Crime and Technology

Hacking with regard to Julian Assange and Wikileaks

Agathe Benichou, Étienne Cossart and Mirjan Neza

Professor Dahl

Due: May 5th 2016

CS200: Computers and Society

Table of Contents

Introduction (Agathe)

Computing technology and the Internet provide the opportunity for people to better themselves and their society. These technologies give people access to a vast amount of information anywhere around the world and gives them the opportunity to educate themselves. However, these technologies also serve as platforms for a wide range of crime such as fraud, theft, forgery, espionage and various other forms of scams. Crimes committed through computing technology, also known as cyber crimes, are generally more destructive and undetectable compared to crimes without computing technology. A very common type of cybercrime is hacking, which ranges from petty pranks to the shutting down of services on which people heavily depend on. A hacker can cause serious damage to one’s life or a government's reputation.

Julian Assange is one of the world's most notorious hackers who founded the company Wikileaks which has been responsible for publishing very secretive and controversial material to the public. As a result, governments have had to adapt, develop and pass laws that specifically addressed hacking. There is a broad spectrum of different political, social and ethical opinions regarding hacking and the effect of Wikileaks.

What is Hacking? (Agathe)

Hacking refers to the practice of modifying or gaining unauthorized access to a computer, a network or information to fulfill an objective that is not in the realm of the creator's original goal. Companies and governments expend time, money and resources in an effort to prevent hacking and the serious damage it can cause. Regardless of one's intention, hacking is a form of trespass. Hackers are able to identify some sort of weakness or flaw in computer systems and exploit it to gain access. Modern computer systems are so complex that there is bound to be a flaw embedded somewhere in the software or hardware. Hackers are commonly experts in all things computers who have a strong sense of curiosity, plenty of time and pride themselves in their skills. Hackers have the ability to breach computer systems, intentionally release computer viruses, crash websites, steal money, destroy files, disrupt businesses and steal sensitive personal, business and governmental information. Hackers can trick a computer user into installing a program which gives them access to the machine. The less a computer is secured, the more likely it is that hackers can access it. Some hackers are lured into hacking by the thrill of getting past security barriers. There are websites and blogs dedicated to the art of hacking where hackers brag about their more recent conquests. Hackers do not always have malicious or destructive intent, some hack to release information that they think will improve the world we live in. Julian Assange is one such hacker whose website, Wikileaks, seeks to "improve transparency which creates a better society for all people.(Wikileaks)" Assange believes in the free movement of information who was inspired by Daniel Ellsberg's 1971 release of the Pentagon Papers to create his own outlet for "uncensored and untraceable mass document leaking and public analysis.(Assange)"

Wikileaks is a not-for-profit organization that was created in 2006 and accepts anonymous submissions of secret or controversial material. Submitted material becomes published on their website to be able to get the raw truth out to the public. Wikileaks provides an anonymous electronic dropbox which provides their sources with a secure way to leak information. Wikileaks believes in the defense of freedom of speech and media publishing and that its efforts could lead to reduced corruption, stronger institutions such as governments and large corporations.(Wikileaks) Rather than competing with other media for information, Wikileaks works with media outlets and publishing organizations around the world to be able to reach the most people as possible. (The Guardian) Wikileaks has been responsible for a myriad of information leaking related to various organizations, governments, political figures and other personalities.

Types of Hacking (Mirjan)

Hacking is often pictured as some computer wiz attempting to get past a security system. However, hacking has developed and changed with society to become a very broad term. The meaning continues to change as computers continue to decrease in size yet increase in prevalence and dependence. There are many actions that can classify as hacking, each with different motives and reasons. One of the biggest types of hacking is criminal hacking which is usually motivated by some short term financial gain. Some of the most common types of criminal hacking include identify theft and credit card fraud.

Before computers became so integrated into our everyday lives, criminals would attempt to find discarded credit card receipts, bank statements, tax notices, or other legal documentation in hopes of gaining enough personal information to use the victim's identity in malicious ways.

With modern day use of computer systems, identify theft criminals can make thousands of attempts at obtaining personal information in very little time such as phishing and public network hacking. Phishing is the practice of sending mass fraudulent emails and it is a popular way that many hackers attempt to retrieve information from unsuspecting victims. These emails are made to look very real and are able to fool many people without close examination. Public network hacking is common in large cities where free WiFi is offered by stores, restaurants and public areas such as parks. Hackers wait around in these public areas and attempt to intercept network traffic to find personal information. With the popularity of coffee shop wifi, hackers are given a myriad of opportunities to attempt to steal one's information. (Baase)

Another type of hacking is political hacking, often referred to as hacktivism, is often performed by government agencies. Even though governments and governments officials are supposed to be examples of moral and law abiding subjects, they are no exceptions to hacking. Controversial financial, political or security information on other governments or certain individuals is enough motivation for governments to hack for their own benefit. Often times, this hacktivism involves countries that are in conflict with one another. However, there is a lack in solid proof of this since governments tend to deny any affiliation with the hacks. A recent example of political hacking involves Russian hackers attempting to influence the 2016 U.S. presidential election. In fact, the CIA concluded that Russia intervened covertly during the presidential election to promote Donald Trump's presidency. The CIA discovered that it was Russian security agents who hacked into the Democratic National Committee as well as Hillary

Clinton's campaign to obtain and release selected Democratic documents to Wikileaks in an effort to undermine Clinton's candidacy. (The Washington Post)

One last type of hacking is hacking as a form of revenge. Hacking as a form of revenge is often done in retaliation to another event, and has been done in the past by individuals as well as governments. Recently, Wikileaks founder Julian Assange released additional internal information on Scientology after a group of Scientology members threatened to press legal action against him for initially leaking Scientology documents. Hackers are known for revenge attacks against former companies or governments, especially those who have openly criticized their former organization.(New York Times)

Be that as it may, hacking does not always have to be malicious. White-hat hacking is regarded as a type of ethical hacking. These hackers are computer expects that use their skillsets to find potential opportunities for malicious hackers, known as black-hat hackers, to enter compute systems. White-hat hackers do this to help companies, governments or individuals strengthen their security systems. (Baase)

History of Hacking and Wikileaks (Etienne)

At the start of computers in the mid 20th Century, a hacker was a term for a programmer who wrote intricate code, and it wasn't until the 1970's that hacking took on the negative connotation it has today. As computers became increasingly popular, so did hacking and abusing the technology. In the 1980's, floppy disks were used to spread viruses and steal information (231-236, Gift of Fire). Several high profile cases occurred during this time such as a German programmer hacking into the U.S. military's computer network to obtain and sell information to the Russians, and a team of programmers from several countries stealing $400,000 from Citicorp and fraudulently transferred $11 million to offshore bank accounts (231-236, Gift of Fire). In 1988, the notorious Internet Worm, written by a college student, traversed the internet and jammed up thousands of computers and caused social disruption. By the mid 1990's, the Internet became more popular and interconnected which lead to more dangerous hacking lead by cyber gangs and criminals (231-236, Gift of Fire). Some of these hackers just wanted to prove a point and the U.S. Department of Justice website was once hacked to say “Department of Injustice” (231-236, Gift of Fire). In 1999 and 2000, the Melissa virus and the “Love Bug” virus wreak havoc on the internet, destroying files, modifying computer operating systems, and collected information (231-236, Gift of Fire). The viruses infected large organizations such as Ford, Siemens, the Pentagon, the State Department, and the vast majority of federal agencies, causing an estimated $10 billion in damages (231-236, Gift of Fire). Other viruses such as Code Red, Zotob, Sasser, and MyDoom also caused hundreds of billions of dollars in damages (231-236, Gift of Fire). In the 2000’s, a 15-year old Canadian caused an estimated $1.7 billion in damages to the U.S. government (231-236, Gift of Fire). In the mid-2000s, an international group sent over $20 billion spam messages in 2 weeks to more hundred of thousands of across over one hundred countries, asking the receiver of the message to give credit card info (231-236, Gift of Fire). New York City lost over $800,000 because of hackers stealing it from the subway fares. Hackers broke into an online gambling website and changed it so that everyone won, and the site lost over $1.9 million (231-236, Gift of Fire). In 2011, “Sony sued George Hotz for showing how to run unauthorized applications on a PlayStation 3, a hacker group launched a denial a denial-of-service attack on Sony and accessed names, birthdates, and credit card information of millions of Sony’s gaming system” (231-236, Gift of Fire).

Wikileaks is one of the world's most successful hacker run websites which has created a safe-haven for whistleblowers. According to Wikileaks website, “Wikileaks will accept restricted or censored material of political, ethical, diplomatic or historical significance. We do not accept rumor, opinion, other kinds of first hand accounts or material that is publicly available elsewhere" (Wikileaks: A Brief History, Columbia.edu). The founder of Wikileaks, Julian Assange was born in 1971 in Australia who taught himself all things related to computers and hacking (Everything You Need to Know About Wikileaks, Molly Sauter, Jonathan Zittrain). He registered the domain name Wikileaks.org in 1999 and began actively using it to release controversial information in 2006 (Wikileaks: A Brief History, Columbia.edu). Assange refers to Wikileaks as a "uncensorable system for untraceable mass document leaking and public analysis." According to *Wikileaks: A Brief History* by Columbia University, the first posting in December 2006 was a decision (never verified) by a Somali rebel leader to execute government officials (Wikileaks: A Brief History, Columbia.edu). In 2007, Wikileaks and The Guardian worked together to publicize the "the private investigations firm Kroll about the alleged corruption of former Kenyan President Daniel Arap Moi". In 2010, Assange wanted to increase public knowledge of his findings so Wikileaks released a 2007 video of two US Apache helicopter pilots allegedly executing people on the ground in Iraq, including two Reuters correspondents (Wikileaks: A Brief History, Columbia.edu). The helicopter video got attention, but much of it focused on Assange's clumsy packaging and editing of the material, which he dubbed "Collateral Murder"(Wikileaks: A Brief History, Columbia.edu). This got immense media attention and became a national debate of whether Julian Assange and Wikileaks are treasonous for the leak or if they are heros for making the information public (Everything You Need to Know About Wikileaks, Molly Sauter, Jonathan Zittrain). From 2011 to 2015, Wikileaks published thousands of documents on many issues including prison files of Guantanamo Bay, the Syrian conflict, the Afghanistan War Logs, the Trans-Pacific Partnership deals, and files showing that the NSA spied on the French government (Wikileaks: A Brief History, Columbia.edu). In 2016, Wikileaks released internal emails of the Democratic National Convention (DNC) uncovering how the Democratic Party altered the course of the election by wrongfully supporting Hillary Clinton rather than remaining neutral the party should do (Wikileaks: A Brief History, Columbia.edu). This caused a media frenzy and the Chair of the DNC, Wasserman Schultz promptly resigned (Everything You Need to Know About Wikileaks, Molly Sauter, Jonathan Zittrain).

Laws on Hacking (Agathe)

With the frequency of hacking and the wide range of its severity, it is important that proper laws are enforced. In 1984, Congress passed the main federal anti-hacking and cybercrime law: the Computer Fraud and Abuse ACT (CFAA) which made it illegal to access a computer without authorization. There are no national borders to hacking and hackers are often regarded as international criminals. The CFAA is intended to reduce malicious hackers and the hacking of government and other sensitive computer systems. Anyone who is found guilty will be subject to a wide range of penalties from fines to imprisonment. After the 9-11 attacks, the US Patriot Act was implemented which expanded the CFAA and increased penalties and prosecutorial power in fighting cybercrime. It also allows the government to monitor online activity of suspected hackers without a court order. While some hackers deserve serious punishment, others are young and have only committed minor offences. Many young hackers with no previous offense are not jail in an effort to still let them become productive member of society with successful careers.

Julian Assange is a self taught hacker who, at 22, was charged on 31 counts of computer hacking and related crimes. (Columbia University) He pleaded guilty to these charges and as a result of his youth, he received minimal punishment and only had to pay a fine. Assange categories the U.S. government as a "secrecy based, authoritarian conspiracy government" and as a result has released a trove of thousands of secretive military and diplomatic U.S. information. In 2007, Wikileaks posted standard procedures for the Guantanamo Bay, Cuba and as a result of legal action in the US, the site was briefly shut down(Britannica) and in 2010, Wikileaks released footage showing US soldiers shooting dead 18 civilians from a helicopter in Iraq. (BBC) In the wake of these leads, lawmakers in the US pushed for the prosecution of Assange and any journalist who collaborated with Wikileaks. (Britannica) Assange has been under political asylum since 2012 in the Ecuadorian embassy in London. The UK government will not allow Assange safe passage out of the country since the UK is legally obligated to extradite him to Sweden where he can be properly investigated for sexual assault charges there. (BBC)

Consequentialist Policy View (Agathe)

Many U.S. government officials have criticized Wikileaks for leaking classified information, claiming the leaks have harmed national security and compromised international diplomacy. However, as a candidate running in the 2016 Presidential Race, Donald Trump seemed to be a big supporter of Wikileaks. One month before the election, President Trump declared “I love Wikileaks!” at a rally in Northeast Pennsylvania and he also referred to Wikileaks as a “treasure trove” of information (CBS News). He applauded Wikileaks for releasing thousands of emails from the personal email account of Democrat Hillary Clinton and the Democratic National Committee which proved that DNC favored pre selected candidates. In fact, President Trump publicly praised Wikileaks for their leak of Clinton's emails claiming that the Clinton Foundation received $12 million in donations from Morocco's king by tweeting “Huma calls it a "MESS," the rest of us call it CORRUPT! WikiLeaks catches Crooked [Hillary] in the act - again. #Drain The Swamp” (Twitter). After the election and the inauguration, President Trump criticized the DNCs lack of security for letting Assange obtain information (CBS News). However, in 2016, Congressmen Pete King called upon Attorney General Eric Holder and Secretary of State Hillary Clinton to prosecute Julian Assange and claimed that Wikileaks meets the legal criteria of Foreign Terrorist Organization. (Observer) Most recently, news emerged that several senior White House officials were involved in the handling of sensitive intelligence information that showed that Trumps campaign officials were caught up in surveillance of foreign nationals as well as involved with Russia's alleged meddling in the presidential election. Information (NY Post). As a result, President Trump tweeted “The real story turns out to be SURVEILLANCE and LEAKING! Find the leakers.” in April 2017(Twitter). Since then, President Trump and his aides have railed against leakers, threatened to find and prosecute them while being very quiet about Wikileaks’ involvement (Chicago Tribune). Trump has also been angered at the leaked accounts of his phone with the leaders of Russia, Australia and Mexico by Wikileaks(The Hill). President Trump seems to value leaks that attack his competition (Hillary Clinton's opposing party (The Democratic Party) or any individual, group or country that opposes him. However, when it comes to him, his administration or any of his decisions, President Trump does not seem to be a fan of leakers, hackers or Wikileaks. It is interesting to note that thus far in his presidency, President Trump has not yet criticized Julian Assange or Wikileaks. Whether this might be for fear of some sort of revenge attack as Wikileaks has been known to do or because President Trump genuinely respects the work Assange and Wikileaks does, President Trump seems to be avoiding putting the notorious hacker and his company on blast via Twitter. Ultimately, Republican political figures as well as Republican lawmakers generally oppose hackers, leaks and Wikileaks. They view it as a threat to the country, to national security and even to their own privacy concerns. As Wikileaks continues to expand its number of whistleblowers, the amount of information it obtains will continue to grow and as a result, Republicans will most likely maintain their views and build on current anti-hacking laws.

Non-Consequentialist Policy View (Mirjan)

In 2012, the Obama Administration passed the Whistleblower Protection Enhancement Act. This act helped to further strengthen Whistleblower protection laws and gave further protection to whistleblowers. Before the Whistleblower Protection Enhancement Act, federal employees were not eligible for whistleblower protection if they fell in a few categories. The categories that ruled out help from the act were if the individual was not the first person who disclosed the misconduct, told a coworker, told a supervisor, disclosed the consequences, or blew the whistle while carrying out job duties. Under the enhanced act, these no longer disqualify whistleblowers. In addition, this act also gives whistleblowers compensation for wrongful reprisal (Obameter, Politifact.com). Later that year, with Presidential Policy Directive 9, some of these protection based acts were further extended to national security and intelligence employees (Obameter, Politifact.com). In light of Edward Snowden and the NSA scandal, Democrats "denounced [Snowden] as a traitor" and "President Obama and former Secretary of State Hillary Clinton have also been unyielding." Snowden, who left the country and is now believed to be in Russia, deliberately broke the law and should not be "brought home without facing the music," according to Clinton. Whether Snowden will return to the United States is unclear. If he were to return however, he would be charged under 18 U.S.C. 641 - Theft of Government Property, 18 U.S.C. 793(d) - Unauthorized Communication of National Defense Information, and 18 U.S.C. 798(a)(3) - Willful Communication of Classified Communications Information to an Unlawful Person. He would most likely be incarcerated as a result. In response to Wikileaks in 2010, the Obama Administration prohibited all unauthorized federal employees from accessing any publicly available classified documents on Wikileaks and the Justice Department considered prosecuting Julian Assange on grounds of encouraging federal employees of stealing and leaking information (Prosecutors Eye Wikileaks Charges, Wall Street Journal). Though liberal policies air on the side of protecting whistleblowers, in the case of Wikileaks and others such as Snowden, liberal government officials believe these sorts of leaks are harmful to society and a danger to national security. Democrat and Republican views are also split. With recent Wikileaks documents, we have seen that they can change. Hillary Clinton's recent email campaign was subject to leaks, and Republicans softened their hate to come to favor Wikileaks (Daily Dot). Democrats have also come to change their opinion on the matter. The government will eventually come to a conclusion on this issue and come to firm their stance, however right now we are in one of the periods of history in which the laws are not caught up to pace with technology and events such as the Edward Snowden case bring this to light.

Consequentialist Public View (Etienne)

In a poll conducted by the Pew Research Center after the diplomatic cables leak, 75% of Americans who identify as being a Republican believe that Wikileaks release of sensitive information harmed the public interest (Daily Dot). In a similar poll conducted in 2010, 70% of Americans, mostly Republicans, responded that Wikileaks causes more harm than good to society (Marist Institute of Public Opinion). After the release of Collateral Murder and other government files in the late 2000's, much of the conservative electorate believed the Wikileak releases were wrong, un-American, and even treasonous. "Julian Assange was Public Enemy

Number One to many prominent conservative figures…[who] openly called for his execution for what they considered his treasonous ways...when WikiLeaks was blowing the whistle on US war crimes in Afghanistan and Iraq and leaking classified diplomatic cables detailing the embarrassing... and even criminal… deeds of the United States… Assange was celebrated as a champion of transparency by many on the Left. Conservatives were predictably less enthusiastic about the leaks, to say the least" (The Surreal Spectacle of Republicans Embracing Julian Assange and WikiLeaks, Brett Wilkins, DailyKos.com). However, when Wikileaks released the emails of Hillary Clinton and the Democratic National Convention, the conservative mindset shifted. "Hannity on Fox... the arch-conservative lengthy, almost fawning interview with Assange, who the host said has "done a lot of good" by leaking Democratic National Committee emails revealing, among other things, how the DNC was in the tank for Hillary Clinton and how it actively worked to sink Bernie Sanders' insurgent grassroots campaign. Hannity actually thanked his former enemy in a recent interview on his radio show, crediting Assange for allowing us to 'see a glimpse of how corrupt, the nature, the institutions of American government and our political system are'..."America owes you a debt of gratitude for that," gushed Hannity" (The Surreal Spectacle of Republicans Embracing Julian Assange and WikiLeaks, Brett Wilkins, DailyKos.com).

According to The Blaze, a popular conservative media outlet, conservatives should be weary of Wikileaks and Julian Assange even after the leak on Hillary Clinton and the Democratic National Convention. Arguing that though conservatives "enjoyed [the Democrats] discomfort over this, there is a fundamental fairness issue here, which is that private organizations have the right to some sort of privacy. … And to put it out there like this is really wrong; it’s theft. And what [the Conservatives are] doing is sort of incentivizing theft in the future.” (Conservatives Warns Against Celebrating Julian Assange and Wikileaks’ Information “Theft”, TheBlaze). The conservative electorate have an opportunistic view on Wikileaks and Julian Assange. At the core issue of whistleblowing, the conservative electorate views Wikileaks’ information as stolen property and morally wrong and believe that it is dangerous to society for whistleblowing to be permitted. However, when the leaks are against Democrats and any enemy of the conservative base, the general feeling towards Assange and Wikileaks shifts to an approval mindset of the leaks. This leaves the conservative electorate in a moral limbo, where the ends justify the means, but only if the end’s outcome is in their favor.

Conclusion (Agathe)

As computer systems continue to replace humans for services and the information stored on the Web and on computers continues to increase, hackers will continue to find more opportunities for crimes. The growth of dependency on computers for communication, business and fast information retrieval as well as the prevalence of social networks only further provides hackers with more reason to do what they do best. Hackers such as Julian Assange and companies such as Wikileaks will continue to thrive under this environment. As technologies continue to advance, law must expand with them to be able to maintain a productive society. In the end, leaks are inevitable; the mere existence of data presents a risk of a leak.

References

Arthur, Charles. "How Computer Hackers Do What They Do ... and Why." *The Guardian*. Guardian News and Media, 06 June 2011. Web. 15 Apr. 2017.

Baase, Sara, and Timothy Henry. *A Gift of Fire: Social, Legal, and Ethical Issues for Computing Technology*. Boston: Pearson Education, 2018. Print.

Crowley, Stephen. "Trump Today: What to Do about WikiLeaks?" *BostonGlobe.com*. The Boston Globe, 08 Mar. 2017. Web. 15 Apr. 2017.

Ellison, Sarah, and Ki Price. "The Man Who Spilled the Secrets." *The Hive*. Vanity Fair, 30 Jan. 2015. Web. 15 Apr. 2017.

Estepa, Jessica. "How Trump Feels about WikiLeaks: A Timeline." *USA Today*. Gannett Satellite Information Network, 08 Mar. 2017. Web. 15 Apr. 2017.

Hancock, Jake. "Conservative Warns Against Celebrating Julian Assange and Wikileaks' Information 'Theft'." *The Blaze*. N.p., 16 Sept. 2016. Web. 24 Apr. 2017.

Keyser, Samuel. "Where the Sun Shines, There Hack They." *IHTFP Hack Gallery: Where the Sun Shines, There Hack They*. MIT, July 1996. Web. 15 Apr. 2017.

Khatchadourian, Raffi. "The Information Trafficker." *The New Yorker*. The New Yorker, 28 Oct. 2016. Web. 15 Apr. 2017.

Moore, Mark. "Trump Rants about 'fake News Media,' Calls for Hunt of 'leakers'." *New York Post*. N.p., 02 Apr. 2017. Web. 24 Apr. 2017.

Podgor, Ellen. "Computer Crimes and the USA PATRIOT Act." *American Bar Association*. N.p., n.d. Web. 15 Apr. 2017.

O'Brien, Michael. "Republican Wants WikiLeaks Labeled as Terrorist Group." *TheHill*. N.p., 03 Feb. 2016. Web. 15 Apr. 2017.

O'Rourke, Lindsey A. "The U.S. Tried to Change Other Countries' Governments 72 times during the Cold War." *The Washington Post*. WP Company, 23 Dec. 2016. Web. 24 Apr. 2017.

Ray, Michael. "WikiLeaks." *Encyclopædia Britannica*. Encyclopædia Britannica, Inc., 26 Jan. 2017. Web. 15 Apr. 2017.

Sanger, David E., and Scott Shane. "Russian Hackers Acted to Aid Trump in Election, U.S. Says." *The New York Times*. The New York Times, 09 Dec. 2016. Web. 24 Apr. 2017.

Strickland, Jonathon. "How Hackers Work." *HowStuffWorks*. N.p., 29 Oct. 2007. Web. 15 Apr. 2017.

Watson, Kathryn. "Pompeo Slams WikiLeaks, but He and Trump Tweeted Praise of WikiLeaks during Campaign." *CBS News*. CBS Interactive, 14 Apr. 2017. Web. 24 Apr. 2017.

Williams, Katie Bo. "Republicans Warm up to Assange." *TheHill*. N.p., 18 Oct. 2016. Web. 15 Apr. 2017.

Wilkins, Brett. "The Surreal Spectacle of Republicans Embracing Julian Assange & WikiLeaks." *Daily Kos*. N.p., 5 Jan. 2017. Web. 28 Apr. 2017.

Zittrain, Jonathan. "Everything You Need to Know About Wikileaks." *MIT Technology Review*. MIT Technology Review, 22 Oct. 2012. Web. 15 Apr. 2017.

"Computer Fraud And Abuse Act Reform." *Electronic Frontier Foundation*. N.p., n.d. Web. 15 Apr. 2017.

"Computer Hacking and Identity Theft." *Computer Hacking and Identity Theft | PrivacyMatters.com*. N.p., n.d. Web. 24 Apr. 2017.

"McClatchy-Marist Poll National Survey December 2010." (n.d.): n. pag. *Marist College Institute for Public Opinion*. Marist College. Web. 24 Apr. 2017.

"Profile: Wikileaks Founder Julian Assange." *BBC News*. BBC, 04 Jan. 2017. Web. 15 Apr. 2017.

"What is the Computer Fraud and Abuse Act (CFAA)? "*Techopedia.com*. N.p., n.d. Web. 15 Apr. 2017.

"WikiLeaks Fast Facts." *CNN*. Cable News Network, 10 Apr. 2017. Web. 15 Apr. 2017.

"WikiLeaks: A Brief History." *Columbia University*. N.p., n.d. Web. 15 Apr. 2017.