while also providing the results of the other models for information and comparative purposes. For the first test, we entered the input text “I play Fortnite.”, and the tool’s result returned as “Your text has an average grade level of about 3. It should be easily understood by 8 to 9 year olds.” This means that the text can be read by an eight or nine-year-old, which currently is about the average age of the child gamer (see Figure 6). This age is clearly considered very young, and the inherent lack of experience in online games and social interactions could be a factor in the selection process of sexual predators.

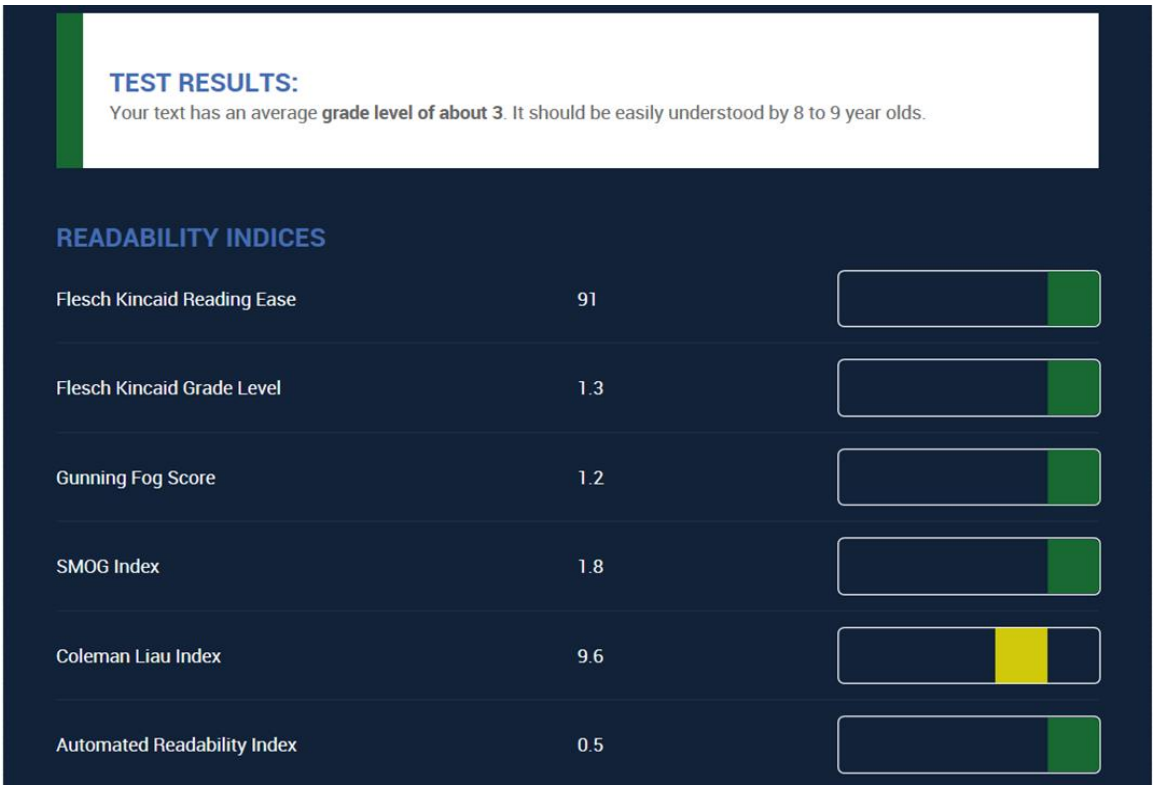



Figure 6. First Test Readability Tool Results

Once this first test was made, actual text from a child solicitor was the next logical step to be input into the readability tool. The input data used in this next test was taken from an affidavit made for an arrest warrant against a now convicted forty-year-old sex offender, named Anthony Gene Thomas. This sex offender

initially contacted his victim through the video game Fortnite which, as mentioned in previous chapters, is a common grooming ground for predators. The affidavit against Mr. Thomas contained evidence in the form of messages exchanged between the victim and Mr. Thomas, which were used as input for the readability tool test.

The second test was made using a message from the seventeen-year-old minor to Mr. Thomas. The victim's message placed into the tool reads "I'm going to tell my mom who got me the new phone and who you are, (My boyfriend) And tell her a bit about you but I'm going to make it straight forward until I'm 18 and then I'll tell her." The results for this text came back as "Your text has an average grade level of about 10. It should be easily understood by 15 to 16 year olds." The results indicate a very close age to that of the person who wrote it – in this case, the seventeen-year-old – and, therefore, it could be inferred that the readability tool could possibly work both ways; it can determine the age of the intended reader as well as the age of the person who wrote the text. So far, in the investigation, this tool seems to be a viable method for future automation, given the accurate approximation of the test results (see Figure 7). However, more tests will be made to ascertain this.


Figure 7. Second Test Readability Tool Results

A text message written by Anthony Thomas was used as the third test of the readability tool with the purpose of determining if a higher age would be returned in the results. The third test was conducted using the following text written by Mr. Thomas: “I pick you up from work and you can go home and shower and get clothes if you want and I’ll bring you back here, and I’ll take you on a date, but if you f*** me, I’m truly done speaking with you, and that’s on my father’s grave (you’re gonna decide if I’m worth gambling or not).” The results presented by the readability tool this time around was “Your text has an average grade level of about 16. It should be easily understood by 21 to 22 year olds.” (see Figure 8).


Figure 8. Third Test Readability Tool Results

The result for the third test of the readability tool showed that this time Mr. Thomas' text message was understood and intended for an older age than the age result from the second test; the minor's text. These results indicate that a kind of text analysis can be applied to text in order to determine an individual's approximate grade level and age which, if paired with a strong artificial intelligence, could possibly bridge the gap for security and detection within chat rooms or other environments where this type of technology can be applied to. An artificial intelligence built for the detection and monitoring of online interactions between individuals could help flag suspicious behavior and raise attention when needed, to stop criminals from hurting more children through the use of online games or other forms of social media. Finally, to further illustrate the results of this readability tool, six readability tools were used to conduct further tests on multiple scenarios.

The resulting age given by Web FX's tool will be included in each test to provide a deeper analysis for the results. The categories for the tests that were conducted and will be displayed are the following:

- News Media
- Fortnite Case
- Undercover Cop Case

The readability tools are:

- Web FX's Readability Tool (webfx.com)
- Readability Formula's Readability Tool (readabilityformulas.com)
- Online Utility's Readability Tool (online-utility.org)
- Datayze's Readability Tool (datayze.com)
- Prepostseo's Readability Tool (prepostseo.com)
- Nivo Media's Readability Tool (nivo-media.nl)

Each tool calculates the Flesch-Kincaid grade assessment and reading ease index. Three tests were conducted with the same three aforementioned sentences initially ran on the WebFx readability tool with the exception of the first sentence, which was edited to "I play Fortnite when I come back from school." And while all the tools utilize the same Flesch-Kincaid model to analyze the sentences, the results varied in some of the tools. Once the tests had concluded, the results were entered into an SQL database, then Visual Basic was used to query the data and create a dataset from the tools' results. The program consisted of a combobox containing the different results for the tests conducted and a button to generate a crystal report of the results. The database table column structure is: the name of

the tool being used to analyze the text, the input sentence or text that is being used as the input data, the Flesch-Kincaid grade level, and, lastly, the Flesch-Kincaid Reading Ease Index. Crystal Reports were then utilized in the Visual Basic program to display a report of the data results in the form of graphs according to the test number. The tests are labeled from one to three, respective to the sentences presented previously and such is the order of the charts of the results, an age approximation using Web FX's tool is provided for each of the tests as well. The following figures illustrate the Visual Basic program, as well as the results. These sentences used as input for the previous three that were conducted will be shown again, but this time the difference is that the six readability tools were used to output the results of the input text. This yielded five additional sets of data for the Flesch-Kincaid grade level and reading ease indexes to be displayed with Crystal Reports via the Visual Basic program (see Figures 9 and 10).

```vb
Imports System.Data.SqlClient

Public Class F1

    Private Sub F1_Load(sender As Object, e As EventArgs) Handles MyBase.Load


        CB1.Items.Add("Test 1")
        CB1.Items.Add("Test 2")
        CB1.Items.Add("Test 3")



    End Sub

    Private Sub BT1_Click(sender As Object, e As EventArgs) Handles BT1.Click

        If SELECTION = "Test 1" Then
            GENREPORT(1)
        End If

        If SELECTION = "Test 2" Then
            GENREPORT(2)
        End If

        If SELECTION = "Test 3" Then
            GENREPORT(3)
        End If
    End Sub



    Private Sub CB1_SelectionChangeCommitted(sender As Object, e As EventArgs) Handles CB1.SelectionChangeCommitted

        SELECTION = CB1.SelectedItem
    End Sub
End Class
```

Figure 9. Visual Basic Form 1 Code (Combobox and Button)

```vb
    Cursor.Current = Cursors.WaitCursor

    ds = New DataSet
    Conncs = New SqlConnection("data source = DESKTOP-04ME567;DATABASE = Read_Results; Integrated Security=SSPI")

    Try
        Select Case testnum
            Case 1
                strQuery = "Select TOOL_NAME, SENTENCE, FLESCH_GRADE_LEVEL, FLESCH_READING_INDEX FROM Tool_Res1"

            Case 2
                strQuery = "Select TOOL_NAME, SENTENCE, FLESCH_GRADE_LEVEL, FLESCH_READING_INDEX FROM Tool_Res2"

            Case 3
                strQuery = "Select TOOL_NAME, SENTENCE, FLESCH_GRADE_LEVEL, FLESCH_READING_INDEX FROM Tool_Res3"

        End Select


        ' CONNECTION FOR POPULATING COMBOBOX1.
        Conncs.Open()

        command = New SqlCommand(strQuery, Conncs)
        adp = New SqlDataAdapter(command)
        adp.Fill(ds)

        ' GENERATE THE CRYSTAL REPORT.
        Dim rptdoc As ReportDocument
        rptdoc = New CrystalReport1
        rptdoc.SetDataSource(ds.Tables(0))
        rptdoc.SetParameterValue("testnumber", testnum)

        F2.CRV1.ReportSource = rptdoc
        F2.ShowDialog()
        Cursor.Current = Cursors.Default

    Catch ex As Exception
        MsgBox(ex.ToString)

    Finally
        ' DISPOSE OF FORM2 AND ADAPTER.
```

Figure 10. Visual Basic Crystal Report Generation Function Code

The first category of tests is News Media. The six readability tools will be used to analyze text extracted from multiple news media outlet's articles to determine the approximate Flesch-Kincaid grade level and reading ease that they are written in. These two values correspond to the academic grade level at which the text is written at the second value reflects how easy it is to read the text; the higher, the easier. The order of the results for the news outlets will be in the following order: Fox News, The New York Times and The Washington Post. As will be the case with all of the readability tests to be conducted, an age approximation required to comprehend the text will be included for each one of the test results. These tests will serve as examples for comparison for the effectiveness and accuracy of the tools, to determine if these tools can be automated as they are currently, or if they are not reliable enough to be used as a security measure by an automated system. Figures 11 through 16 show the text that was used as input for the six readability tools as well as the resulting bar graphs for the grade level and reading ease indexes.

As seen from these findings, all three news media outlets' test results establish that they wrote at an age and grade level that can easily be understood by teenagers. For Fox News' text written by Casiano (2019), the readability tool from Web FX placed the text at a tenth grade level, and a required reader with an age of around 16. The averages for the grade level and reading ease were 7.74 and 65.80, respectively. For the second text, from an article for The New York Times written by Lipton & Turkewitz (2019), the readability tool's results show that they wrote at a high school senior level, with an estimated required age of 18. The

averages for these tests were 12.70 for grade level and 42.63. For the third text written by The Washington Post's Hanna-Attisha (2019), the result placed their text at a grade level of 9 and an age of 15. The resulting averages for grade level and reading ease respectively were 10.82 and 50.72. It is important to note that the articles chosen for these tests from all three news media were based on serious matters, which could explain the high grade levels seen in the results.

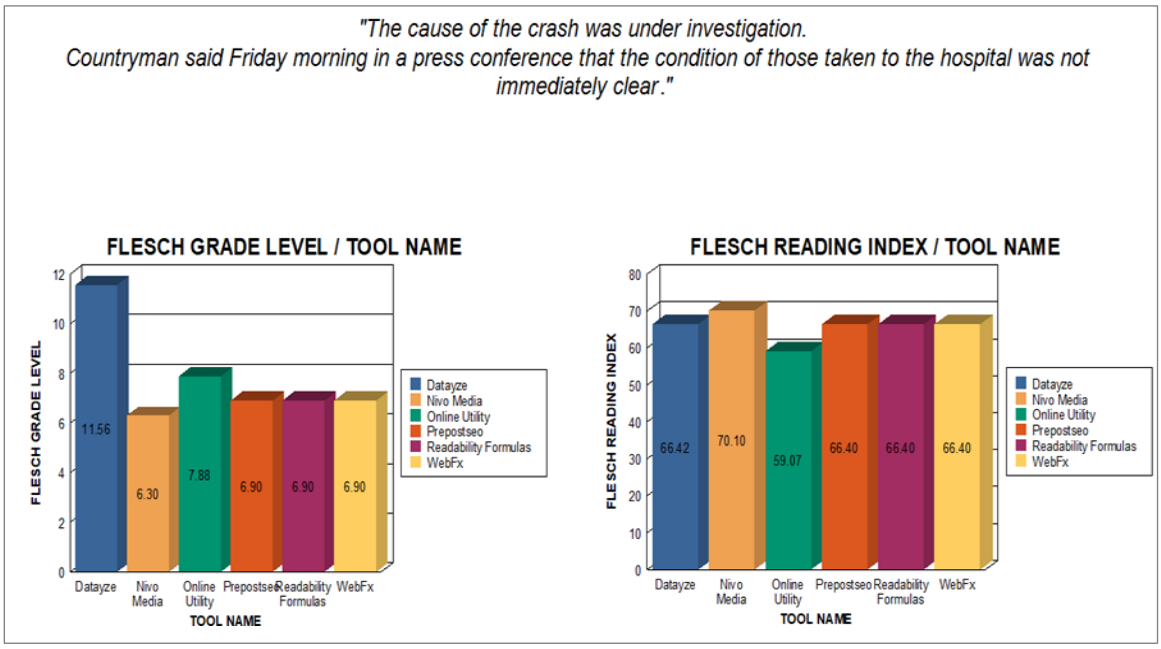


Figure 11. (a, b) Fox News Readability Test – Grade Level and Reading Index

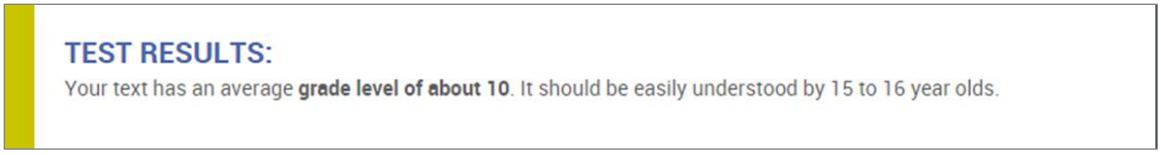


Figure 12. Fox News – Approximate Age

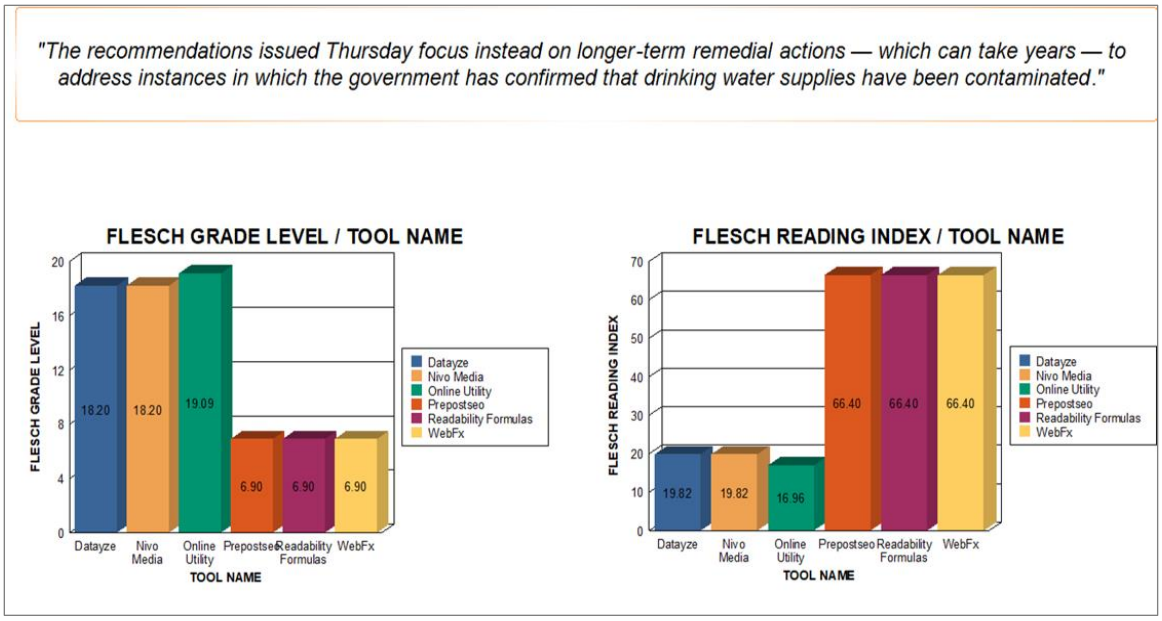



Figure 13. (a, b) The New York Times Readability Test – Grade Level and Reading Index

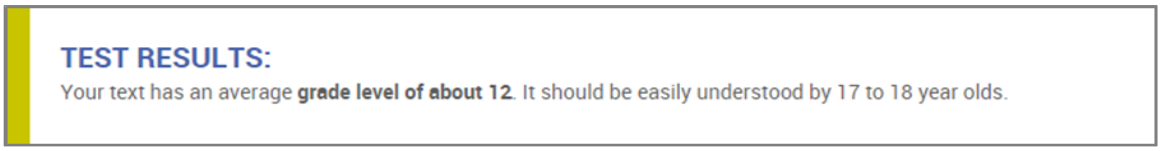



Figure 14. The New York Times – Approximate Age

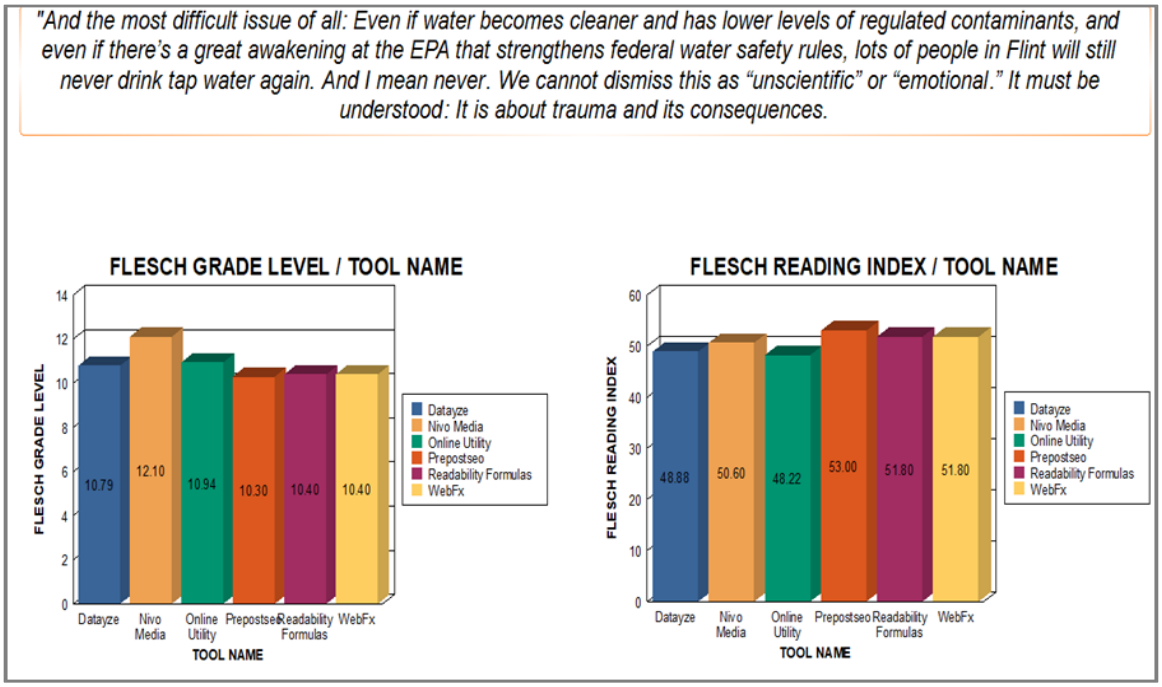



Figure 15. (a, b) The Washington Post Readability Test – Grade Level and Reading Index

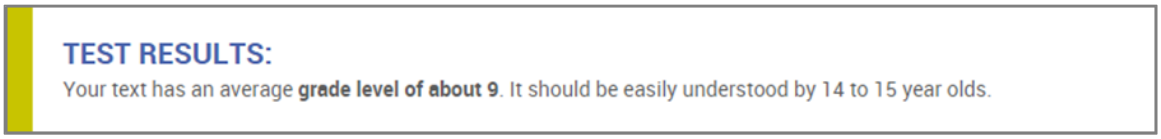



Figure 16. The Washington Post – Approximate Age

The next readability tests involve Fortnite and the case of Anthony Gene Thomas using texts extracted from Mr. Thomas' arrest affidavit, originally presented in chapter two. The results for these tests showed a favorable outcome. In test 2, the tools successfully approximated the grade level and age of the victim who was seventeen. The third test -which belongs to the criminal– resulted in an age that was older than that of the victim, which is true in real life. However, it did not reach an accurate estimate of the predator's age which was actually forty-two. This shows the shortcomings that would be faced if this kind of tools were to be made automatic with the use of artificial intelligence; the accuracy of the results is not yet optimized for the effective detection of criminals in terms of age. Steps would have to be made toward obtaining foolproof and accurate demographics of the persons interacting on a given platform to avoid false positives results using inaccurate data. The tools used in this section currently do not take any other input to be processed aside from the texts entered. An AI using natural language processing and text analysis similar to these readability tool's internal processes would need much more data to make educated decisions when flagging individuals for suspicious behavior. Figures 17 through 22 show the results for the second case, the Fortnite case involving Mr. Thomas.

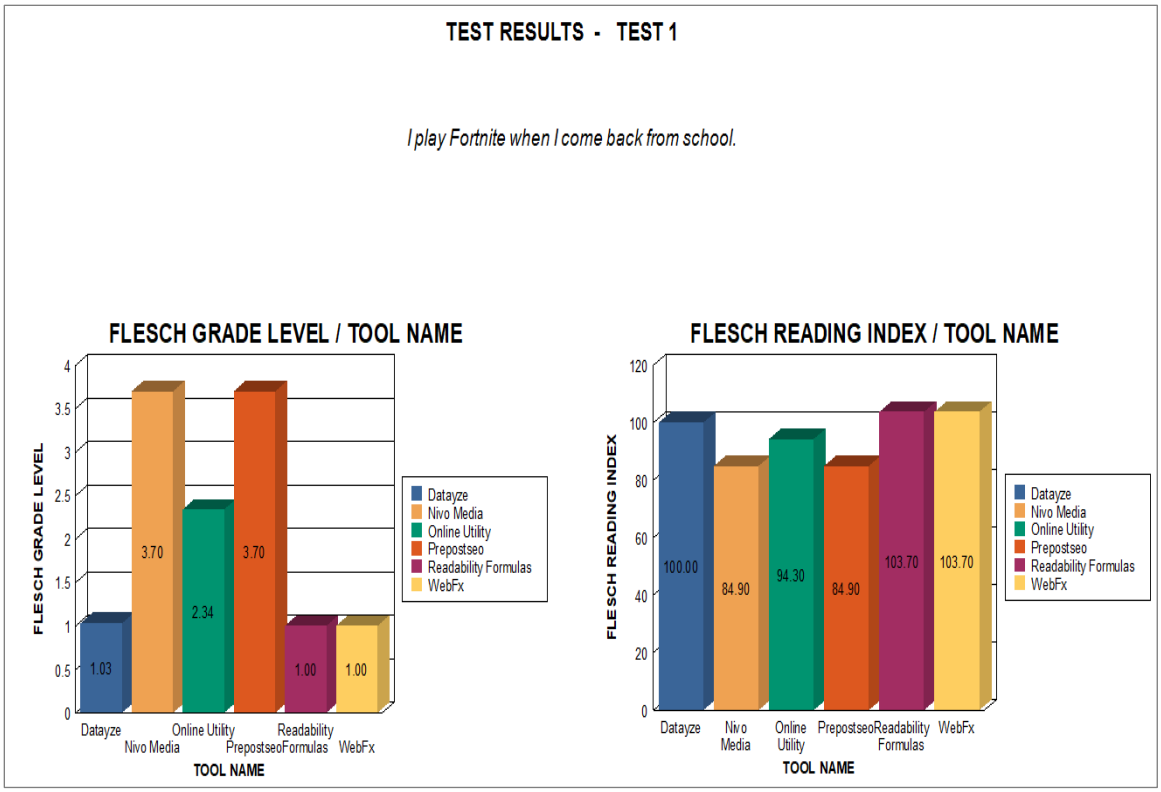



Figure 17. (a, b) Fortnite Test 1 Results - Third Grader Phrase Grade Level and Reading Index


Figure 18. Fortnite Test 1 – Approximate Age

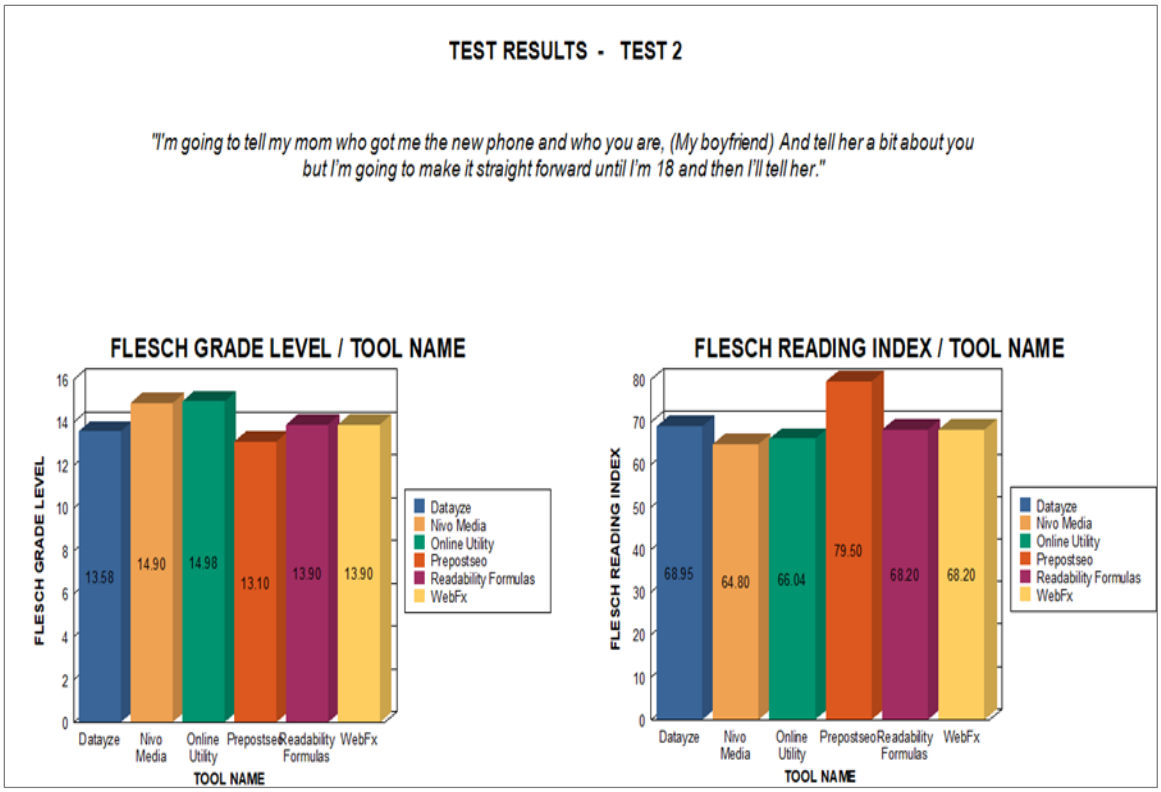



Figure 19. (a, b) Fortnite Test 2 Results – Victim's Text Grade Level and Reading Index

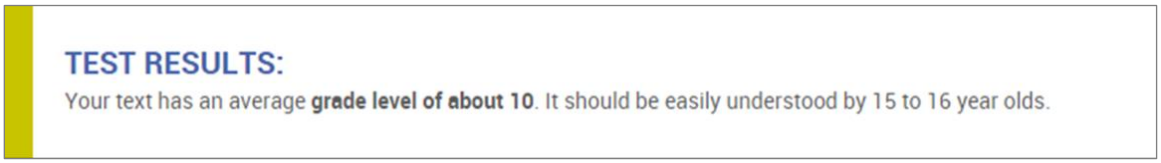



Figure 20. Fortnite Test 2 – Approximate Age

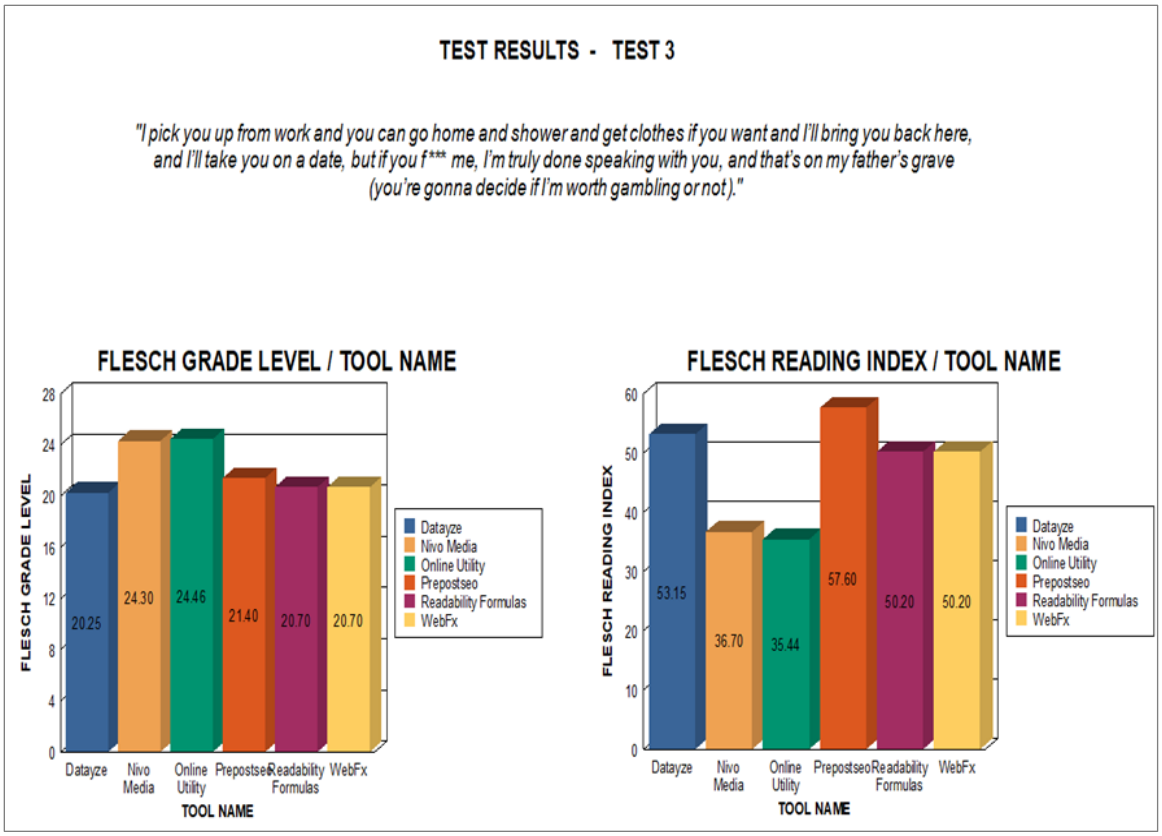



Figure 21. (a, b) Fortnite Test 3 Results – Mr. Thomas Text Grade Level and Reading Index

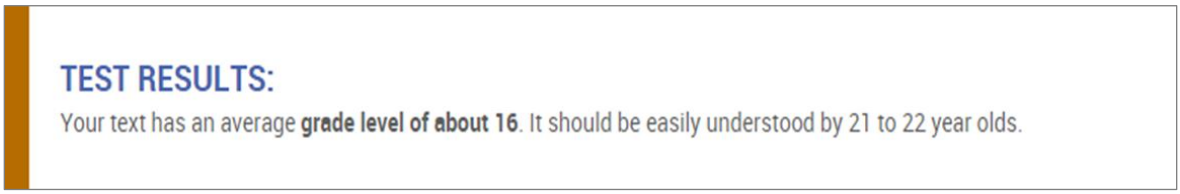



Figure 22. Fortnite Test 3 – Approximate Age

Various tests were conducted with these tools, but one of the most curious cases came from a case covered on *Vanity Fair* by Mark Bowden (2009), where an undercover detective successfully captured a sexual predator. This detective managed to trick the criminal into meeting in person, where law enforcement officials were readily waiting for his arrival. Several tests were ran using texts from their actual conversation. The results showed that the detective managed to consistently speak like someone in the third grade. On the other hand, the criminal

spoke a sixth grade level. The important finding in this experiment is that it proves this tool could be tricked. If this tool were to be automated as is, criminals would be able to exploit it and fool it. Unsupervised learning could be the key in developing a tool that can better understand human language and thought process to refine the output of the texts that would be processed. Figures 23 through 28 show the resulting bar graphs for this encounter (the first two sentences are from the detective). The results are displayed in the same manner as they have up to this point, but it is in this test that the findings begin to vary. The most important thing to note in the test's results is that the detective's text was perceived by the readability tools as having been written by a third grader, between the ages of eight to nine.

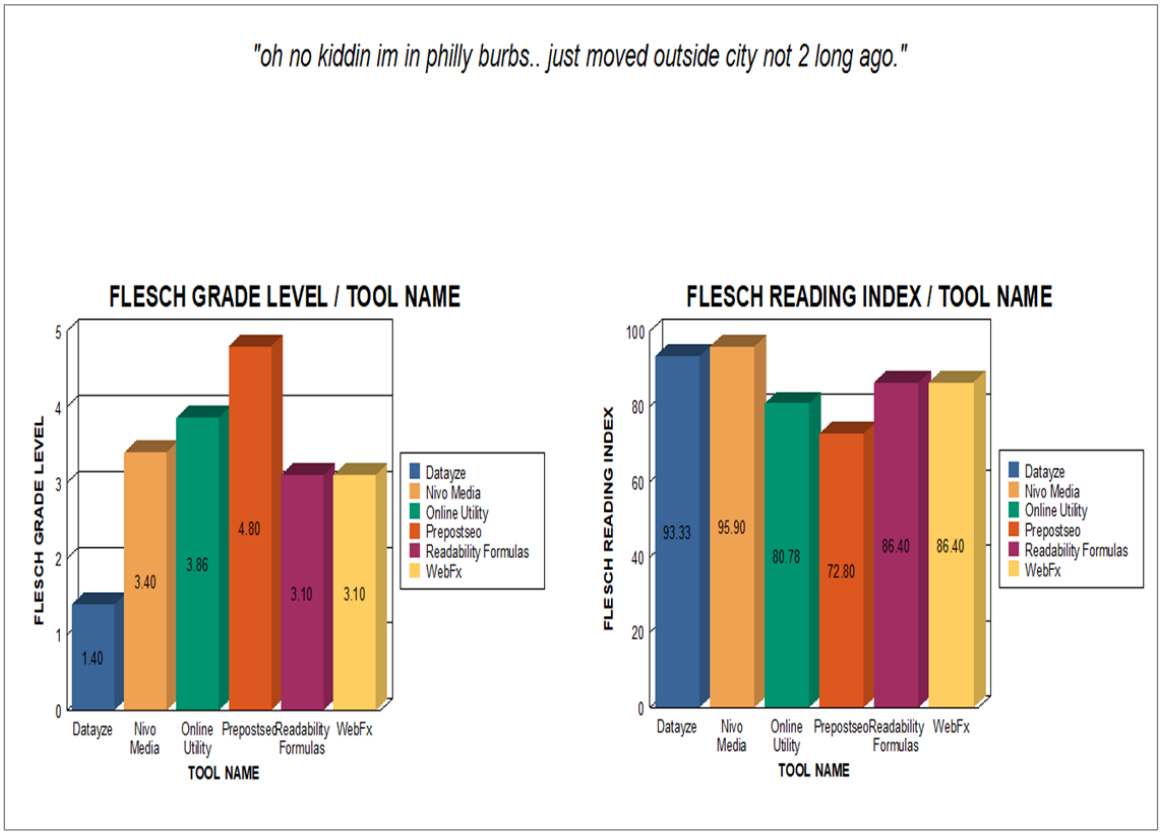



Figure 23. (a, b) Undercover Detective Test 1 Result – Detective Text 1 Grade Level and Reading Index

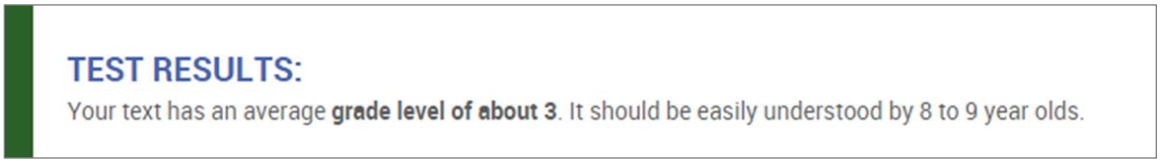



Figure 24. Undercover Detective Text 1 – Approximate Age

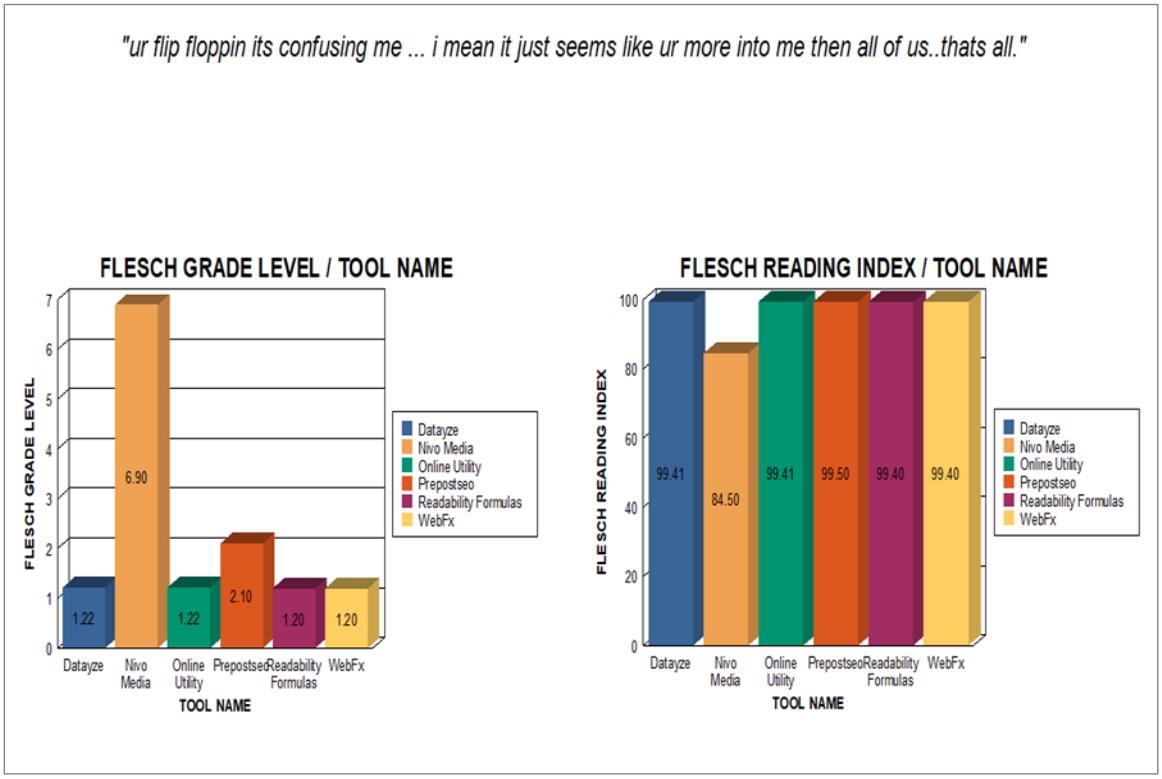



Figure 25. (a, b) Undercover Detective Test 2 Result – Detective Text 2 Grade Level and Reading Index


Figure 26. Undercover Detective Text 2 – Approximate Age

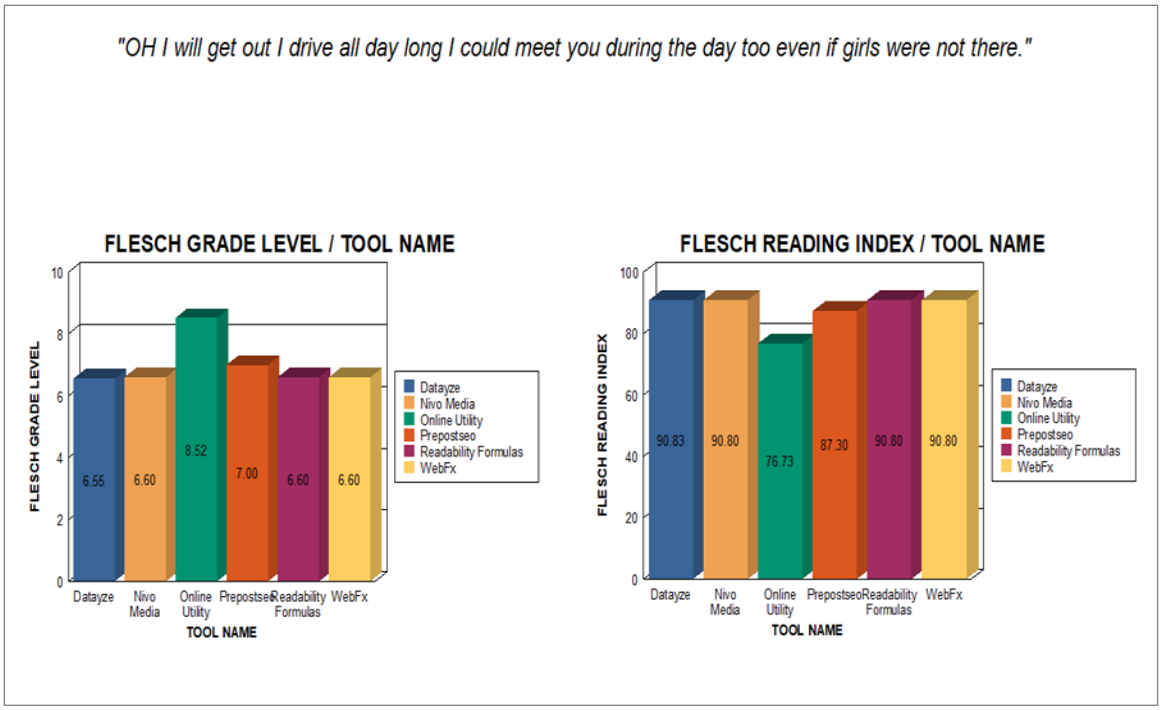



Figure 27. (a, b) Undercover Detective Test 3 Result – Sexual Predator Text Grade Level and Reading Index

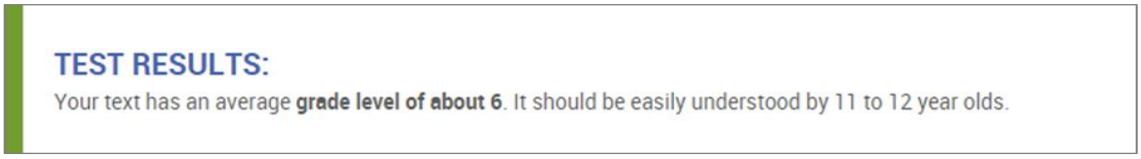



Figure 28. Undercover Detective Sexual Predator Text 1 - Approximate Age

After all of these tests concluded, the average for all previously shown test results were calculated with the purpose of arriving at an approximate, aggregated grade level and reading index for these results. For the first result set in the Fortnite case's tests, the average for the grade level index and reading ease index were 2.13 and 95.25 respectively with an approximate age of 9. The second test yielded the averages of 14.06 for the grade level and 69.28 for the reading ease index with an approximate age of 16. The final test conducted for the Fortnite case returned the averages of 21.97 and 47.22, for grade level and reading ease respectively, with an estimated age of 22. The results show that these tools can provide a

possible, useful approximation for the age of the reader and perhaps the writer as well, while also demonstrating their shortcomings because it can be seen how the tools can be fooled, if wanted. In fact, one test in particular showed that the readability tools don't handle single, more "complex" words at all (see Figure 29). To successfully implement such an approach to an artificial intelligence in the future, an aggregate of the results in the form of averages, could possibly yield firmer, more accurate results to partake in the machine learning process of the automated detection tool.


Figure 29. Test Age Result for the Word "Unprecedented"

Finally, the test results for the aforementioned case of the undercover detective who was investigating a sexual predator also serve to demonstrate the previous statement. In this case, the undercover detective consistently comes through as a nine-year-old, while the sexual predator's age returns as approximately twelve-years-old. This further accentuates the issue with this tool as an automated detection system. The averages for the first test results of this case returned as 3.28 for the grade level index and 85.94 for the reading ease index. The second test's resulting averages were 2.31 and 96.94 for grade level and reading ease, respectively. The final test, which now analyzing the sexual predator's text, returned as 6.98 for the grade level index and 87.88 for the average reading ease index. These results showcase the way that this tool is not as accurate as wanted for the case of future implementation. And also shows that a

combination of machine learning and real-time text analysis, could be refined into an automated detection system with the integration of key, unfalsifiable demographic information on the individuals before they are flagged by the artificial intelligence serving as a detection system.

# CHAPTER 7

## CONCLUSION AND FUTURE WORK

Digital forensics and cybersecurity strategies are being implemented to protect users online. However, this thesis attempts to shed light on areas where cybersecurity strategies have not been a sufficiently effective force in protecting children and adults from criminals over the internet. The thesis' topic was chosen as a response to recent news regarding sexual predators using the popular video game, Fortnite to contact and solicit minors. The child predators would initiate contact with children through Fortnite and talk with the children until the predator was ready to establish contact in the physical world. This event occurred during the height of Fortnite's popularity in 2018, when many media outlets were reporting numerous instances of similar incidents regarding sexual predators using the game's text and voice chat features to groom minors, as described in section 2.2.2. Moreover, there is a present need for means of protecting children in video games and other platforms.

The YouTube scandal mentioned in chapter 4 is only the latest of the incidents that have continued to surface at the time of this writing. In section 1.2 it was shown how most social media networks already have policies in place that specifically prohibit the use of their services if the user is a sexual offender, yet this clearly is not stopping criminals from using their applications, regardless of the established terms and conditions. A possible reason for this lack of policy enforcement could stem from lack of an effective detection system for these types of users. The YouTube team has since then been doubling down on the

surveillance and detection of criminal behavior. However, at the time of this writing the implemented detection system has mostly been limited to the video content that users upload on to their website, so the comments section of the videos could still be exploited again in a similar fashion to the child abuse scandal in the future.

Fortunately, during the development of this work it was found that researchers, such as the Purdue University professors mentioned in section 1.2 and 4.1, are taking the necessary investigative steps into exploring artificial intelligence as a detection tool for these sexual predators. Strong AI are currently being developed and are hopefully on their way to becoming effective deterrents against cybercrimes and child predators, as well as providing new means of enhancing the online experiences of users throughout the internet. Two additional points, mentioned in chapter two and chapter five, include evidentiary and court-related procedures that should be kept in mind when implementing new technologies such as artificial intelligence. There are constitutional rights that must not be violated, such as the Fourth Amendment, as well as a need for open systems that can be examined by the people of the court if new sophisticated technologies become key factors in bringing individuals to justice.

In chapter six the goal was to determine if there are ways in which a system or tool could determine variables to differentiate people based on their online interactions, in this case using text. A detection system, to be implemented as a means for capturing criminals, would have to use other factors to single that individual out from the rest of the users without any visual cues. In the case of online interaction, speaking with other users is mostly done through the means of

text or voice chat. Perhaps artificial intelligence could be applied to monitor websites that utilize webcam video, in future research. For the tests conducted in chapter six, readability tools hosted by sites such as WebFX.com were utilized to see if the tool's algorithm – which employed the Flesch-Kincaid reading ease and grade level indexes– could determine the age differences and approximate academic grade levels between a sexual predator and a minor, using predators' written texts as the tool's input. Future research could be done in this area for monitoring the voice chat features within different social and interactive platforms with the use of the combined benefits of strong artificial intelligence and NLP techniques.

The resulting outputs demonstrated that a difference in age and grade could be inferred based on the texts that were analyzed. They also showed that these tools are not foolproof and that there is still much work to do for the future of online security. During one of the tests, we entered three different texts, beginning with something a child would write, then text written by the victim of a convicted offender, and then the sex offender's text. The results revealed a similar age and grade level to the persons who initially wrote the texts. For example, the first test returned an age range of eight or nine, the second of fifteen to sixteen, and the third and final test returned an age range of twenty-one to twenty-two. However, there is a certain margin of error in this particular test method that must be mentioned because the Flesch-Kincaid does not necessarily reflect the age of the person who wrote the input text, but rather an approximate. There is still a need for reliability in the results. However, it could be said that an older, more educated

individual will express themselves in more sophisticated words than the average minor would. This could be used to establish suspicion if an artificial intelligence were to utilize a similar algorithm for the detection of these differences, while also observing for signs common to sexual predators and deviants. A future detection tool should look at demographics or personal details that simply cannot be falsified. These details could include special sexual or suggestive keywords for the artificial intelligence to use to raise flags, or even a way to look at linked credit card information that hold the account user's real name and age, for example.

This thesis' main purpose was to raise awareness for the situations mentioned throughout the chapters which are happening at the time of its writing all over the internet. Many of the events that were presented occurred very recently, and these events show a present need that merits and requires the attention of authorities and cybersecurity teams. The tools utilized and explored in chapter six are presented as a proof of concept for future implementation. There is a need for artificial intelligence to utilize this type of analysis inside chatrooms and other interactive platforms to provide security. For example, through the use of a flag and boot system where an individual that raises a certain number of flags in simply removed from the service due to breaking the policy and guidelines of a given platform. This could be fairly similar to an intrusion detection system that sends an alert when a breach is detected. As we have seen, there are gaps that need to be filled and work to be done before we reach this ideal security solution in the near future. An artificial intelligence using machine learning and text analysis will indubitably be more capable of analyzing large volumes of chat texts than any

number of humans working together can manage, and at exponentially faster speeds as well and therein lies the reason to consider this alternative as the approach to establishing this security measure.

In closing, an actual problem with the online world is essentially that every day more children are using the internet without the necessary education or supervision, and this exposes them to people who would abuse of their inherent social inexperience. While the problem does extend to teenagers and adults as well, the issue still is that there isn't enough being done to prevent this population from harm. No detection, only remediation once the damage has been done. That is why the implementation of an automated detection system, run by an intelligent and accurate artificial intelligence that could read through all the text in a chat at speeds not achievable by humans regardless of manpower, could be the key to flagging these individuals' actions and to intercept them with enough time to prevent said actions from harming others. This research's purpose is to help shed light upon different areas of improvement for online security, while also presenting a proof of concept utilizing technologies that are available today. This in the hopes that in the near future a robust and effective tool will be automatized and implemented to provide a safer environment for users of all ages.

## BIBLIOGRAPHY


Alexander, J. (2019, February 21). YouTube Terminates More Than 400 Channels Following Child Exploitation Controversy. *The Verge*. Retrieved from https://www.theverge.com/2019/2/21/18234494/youtube-child-exploitation-channel-termination-comments-philip-defranco-creators.

American Psychological Association. (2010). *Publication Manual of the American Psychological Association*. Washington, D.C. American Psychological Association, 6th Edition.

Automatic Readability Checker, A Free Readability Formula Consensus Calculator. (2019). Readability Formulas. Retrieved from http://www.readabilityformulas.com/free-readability-formula-tests.php.

Bowden, M. (2009, November 3). Was a Chat-Room Conversation a Twisted Game of Seduction or Signs of Child Predation? *Vanity Fair.* Retrieved from https://www.vanityfair.com/news/2009/12/sexual-predators-200912.

Butt, D. (2017, June 1). Should Artificial Intelligence Play A Role in Criminal Justice? *The Globe and Mail.* Retrieved from https://www.theglobeandmail.com/opinion/should-artificial-intelligence-play-a-role-in-criminal-justice/article35167201/.

Calhoun, J. (2018). News 13 Investigates: Internet Predators Using Online Games to Lure Children. *WBTW News13* Retrieved from https://www.wbtw.com/news/grand-strand/news-13-investigates-internet-predators-using-online-games-to-lure-children/1595270454.

Casiano, L. (2019, April 26). Multiple People Dead in Fiery Crash on Colorado Freeway. *Fox News*. Retrieved from https://www.foxnews.com/us/multiple-people-dead-in-fiery-crash-on-colorado-freeway.

Circuit Court of the Eighteenth Judicial Circuit Brevard County Florida (2018) Affidavit to Arrest Thomas, Anthony Gene. Retrieved from https://media.local10.com/document_dev/2019/01/17/Anthony%20Gene%20Thomas_Redacted_17630093_ver1.0.pdf.

Coatney, M. (2017). The Coming AI Revolution in Digital Forensics. [Blog post] Retrieved from https://accessdata.com/blog/the-coming-ai-revolution-in-digital-forensics.

Cornell Law School. (2010, February 5). Fourth Amendment. LII / Legal Information Institute. Retrieved from https://www.law.cornell.edu/constitution/fourth_amendment.

Easttom, C. (2014). *CCFP Certified Cyber Forensics Professional All-in-One Exam Guide.* New York, NY: McGraw Hill Professional.

Edwards, W. (2017, May 11). The Courtroom and Artificial Intelligence in Judicial Decision Making. Retrieved from http://columbusdefenselawyer.attorney/criminal-lawyer-columbus/2017/05/ai-in-the-courtroom/.

Faggella, D. (2019). AI for Crime Prevention and Detection – 5 Current Applications. Emerj Artificial Intelligence Research. Retrieved from https://emerj.com/ai-sector-overviews/ai-crime-prevention-5-current-applications/.

Georgia State University. (2018) Artificial Intelligence Gets Its Day in Court. *Phys.org*. Retrieved from https://phys.org/news/2018-03-artificial-intelligence-day-court.html.

Hanna-Attisha, M. (2019, April 25). Is Water in Flint Safe to Drink? It's Not Just a Question of Chemistry. *The Washington Post.* Retrieved from https://www.washingtonpost.com/opinions/is-water-in-flint-safe-to-drink-its-not-just-a-question-of-chemistry/2019/04/25/01f6ffe2-66a6-11e9-8985-4cf30147bdca_story.html?utm_term=.6919f1bf3eb2.

Harper, J. (2019, February 22). Modernizing Natural Language Processing with Deep Neural Networks. *A.I. Business*. Retrieved from https://aibusiness.com/natural-language-processing-deep-neural-network/

Home - ShotSpotter. (n.d.). ShotSpotter. Retrieved from https://www.shotspotter.com/.

Instagram, Inc. (n.d.). Instagram Terms of Use. Retrieved from https://help.instagram.com/478745558852511/.

Lipton, E., & Turkewitz, J. (2019, April 26). E.P.A. Proposes Weaker Standards on Chemicals Contaminating Drinking Water. *The New York Times*. Retrieved from https://www.nytimes.com/2019/04/25/us/epa-chemical-standards-water.html.

Marr, B. (2017, March 16). Supervised V Unsupervised Machine Learning -- What's the Difference? *Forbes.* Retrieved from https://www.forbes.com/sites/bernardmarr/2017/03/16/supervised-v-unsupervised-machine-learning-whats-the-difference/#56467882485d.

Miller, A. (2018, September 24). Predicting A Predator: Purdue AI Tool Identifies Online Deviants Before They Act. *Purdue.edu*. Retrieved from https://www.purdue.edu/newsroom/releases/2018/Q3/predicting-a-predator-purdue-ai-tool-identifies-online-deviants-before-they-act.html.

Nath, D. (2018). Fox on Tech: Predators Using Online Games, FBI Warns. Fox News. Retrieved from https://www.foxnews.com/tech/fox-on-tech-predators-using-online-games-fbi-warns.

National Center for Missing & Exploited Children. (2019) Media Key Facts. Retrieved from http://www.missingkids.com/footer/media/keyfacts.

NBC. (2018). Naked Intruder in 13-Year-Old Girl's Bedroom Found Home Through Her Social Media Posts, Police Say. *WPTZ*. Retrieved from https://www.mynbc5.com/article/naked-intruder-in-13-year-old-girls-bedroom-found-home-through-her-social-media-posts-police-say/22997339.

Neal, D. (2019, January 17). Man Arrested on Child Pornography Charges Met Victim through Fortnite, AG Moody Says. *The Miami Herald.* Retrieved from https://www.miamiherald.com/news/local/crime/article224709015.html.

Nivo Media. (n.d.). Free Online Readability Tool | Nivo-Media. Retrieved from https://www.nivo-media.nl/readability-tool/.

Pfefferkorn, R. (2018, April 18). The Dark Side of the “Apple vs. FBI” OIG Report. The Center for Internet and Society at Stanford Law School. Retrieved from http://cyberlaw.stanford.edu/blog/2018/04/dark-side-“apple-vs-fbi”-oig-report.

Pilcher, G. (2018, January 18). Supervised Vs. Unsupervised Machine Learning. *Elder Research*. Retrieved from https://www.elderresearch.com/blog/supervised-unsupervised-machine-learning.

Readability Analyzer. (2019) Datayze. Retrieved from https://datayze.com/readability-analyzer.php.

Readability Checker - Flesch Kincaid Grade Level Readability Test. (2019, February 23). Prepostseo. Retrieved from https://www.prepostseo.com/readability-checker.

Readable | Free Readability Test Tool. (n.d.). WebFX. Retrieved April 3, 2019, from https://www.webfx.com/tools/read-able/.

Robinson, R. (2018). Online Predators Are Using ‘Fortnite’ to Prey on Kids. Retrieved from https://www.fatherly.com/news/online-predators-using-fortnite-prey-kids/.

Rouse, M. (2014, May 1). What is Computer Forensic (Cyber Forensic)? - Definition from WhatIs.com. Retrieved from https://searchsecurity.techtarget.com/definition/computer-forensics.

SAS Institute. (2019). Natural Language Processing: What It Is and Why It Matters. Retrieved from https://www.sas.com/en_us/insights/analytics/what-is-natural-language-processing-nlp.html.

Shechory, M., & Ben-David, S. (2005). Aggression and Anxiety in Rapists and Child Molesters. *International Journal of Offender Therapy and Comparative Criminology*, 49(6), 652-661. DOI: 10.1177/0306624X05277943. Retrieved from https://pdfs.semanticscholar.org/d99a/d3c0b857d8954097d216220689efda947d64.pdf.

Siewert, P. (2015, January 22). Case Study: Commonwealth V. Emanuele. Professional Digital Forensic Consulting, LLC. Retrieved from http://prodigital4n6.blogspot.com/2015/01/case-study-commonwealth-v-emanuele.html

Sraders, A. (2019, January 3). What Is Artificial Intelligence? Examples and News In 2019. *TheStreet.* Retrieved from https://www.thestreet.com/technology/what-is-artificial-intelligence-14822076.

Tatera, K. (2015, September 2). Using Artificial Intelligence to Take Down Cyber Criminals. *The Science Explorer*. Retrieved from http://thescienceexplorer.com/technology/using-artificial-intelligence-take-down-cyber-criminals.

TechHelpline (2018, January 30). What You Post Online Could Put You at Risk. Here Are 4 Ways to Stay Safe. Retrieved from https://www.techhelpline.com/geotagging-four-ways-stay-safe/.

Techopedia. (n.d.) Digital Forensics: Definition - What does Digital Forensics mean? Retrieved from https://www.techopedia.com/definition/27805/digital-forensics.

Tests Document Readability. Online-Utility. (n.d.). Retrieved April 23, 2019, from https://www.online-utility.org/english/readability_test_and_improve.jsp.

The Canadian Press - Global News. (2018, November 8). Police Investigate Sexual Extortion Case Involving Game 'Fortnite'. Retrieved from https://globalnews.ca/news/4644088/police-investigate-sexual-extortion-case-involving-game-fortnite/.

The Fortnite Team (n.d.). Fortnite Battle Royale: Code of Conduct. Epic Games. Retrieved from https://www.epicgames.com/fortnite/en-US/news/fortnite-battle-royale-code-of-conduct.

The Telegraph News. (2018). Fortnite Game Craze Is Putting Children at Risk from Online Pedophiles, NCA Warns. Retrieved from https://www.telegraph.co.uk/news/2018/04/05/fortnite-game-craze-putting-children-risk-online-paedophiles/.

Turvey, B. (2017, May 15). *What Is Criminal Profiling and Why It Is Important | Twisted Minds - A Website About Serial Killers*. Retrieved February 28, 2019, from http://twistedminds.creativescapism.com/psychological-disorders/profiling/.

University of Chicago. (1993). *The Chicago Manual of Style: The Essential Guide for Writers, Editors and Publishers*. Chicago: University of Chicago Press, 14th Edition

USLegal. (n.d.). Cybercrimes Law and Legal Definition. Retrieved February 26, 2019, from https://definitions.uslegal.com/c/cybercrimes/.

WebFX. (n.d.) Free Flesch-Kincaid Readability Test Tool - Readable. Retrieved from https://www.webfx.com/tools/read-able/flesch-kincaid.html.

WePC. (2018) Video Game Industry Statistics, Trends & Data - The Ultimate List. Retrieved from https://www.wepc.com/news/video-game-statistics/.