

Bryan Quinonez
9/19/16
Writing 5
Literature Review


Hackers vs. Media: The Search for the Truth

The average citizen has no way of immediately knowing about the rest of the world without the use of technology. We have grown so used to the ability to pull out our phones or open up a computer that at times we have failed to recognize our dependence on technology. And so, it only makes sense that as technology advanced to become a staple of modern utility in all shapes of human life, so did the ways that people could exploit it and essentially exploit people. Hackers, people who break into electronic devices and manipulate them for their own benefit, have grown synonymous with the use of technology and have been portrayed in media for a while. A writer for ZME Science who has explored the transition of the hacking topic, looking back approximately 60-70 years reports that while hacking began attracting the public eye in the 80s, “students at universities like MIT had been hacking into systems since the mid 60s. Some of these earliest hacks involved breaking into telephone systems to make free long-distance calls” (4). Some of the best and most intelligent students in college built the foundations for hackers, accomplishing small feats in order to get something more efficiently or slightly cheat the system for their own personal gain. Mischief and small favors were a theme of early hacking practices, which continued not only on college campuses but in media too.

While films have stereotyped hackers to be reckless and foolish young nerds, the term has spread to include more than just a talented adolescent. Hackers are criminals. At least, in the eyes of many people. And you can't blame them, especially after learning what Tech Insider describes as some of the worst hacking crimes of 2015 alone, including roughly \$1 billion dollars of stolen money from 100 different banks from 30 different countries, the theft of 15 million T-

Mobile customers' private information as well as the nearly 80 million patient records stolen from the health insurer, Anthem Inc. (5). The attacks that took place in 2015 are more than unfortunate accidents or slip-ups on from large corporations but instead show a growing threat of skilled and informed criminals who know who to strike and how to get the most information possible with each and every strike. Hackers are not just local criminals who want to exploit weak corporate security systems or even college students who want to save a quick buck, they also consist of organized criminals worldwide who have more sinister intentions that usually involve messing with millions of people and dollars all at once. However, while many hackers have ill-intentions, there are certainly a plethora of hackers who transcend the mischievous nature that has been deemed "required" of a hacker.

Hacktivists are hackers who hack with a mindset of promoting social justice.

Anonymous, a group with more than a decade of experience and growth that makes it one of the most prominent hacking organizations in the world, has evolved into a hacktivist force. 

Anthropologist Gabriella Coleman, who has done years of research on Anonymous and even published a book which speaks of their positive endeavors supports their transition into being a leader in the world. Coleman describes how since 2008, Anonymous has "undertaken a series of "ops," protesting everything from Internet censorship by dictatorships during the Arab Spring, to PayPal's refusal to process payments to WikiLeaks, to the rape of a high-school girl in Steubenville, Ohio" (2). The group is still very active to this day as CNBC correspondent, Holly Ellyatt, reports how Anonymous declared war on the terrorist group ISIS after the recent terrorist attack in Paris which killed over a hundred people (1). This group that used to be considered troublemakers on the internet have evolved to being a global force that can support nations and groups as a whole, taking on anything from a local town's dilemma to one of the most prominent

terrorist groups in the world. However, while Anonymous has certainly achieved a lot in their most recent years that has garnered the support of the public eye, their track record is far from clean. Depending on a person's profession or even socioeconomic background, Anonymous may be considered a villain throughout their existence. Also, their own social justice views greatly differ from a lot of people and the group only acts when they see it necessary, unmoved by anyone else's agenda or prioritization of global issues. And so, while Anonymous is nowhere near perfectly nice and while a group like this could never be controlled, especially due to their creed of staying anonymous, there are certainly hackers that are only used for good.

Seung Lee, a writer for Newsweek's Tech and Science branch, describes an example of benevolent hackers, known as "white hat hackers" (3). Lee explains how these hackers were made prominent by large corporations that feared their security systems were viable to get hacked, and so they began hiring hackers to try and find cracks in their systems so that they could be fixed before a malevolent hacker tried to break through it (3). This preventative-measure synergy of hacker and hacked benefits both parties and attempts to maintain higher level of security ultimately for the consumer's sake. But although, hackers all have their own objectives, activities or desires, it is easy to try and generalize the term under one large umbrella of good or bad.

Generalized labeling usually comes from news outlets that try to analyze hacker activity under a certain light, usually trying to simplify the process of deciding for the viewer their opinions of hackers by just giving their own viewpoints. The media and hackers have been feuding for quite some time. However, not that long ago, the two groups sort of worked together. During Anonymous' beginnings, there was minimal tension between the two groups as Anonymous was less of a group and more of an activity. People would spend their days on

Internet Relay Chat (IRC) and discuss possible plans to work together without any real intentions to do anything. Back when Anonymous was more of an idea than the near tangible force that it is today, journalists were interested in the growing authority of this group on IRC and would attempt to communicate with members directly, sometimes with minimal success. However, it was not uncommon for connections to be made between journalist and Anonymous as happened with Gabriella Coleman, who to this day has remained an avid supporter of Anonymous and their objectives. Coleman specifically recalls her initial connections to Anonymous members, when they gained public attention in December of 2010 after only previously being known for online pranks, in an article she wrote for the *Limn* (6). In the article, Coleman describes her hidden obsession for the group and how she suddenly came into contact with members of Anonymous after being kicked from an IRC chat where the three members present could not confirm who she was (6). After this incident, Coleman was able to apologize and began talking to the members until she eventually got so close that she felt she was almost a member of Anonymous herself, hence her quandary in her title about her possible membership in the Anonymous organization (6). One of the most interesting aspects that Gabriella Coleman discusses in her encounter with Anonymous is the aspect of trust. Trust is a key component of being in the know, therefore everyone was very cautious of outsiders and a person's loyalty would be constantly tested. Trust is a big deal in a group that wants to stay as hidden as possible, therefore potential members/potential trustworthy people "acquire respect by engaging in activist interventions, some of them risky and illegal" (6). And while the spectrum of "risky and illegal" is incredibly broad in the U.S. justice system, these activities were anything but insignificant as Coleman goes on to report "there have been over two dozen arrests" (6). Anonymous' regular activities are

incredibly dangerous and so it makes sense that the building of trust serves as a form of initiation into the digital being that is Anonymous.

However, trust is not only important within the Anonymous community, trust is also a major issue from the perspective of the media to the public. The media is a multimodal idea since the media can be anything from news on the t.v., in the local newspaper, on the radio, and definitely on the internet. And so, considering how much news sources have to cover and how much people rely on news sources for information, building trust between the consumer and the news source is a necessity since at the end of the day, news sources come from corporations that need consumers in order to be successful. Therefore, news sources have to be very careful when covering cases like Anonymous, whose activities are purposefully very secretive and who take ownership very indirectly. An example of a failed media presentation of hacker activity was the case of AntiSec's hacking of 12 million user Apple ID's in 2012. All Things Digital writer, Arik Hesseldahl, who has written many articles for the technological news source since 2010, describes how the hacker organization AntiSec, which is a deviation from Anonymous, declared that they got access of 12 million user accounts from Apple's network through hacking an FBI computer, which would incite claims that the FBI has access to user's information even though Apple was very stern in promising the privacy of individuals (7). This would have been a major deal that would tie back to government surveillance of citizens similar to the NSA exposure from Edward Snowden, if the case was real. However, Hesseldahl writes about how the FBI soon came out to the public saying that no records were stolen and that these accusations were false (7). And while AnitSec's public announcement of its attack would shock a lot of people, the fact that the media brought the incident to a broader audience blew up the story much more than necessary as major news sources like USA Today had to change their articles with short

apologetic-edits like “The FBI says there is ‘no evidence indicating that an FBI laptop was compromised’ by the hacker group AntiSec” (8). And so, while news sources can be commendable for their quick responses and analysis to major crisis or problems around the globe, the domain of online hacking organizations is a tough one to track as people can attempt to make claims about activities they don’t even commit, which leaves both the news outlet and their followers dumbfounded.

And yet, while on many cases the news and hackers clash, they are still very alike in their goals, especially when comparing the news to the famous Anonymous hacker group. Both the news and Anonymous try to expose information to the public so that they can be well informed of what is going on around them that they would not be able to access easily on their own. In many instances, reporters and hackers push shady business activities in order to find out the truth about what a corporation is doing and bring to light the facts that would change the audience’s opinion of that corporation or organization. Both news sources and hackers commit many mistakes, whether it be from false information or from internal issues, both have a lot riding on them and many people they hope to please. There will always be critics, however in the general scope of the public’s eyes Anonymous is beginning to seem like a better and better organization and it may all be due to the way the news presents them.

Works Cited

<http://www.cnbc.com/2015/11/16/anonymous-hackers-declare-war-on-islamic-state.html> (1)

<https://www.thenation.com/article/truth-about-anonymouss-activism/> (2)

<http://www.newsweek.com/good-hackers-are-losing-internet-war-bad-hackers-says-experts-412974> (3)

<http://www.zmescience.com/tech/hacker-stereotypes-0643654/> (4)

<http://www.techinsider.io/cyberattacks-2015-12> (5)

<http://limn.it/am-i-anonymous/> (6)

<http://allthingsd.com/20120904/fbi-says-antisecc-hackers-lied-about-list-of-iphone-id-numbers/>
(7)

<http://content.usatoday.com/communities/ondeadline/post/2012/09/hackers-claim-breach-of-fbi-laptop-nets-apple-device-ids/1?AID=10709313&PID=4003003&SID=itm9xkj9pf01b0nu00dti#.V-smZpMrKgR> (8)