Cyber-Crime and Anonymous

Written by: John Mitchell Price

Technology is advancing at an alarming rate. Over the course of a couple of generations we have gone from landline telephones to smartphones to even 3D televisions. Technology is rapidly becoming an important part of not only our culture, but also in how we are able to communicate and make an impact on the world. With this fast paced progression of technology, it's hard for laws to keep up and maintain a level of civility and order for its use.

Nowhere is this more of a controversial challenge than in the continual upholding of cyber laws against the ever-present danger of cybercrimes over the internet. I am all for the enforcement of cyber laws as they give the internet a sense of structure and legality against would be cyber outlaws, despite their limited influence over many of the darker places on the web. However, a decent portion of those that commit cybercrimes are more Robin Hood in their approach, which complicates matters. The hacktivist organization Anonymous best exemplifies this dichotomy. Cyber laws themselves aren't perfect, and neither is Anonymous, which is why they complement each other well. This organization's own Operation Payback is an example of how good intentions can meet bad actions. However, they should be worked with and used to hunt down other cybercriminals and menaces instead of being locked away. Organizations like Anonymous should encourage discussion on cyber laws, instead of scorning the organizations as bad.

According to www.definitions.uslegal.com, "Cyber-crimes includes 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." (www.definitions.uslegal.com). Many of these cyber-crimes include DDoS attacks, internet fraud, hacking, child pornography, and illegal media torrenting. DDoS and hacking tend to be the most dynamic and well-known

cyber-crimes today. DDoS (distributed denial of service) is when a website becomes unavailable due to massive traffic towards the website, which results in users not being able to access the site. DDoS events are coordinated attacks by a group, which is why it's the favorited method of hacktivist and troll groups. Hacktivists are individuals who use the internet and their hacking skills as a form of political and social protest. They can cause serious damage to websites, which allows them to be hacked and manipulated by the attackers. From a legal perspective, "The Computer Fraud and Abuse Act (CFAA) is the applicable law (18 U.S.C. §1030). For a person to violate the CFAA, he has to intentionally cause damages to a computer system part of interstate or foreign commerce." (Kostadinov).

In order to understand the motivations of Anonymous we must first understand its culture. The organization originated in one of the most controversial websites on the internet: 4chan. 4chan was created by American internet coder and entrepreneur Christopher Poole and it was launched on October 1, 2003. The site was originally set up to discuss cartoons and pop culture forums similar in organization and activity to those found in Japanese forums. Its design was straightforward: users posted images and comments across 50 themed boards. There was no registration, account info or login required, meaning the vast majority of posts fell under a default username: Anonymous. Over the course of several years it grew steadily in popularity and in size. "Between 2009 and 2011, 4chan grew from 5 million monthly unique visitors to 10 million. It now collects 22.5 million each month" (Alfonso). Over the years, the site caused several controversies and incidents. These events caused many, even within the government, to try to control or even eliminate the site. Incidents like piracy, trolling of individuals and companies, child pornography, and black market deals gave the site an infamous and chaotic

aura. However, during the course of the last two years, Poole (otherwise called by his username moot) and the site's moderators have cracked down on the illegal content.

Anonymous originated from the various boards within this website. The name of the group came from the anonymous accounts and avatars that came from the early posters. Everyone who posted on the site were labeled with random numbers, thus making them anonymous. Today they are considered anarchists, but try to act on behalf of the middle and lower classes and to fight against tyranny. There is no true leader of the group, only several older members, but the organization works as a community and makes their own decisions individually.

The group opposes internet censorship and control, and the majority of their actions target governments, organizations, and corporations that they accuse of censorship. They believe in the secrecy of its members and have shown a zeal for this belief. They firmly believe that anyone can make a difference, but to do so requires secrecy and anonymity. They also target corporations and governments that fight illegal online piracy websites as well as those who abuse and ignore basic human rights. They aim to use the power of media and online communications to make a difference in the world and to force world leaders realize that the common people still have power.

They first garnered public attention in 2008 for their self-titled mission "Project Chanology" which was intended to expel Scientology's influence from the internet due to its illegal actives of private data mining, indentured member servitude, and abuse of its tax exempt status. This movement was a major success and put the organization onto the world stage, and it has since become an iconic part of the internet as well as a voice for activism everywhere. This group was also responsible for the spread of the Occupy Wall Street Movement, hacking the

Westboro Baptist Church's website, and numerous other cyber-attacks on fascist countries such as North Korea and Libya under Muammar Gaddafi.

The one operation that propelled Anonymous into darker, more controversial territory was Operation Payback. On December 7th, 2010, Anonymous led several successful DDoS assaults that ended up bringing down the main MasterCard, Visa, and PayPal websites. "PayPal, which was also targeted -- but not cited in the indictment -- has said it suffered losses of $5.6 million as a result." (Schwartz). The reason for the attacks was that these companies had ended all financial transactions with WikiLeaks. Anonymous and 4chan were both major supporters of WikiLeaks and they held its creator, Julian Assange, in very high regard. Julian's firm belief in knowledge for the public resonated deeply with both organizations. Rumor was that they ended business due to pressure from U.S Government. They did not stop there as several other companies started getting attacked, organizations like Amazon, several U.S government sites and even several cyber-security firms. The results of these attacks ended up with thirteen members being arrested and tried. It also came up with more discussion on cyber-crime and cyber-warfare. Is Anonymous actually a front for criminals? This was the thought that many had after these attacks.

Cyber-Crime Laws exist to make sure that the security, privacy, and integrity of internet users remain intact. One of the benefits is that they penalize offenders of child pornography and cyber-sex laws. The rights of the children and victims of these actions are protected due to cyber-crime law. This helps eliminate these illegal and horrific acts that are unfortunately still a major problem on the internet. Cyber-crime laws also protect those from cyberbullying, which is becoming a major issue with today's youths. Cyberbullying can happen anywhere and at any time of the day. This is what makes it such a problem. Most non-cyber youth bullying occurs

within schools, practices, or at social gatherings, so targets at least can get a respite when they go home. However, cyber bullying is constant. The threat of such constant tormenting and bullying has forced many victims to commit suicide or even caused them to commit violent acts like shootings. A recent survey shows that "20% of children and young people indicate fear of cyber bullies made them reluctant to go to school" (http://www.bullying.co.uk/). This makes them act out in abnormal ways due to fear and depression. Laws also protect us against online identity theft and provisions within the laws secure and protect individual's privacy and protections. Thanks to the Identity Theft and Assumption Deterrence Act of 1998, laws regarding identity theft are now more serious. The act describes identity theft now as "knowingly transfer or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law." (http://ojp.gov/).

However, there are drawbacks as well. One of the drawbacks to these laws is that many of the terms are ambiguous and not as clearly defined. This opens the definition of such laws to interpretation, which could lead to dangerous actions. Data collection is one of these examples. There are numerous broad and ambiguous terms on the provision of data collection. Libelous statements online are another example. Libel found online does not define the traditional standards of what is considered prosecutable libel, due in part to the anonymity of posters and open forum styles of discussions.

The other drawback is that Cyber laws can threaten free speech. The ambiguity of the provisions laid out in the law sometimes makes it hard for people to speak their minds on certain sites. The pursuit of the truth can be seen as libelous purely in the manner of how it is dealt with. This makes people nervous and can thus feel restrained and pressured by the law and the

government. People sometimes fear that any negative criticism, opinion, or comment made could be seen as a direct attack to someone and could then be held against them.

This is where the benefits of Anonymous and hacktivists come in. These groups doggedly ensure that the right of free speech, as well as web ownership, is protected and ensured with respect everyone. They are an open-minded organization that stresses the importance of human rights, freedom, and privacy. They actively fight against government ownership of the web because they believe that the internet belongs to everyone and should not be owned. It is their core tenet that the internet belongs to the people, not the establishment.

These organizations also target certain social and cultural issues that go on in our global society. Going after Scientology, ISIS and the Westboro Baptist Church, all hateful and bigoted organizations that have caused turmoil to many, represents the core values of the organization. They are against intolerance, hatred, murder, and evil. Everyone is equal in their eyes and that belief must be upheld.

However, their methods leave a lot to be desired in many circumstances. It's not uncommon for them to go after innocent people in their pursuit of their goals. One of these instances was that in the aftermath of the Michael Brown shooting, Anonymous vowed revenge. In their pursuit of vengeance "associate of Anonymous tweeted photos of Belmar's family and the home address of a Ferguson police officer." (Rose).

Without a doubt, cyber-crime is a major issue and the laws that are in place today are very effective. They help weed out many of the criminals on the web, some of which are among the worst kind. However, this is grey to the situation because some of the so-called criminals are actually doing some noble acts by committing cybercrimes like hacking and DDoS'ing.

Anonymous are among those who are using these methods to try and make the world more tolerant, and less corrupt and violent. They've done much good, and have shown their hacking capabilities to the point that the U.S. government is using them in the fight against ISIS. However, just like any organization, they have several flaws and have also done much wrong. Cyber-crimes, like any other crimes, are sometimes not black and white, but very grey. For Anonymous, doing the right thing has sacrifices, and among those are attempting to use illegal methods to make the world a better place in their eyes.

Bibliography

- Alfonso, Fernando, III. "Now 10 Years Old, 4chan Is the Most Important Site You Never Visit." *Http://www.dailydot.com/*. N.p., 1 Oct. 2013. Web. 27 Nov. 2015. http://www.dailydot.com/business/4chan-10-years-christopher-moot-poole/
- "Cybercrimes Law & Legal Definition." *Cybercrimes Law & Legal Definition*. N.p., n.d. Web. 27 Nov. 2015. http://definitions.uslegal.com/c/cybercrimes/
- Schwartz, Matthew J. "Operation Payback: Feds Charge 13 On Anonymous Attacks." *Dark Reading*. N.p., 4 Oct. 2013. Web. 27 Nov. 2015. http://www.darkreading.com/attacks-and-breaches/operation-payback-feds-charge-13-on-anonymous-attacks/d/d-id/1111819
- Kostadinov, Dimitar. "Legality of DDoS: Criminal Deed vs. Act of Civil Disobedience." *Http://resources.infosecinstitute.com/*. N.p., 12 Dec. 2013. Web. 27 Nov. 2015. http://resources.infosecinstitute.com/legality-ddos-criminal-deed-vs-act-civil-disobedience/
- Rose, Sandra. "Anonymous Targets the Family of St. Louis' Chief of Police."*Http://sandrarose.com/* . N.p., 12 Aug. 2014. Web. 27 Nov. 2015. http://sandrarose.com/2014/08/anonymous-targets-the-family-of-st-louis-chief-of-police/>
- "Effects of Cyber Bullying." *Effects of Cyberbullying*. N.p., n.d. Web. 27 Nov. 2015. http://www.bullying.co.uk/cyberbullying/effects-of-cyberbullying/

- "Identity Theft and Financial Fraud." *Expanding Services To Reach Victims of*. U.S. Department of Justice, n.d. Web. 27 Nov. 2015. http://ojp.gov/ovc/pubs/ID_theft/idtheftlaws.html