How ethics impacts hacktivism: a reflection of events

Brian J. Galli

School of Computer Science, Innovation and
Management Engineering,
Long Island University,
Brookville, New York, USA
Email: brian.galli@liu.edu

Abstract: This paper analyses the ethics of hacktivism by studying the actions of the hacktivist group called anonymous. The paper is intended to discern whether the actions of anonymous are considered ethical. In order to determine the ethics of their activities, this study discusses five major operations induced by anonymous, including ethical implications relating to each. The research indicates that of the five operations, only one operation provided substantial evidence that demonstrates unethical behaviour by the group.

Keywords: ethics; hacktivism; information technology; anonymous.

Reference to this paper should be made as follows: Galli, B.J. (2018) 'How ethics impacts hacktivism: a reflection of events', *Int. J. Qualitative Research in Services*, Vol. 3, No. 1, pp.11–20.

Biographical notes: Brian J. Galli obtained his Doctoral degree in Engineering Management from the Old Dominion University. He also obtained his Bachelor of Science in Industrial Engineering from the Binghamton University and Masters of Science in Engineering Management from the Missouri University of Science and Technology. He works as an Assistant Professor of Management Engineering at the Long Island University – Post. He also owns Apex Strategies, Ltd., a company that specialises in continuous improvement consulting and training. He has over nine years of experience in applying continuous improvement tools in many arenas.

1 Introduction

Much debate occurred recently over issues relating to ethics and illegality of actions. One question constantly asked is, if a person breaks the law for an ethical cause, are his actions deemed illegal? Some will argue that an individual's motives do not exonerate him from breaking the law. However, it is feasible to consider this implication as more complex. This is especially true when addressing the modern issue concerning hacktivism.

Hacktivism is defined as hacking a website, computer, or computer network to accomplish some type of political or social goal. While the act of computer hacking is undoubtedly illegal, hacktivists introduce a new, ethical grey area. This is the case because in most scenarios, hacktivists' actions produce a form of greater good for the majority.

One of the most famous hacktivist groups around the world is anonymous. This group implements different hacking techniques to spread political and social messages. While anonymous members are breaking the law by hacking into systems, their actions are also producing more benefit than harm. In this respect, their actions are considered ethical and should not be deemed illegal. This report intends to prove that anonymous' actions are ethical.

2 Research methodology

This paper collects and analyses existing literature about the impact of ethics in the activities of hacktivist group anonymous. We conducted a meta-analysis instead of a traditional literature review because the meta-analysis is a quantitative approach. With meta-analysis, the researcher can standardise the methods and results from different studies. Because we can compare estimates, bias is eliminated from the process. The meta-analysis can also be conducted over all papers internationally available, based off priori-defined criteria. This is what eliminates potential bias. A meta-analysis also has some limitations. For example, it returns a narrower range of results than a traditional review because of the confinements. It may be more difficult to identify studies of interest, because the meta-analysis will only look into research that was published and reports significant results. When a meta-analysis cannot unearth relevant studies, it is coined the 'file-drawer' problem. Fortunately, this limitation can be avoided, since many new ways have been developed in methodological literature to test and eliminate it (Rosenthal, 1979; Card and Krueger, 1995; Begg and Mazumdar, 1994).

Before the meta-analysis, we conducted a traditional review by collecting articles from various online databases, including Scopus, ISI, and Elsevier. We conducted the study for four months, from January 2017 to April 2017. We only collected articles and chapters in books and monographs. We also included searches with several general keywords, as listed before the introduction of this paper. As a result of the searches, 30 pieces of literature were identified (N = 30). We filtered the 30 with a meta-analysis. When we reached the saturation point, we stopped the search. This is when combining keywords and incorporating new ones returns information we already have.

We incorporated search filters and Boolean functions including AND, OR, and NOT to filter the information. The search filter had a balance of sensitivity and precision. Sensitivity is finding all relevant material while precision is the ability to reject irrelevant material. The initial filter had high sensitivity. Over time, we adjusted it to a more suitable level of precision balanced with sensitivity.

The filter was not as beneficial in identifying wider gray literature, which is material not commercially published. This literature had to be identified via manual searching on online, internet based databases. We got the N of 30 studies down to a sample size of 15 (n = 15), which is 50% of the total literature identified. We then used textual content analysis, both quantitative and qualitative, to find similar traits in all the literature identified. We categorised the results into themes and patterns via an affinity diagram, which was used to create the sections and themes of this paper. Thus, we identified 11 potential articles that incorporate the keywords and topics in this study.

The selection of studies began with an N of 30 potential articles. However, the complete search procedure returned a total of 11 (36.67% of the original population). With thorough review of the 11, it was found that the results varied in focus and depth

pertaining to the focus of this study. The next section presents the findings of the research methods in the scope of the themes/topics discussed in the subsequent sections.

3 Findings

3.1 What is hacktivism?

Hacktivism is different from other forms of hacking, such as cyberterrorism, for one primary reason. The end goal of hacktivist actions is to relay a morally and ethically beneficial message to the public. Cyberterrorism, on the other hand, derives from an interest to terrorise, or alienate, the public. The term hacktivism was coined in 1996 by a member of The Cult of the Dead Cow, a group of hackers (Casserly, 2015). Prior to 1996, individuals were hacking into systems, but for different purposes.

One instance of early hacking is known as the 'Blue Box', created by Steve Jobs and Steven Wozniak during the 1960s and '70s. The Blue Box was a device that could override automatic operators in telephones. As a result, the user could make free long distance phone calls. At that time, placing distance phone calls was very expensive, so Jobs and Wozniak created a way in which the public could circumvent expensive costs in communication. Such a situation is arguably one of the earliest forms of hacktivism because Jobs and Wozniak provided a service that would benefit the general public, even if it were considered illegal.

In most instances, modern hacktivists use hacking techniques as a means to demonstrate civil disobedience to protest issues such as government control and censorship. Hacktivists implement a variety of techniques, including distributed denial of service (DDoS) attacks, information theft (Doxing), website defacement, and virtual sit-ins (Techopedia, n.d). There is a plethora of other methods that can be utilised in matters of civil disobedience. The bottom line is that today, "Hacktivists continuously initiate and engage in court battles challenging freedom of internet speech and other digital media restrictions" (Techopedia, n.d). This form of hacktivism, fighting for free speech across the internet world, is considered one of the most important causes that the group anonymous stands for.

3.2 What is anonymous?

To better comprehend who and what anonymous is, it is crucial to understand the group's origins. While they officially made their presence in 2008, the group was already forming prior to that. As early as 2003, a website entitled 4chan was developed as an image-based forum. It boasted utter anonymity for all of its users (Stanek, 2015). This, in part, impacted the naming of the group, anonymous. When a user made a post to 4chan, he had the option to post under his name or post under 'anonymous'. As more and more people joined the site and found interest in writing under anonymity, most of the website threads were filled with 'anonymous' submissions. People could essentially voice their opinions and thoughts without any repercussions, because there was no tracing of an anonymous user. The website also played a major role in creating the actual group anonymous.

4chan works in a very unique way compared to other websites that support thread and blog creation. With 4chan, if a thread is inactive for a while, it will eventually disappear. Essentially, it leaves no trace in the World Wide Web and is not archived. This type of

structure promotes users to start threads with the intention of provoking immediate reaction out of someone, usually through a funny or shocking outlet. In some ways, 4chan became the hub for the creation of 'memes' and other internet in-jokes. As a result, 4chan introduced a new type of international internet culture to millions of anonymous people sharing a common social platform (Knappenberger, 2014).

A large aspect of this new culture is the concept of 'trolling'. Trolling is considered the act of deliberately enraging another person over the internet, especially in the event that they take something too seriously. Trolling became an influential factor in the creation of anonymous, especially since it would become a tactic they would use later down the road. Users of 4chan began 'invading' other websites with the intention of offending users from using that site. Such deliberate actions demonstrated that 4chan users would be able to accomplish many things and have an impact across the internet as long as they worked together. This realisation is one of the reasons 4chan users worked together to turn against a man named Hal Turner, the host of an internet talk show.

3.3 Hal Turner

In 2006, 4chan collaborated to shut down Hal Turner's talk show on the internet. They were firm believes that he was a 'neo-Nazi' who was spreading negative beliefs across the internet. The attack began in different forms. At first, the attacks consisted of prank phone calls to his show. Then, 4chan members escalated these attacks by posting personal information about Turner and his family on the web. They further began a DDoS attack on his website as a way to make it unavailable to the public (Olszewski, 2010). Finally, anonymous users had 'countless' pizzas delivered to his house with pallets of industrial materials. This attack ended up costing Turner thousands of dollars, which ultimately prevented him from being able to afford the talk show any longer (Knappenberger, 2014). Eventually, 4chan brought enough attention to Hal Turner and his actions, because he was arrested for making threats against numerous public figures. This is considered an accomplishment and important event in the history of anonymous' formation. It demonstrates that goals could be achieved if everyone worked together across the internet for a common cause.

There is no denying that the tactics used to attack Hal Turner were considerably illegal. However, there were ethical motives behind the attacks, which justifies 4chan users' actions. According to some members of anonymous, among many of the negative actions under Turner's name, he bullied a well-known member of the 4chan community. As a result, the other users felt it was their obligation to come to the user's defense by shutting down Turner (Knappenberger, 2014). Perhaps ruining a man's career in owning a talk show may be considered a slight overreaction and unethical, however in this particular scenario, that is not the case. Hal Turner's talk show was a platform for him to broadcast all of his hate speech and racist propaganda. 4chan's initial intentions may have been unethical or over-reactionary, however by the end of the attacks, it was proven that they were acting out for the greater good of the general public.

3.4 Project chanology

The next operation, also known as an op, that anonymous conducted was in 2008. This was when the name anonymous became officially known to the public. The op was called project chanology. It began after a video that featured the actor Tom Cruise discussing

Scientology was leaked to the internet. The Church of Scientology found the video to be embarrassing, and worked around the clock to make their legal team remove the video every time it was posted (Casserly, 2015). To anonymous, censoring the internet is considered an attack on freedom of speech. This is one of the group's highest held beliefs. And, they were not happy to see the Church of Scientology going against this fundamental right. Thus, soon after the video was repeatedly removed from the internet, anonymous formed a group to perform project chanology, and released a video to rally their troops (below is the transcript of that video):

> "Over the years, we have been watching you. Your campaigns of misinformation; suppression of dissent; your litigious nature, all of these things have caught our eye. With the leakage of your latest propaganda video into mainstream circulation, the extent of your malign influence over those who trust you, who call you leader, has been made clear to us. Anonymous has therefore decided that your organization should be destroyed. For the good of your followers, for the good of mankind--for the laughs--we shall expel you from the Internet and systematically dismantle the Church of Scientology in its present form. We acknowledge you as a serious opponent, and we are prepared for a long, long campaign. You will not prevail forever against the angry masses of the body politic. Your methods, hypocrisy, and the artlessness of your organization have sounded its death knell....
>
> You cannot hide; we are everywhere.
>
> We cannot die; we are forever. We're getting bigger every day--and solely by the force of our ideas, malicious and hostile as they often are. If you want another name for your opponent, then call us Legion, for we are many....
>
> Knowledge is free.
>
> We are Anonymous.
>
> We are Legion.
>
> We do not forgive.
>
> We do not forget.
>
> Expect us." (Jacobsen, n.d.)

The attack on the Church began shortly after this video was posted, in January of 2008. Much like the attacks against Hal Turner, this one included a DDoS attack and a 'real' attack on the Church's phones and fax machines (Knappenberger, 2014). On 26 January, a man named Mark Bunker uploaded a video to YouTube with the intention of encouraging members of anonymous to avoid illegal means in battling the Church. Instead, he suggested the anonymous members to utilise legal strategies, such as picketing, to get their message across (Jacobsen, n.d.). Anonymous heeded his advice and created another video that urged all anonymous members to go to their nearest major city and protest the Church of Scientology. This was accomplished on 10 February 2008. Anonymous also created a code of conduct video that explained how their members ought to behave during protests. They urged members to wear masks in order to protect their identity via anonymity (Knappenberger, 2014). Over 7,000 protesters appeared on 10th of February across multiple major cities around the world (Jacobsen, n.d.).

This op demonstrated that anonymous members could yield much power when they worked together towards a common goal and/or cause. Project chanology created new channels for news outlets and opponents of the Church of Scientology to publicly

question or disagree with them. Prior to the op instilled by anonymous, the Church was not faced with opposition because people were too afraid to counter it. The Church responded to any opposition with strong legal force. Because of anonymous, they developed a slight sense of fear from retaliation of the general public.

The call to arms video for project chanology is a valid example of the anonymous code of ethics as well as their motivations. As anonymous would say, "For the good of your followers, for the good of mankind – for the laughs" (Jacobsen, n.d.). This is the best quote that explains anonymous' ethical guidelines. A majority of the time, anonymous members act out for what they believe is the benefit of the general public. However, they also make these decisions out of pure enjoyment. This may be the issue by which anonymous intentions may not be the most ethical. It is not the most ethical decision to launch an attack against a large group of people solely for entertainment purposes. However, because of the way in which anonymous frames its attacks, there is support that the members will carry out the attacks more for the benefit of the public rather than for personal enjoyment. When anonymous conducts an op, members are free to come and go as they please. In other words, if a member feels that it would be beneficial to the public, they can choose to join an op. It is up to the members to discern whether or not an op is ethical and morally right. Anonymous members also do not follow any specific leadership. Instead, they have different leaders according to the ops and tasks at hand. As a result, they are not under strictly enforced orders to just wreak havoc for fun. In fact, the leaders of ops want the members to act for one cause, and for the benefit of the public. The ops must be taken seriously.

Project chanology, being the first major anonymous op, was a great success in proving that anonymous had power, but also in showing that anonymous cannot be considered a terrorist organisation. Project chanology demonstrates that anonymous yielded great power, which they respected and used for the greater good of the public. anonymous witnessed an injustice being carried out against freedom of speech across the internet and took action to put a stop to it. Perhaps some of their methods to achieve such a goal are considered illegal, but they were not executed with unethical intentions. For example, one could, and many often do, argue that the DDoS attacks are modern versions of a sit-in protest. As per the case of anonymous, DDoS attacks are one of the worse legal offenses they commit, but even that can be identified as an ethical form of protest in today's technologically advanced society.

3.5 Operation payback

The next major op led by anonymous was operation payback. Operation payback began when major media companies attempted to take down two internet piracy website, Megaupload and ThePirateBay. Such actions caught the attention of anonymous because the major media companies were utilising DDoS attacks to shut down the two websites. Anonymous considered this a major form of hypocrisy.

The op began as an attack against the media companies, but eventually evolved into a grander attack. This was made possible primarily by the introduction of WikiLeaks. WikiLeaks is a website that encourages sources to send information to them and then publish the raw documents alongside articles (Sauter and Zittrain, 2010). In 2010, credit card companies, such as MasterCard, Visa, and PayPal, halted their donations to WikiLeaks in an attempt to censor the documents that were being leaked. A member

of anonymous stated, "Anonymous is supporting WikiLeaks not because we agree or disagree with the data that is being sent out, but we disagree with any form of censorship on the internet" (Halliday and Arthur, 2010). This was another instance in which anonymous found the general public's freedom of speech and large companies were infringing upon censorship rights. As with previous ops, anonymous launched numerous DDoS attacks against the companies in question. Anonymous further targeted websites, such as white supremacist websites, that PayPal allowed donations to.

This op is especially important in deciding whether or not anonymous is ethical in its actions. It is well known that anonymous did not curb its use of illegal methods to get a point across. However, during this op, other major companies implemented such illegal methods in order to censor the internet. This begs the question: Why are some allowed to use DDoS attacks and others are not? If major media corporations can fight back against piracy with DDoS attacks, then why are private citizens, grouped together in anonymous, not allowed to do the same when they face an injustice? If DDoS attacks are illegal for members of anonymous, then they should be illegal for everyone, even if they are being utilised against illegal piracy websites. As a result, this op, more than any other, puts anonymous' actions into an ethical grey area. It sheds significant light on the notion that their tactics are in fact legal and ethical.

Operation payback also included a second part, which was similar to project chanology. A major company was attempting to silence voices on the internet for various reasons. Anonymous stepped in in order to keep their freedom intact. As stated earlier, the members of anonymous did not necessarily agree with what WikiLeaks was doing, but the group was more than willing to defend WikiLeaks' right to share information on the internet. After the op was completed, it was noted that PayPal alone lost over $5.6 million (Schwartz, 2013). This is a major punishment, and some would say that the punishment does not necessarily fit the crime. However, one may also argue that there can be no price tag to put on freedom of speech and censorship of media outlets.

3.6 Operation Egypt

In 2011, Egyptians were protesting against their government, which they deemed was more dictatorial in nature. One of the first actions made by Egypt's government was to restrict internet usage in an effort to curb citizens' ability to communicate about the changes and social unrest in the country. Anonymous surveyed that Egypt blocking their citizens' access to the internet was incorrect, and therefore instituted a new op called operation Egypt.

This operation was unlike those they had done in the past because, instead of taking on a corporation, they were going against an entire country. Anonymous used several different tactics for this operation. The group sent out tweets geared towards the people in Egypt that were unable to access Twitter. They set up live feeds of the Egyptian protests, which clearly depicted the police brutality and shootings (Knappenberger, 2014). Eventually, Egypt completely shut off the internet for the entire country. Anonymous responded by setting up communication lines and dial up internet connections for Egypt's citizens. Anonymous even created PDF files in Arabic that explained how to treat tear gas. This was their effort to help the citizens against the harsh police attacks (Knappenberger, 2014). Eventually, the dictatorship in Egypt fell, and the people were once again free to communicate. However, it is important to note that this would not have

been as possible if anonymous had not taken an ethical, yet illegal stance, in going against the government to benefit the wellbeing of the general public.

This is considered one of the first times in which anonymous became involved in an issue whose scope reached beyond just the internet. Furthermore, this is the best operation that demonstrates anonymous' ability to bring about a large amount of good for the people. Without anonymous' help in Egypt, the citizens may not have been able to convey to the world the extreme oppression they were facing from their government. Even though anonymous is known for protecting freedom of speech across the internet, they also will take it a step further, as they did in Egypt. After seeing anonymous' beneficial acts in Egypt to save lives and promote freedom from oppressive governments, it is safe to assume that their actions are ethical.

3.7 Knightsec and the unethical side of anonymous

The final op that should be discussed is the Steubenville op. This was an operation run by an offshoot of anonymous that called them Knightsec. The operation was important because it took a relatively small town with a population of roughly 18,000 and put them 1on the main stage in national media. Two high school football players in Steubenville were convicted of raping a 16-year-old girl. However, when this occurred, there was a major cover-up by the superintendent of the school district (Baker, 2013). Many others in the district supported the cover-up.

Anonymous performed an op against this town in order to expose the truth about the girl's rapists. Anonymous used doxing to achieve its goal. Doxing is the act of finding and exposing private documents online. Eventually, anonymous was successful in bringing this issue to the nation's attention. However, they were faced with an obstacle. Many of the claims made by anonymous in an attempt to unearth the truth were in fact false. Additionally, many people paid a very real price for such carelessness. For example, "If you Google the name of a 16-yearold girl who was out of town the night of the rape, you'll find her photo alongside untrue claims she drugged and lured the victim to the party" (Baker, 2013). Unfortunately, this is not the only person who has her name wrongly associated with such a horrible crime. Now, many people in Steubenville are forced to deal with untrue claims such as this one because they helped to coverup the rape. This is the backlash of anonymous not using caution before releasing documents online.

This is one of the main ops that one could point to in order to claim that anonymous is not an ethical organisation. It may allude to the belief that anonymous strives on starting and maintaining a state of chaos. While it is hard to defend the idea that anonymous strives on chaos, it does not necessarily make them unethical. Most operations do not last for more than a few months since the attention of the group will shift quickly. Because of this fact, anonymous members need to act quickly in order to accomplish a goal. In this particular operation, the need to act quickly led to cutting some very unfortunate corners that damaged innocent people's lives. There is no defending the ethics of this decision because it is unethical to rush a job, especially one as sensitive as this, to reach a goal. In the end, however, two rapists were convicted that would have otherwise gotten away with a crime because they were the lead football players.

4 Conclusions

When it comes to determining the ethics of a hacktivist group such as anonymous, it is no simple task. Anonymous is an amorphous group, which means it is constantly changing its goals and members, with no sense of concrete leadership. This leads to the implication that the group cannot determine and solidify ethical codes. However, it is possible to look at their past actions and make a judgment based on how they behaved in each scenario. As seen throughout this report, anonymous behaves ethically in almost all operations. They are constantly fighting for freedom of speech across the internet, but also fighting against censorship and oppressive government regimes. They lash out against actions that go against the morals and ethics of the general public's wellbeing. Anonymous may use some illegal tactics to achieve a goal, but as time prevails, they transgress into a more legal area by using protests rather than hacking or pranks across the internet. Only time will tell if this movement continues. It is safe to assume that unless there is a drastic change in their ethics, anonymous is a force for the good.

In terms of future research, there are many new avenues that research into hacktivism could take. More specifically, it is suggested that future research evaluates hacktivism efforts by other groups in addition to anonymous. While anonymous has perhaps the most visibility, there are many other groups that have performed hacktivism efforts. It would be interesting to investigate the efforts and impacts of these different groups. Another area of future research could be to investigate hacktivism efforts but in different business/industry sectors; as the paper has shown, there have been hacktivism efforts in many different industries, from healthcare to government. So it would interesting to investigate the efforts and evaluate their impacts across the many industries.

References

Baker, K.J. (2013) *A Town Destroyed for What Two People Did: Dispatch from Steubenville*, September 16 [online] http://jezebel.com/a-town-destroyed-for-what-twopeople- did-dispatch-fr-1298509440 (accessed 6 April 2017).

Begg, C.B. and Mazumdar, M. (1994) 'Operating characteristics of a rank correlation test for publication bias', *Biometrics*, Vol. 50, No. 4, pp.1088–1101

Card, D. and Kruger, A.B. (1995) 'Time-series minimum-wage studies: a meta-analysis', *The American Economic Review*, *Papers and Proceedings of the Hundredth and Seventh Annual Meeting of the American Economic Association*, Vol. 85, No. 2, pp.238–243.

Casserly, M. (2015) *Who is Anonymous? A Short History of Hacktivism*, 18 November [online] http://www.pcadvisor.co.uk/feature/Internet/what-is-hacktivismshort-history-anonymous-lulzsec-arab-spring-3414409/ (accessed 6 April 2017).

Halliday, J. and Arthur, C. (2010) *WikiLeaks: Who are the hackers behind Operation Payback?*, 8 December [online] http://www.theguardian.com/media/2010/dec/08/anonymous-4chan-wikileaks-mastercard-paypal (accessed 6 April 2017).

Jacobsen, J. (n.d.) *We Are Legion: Anonymous and The War on Scientology*, [online] http://www.lisamcpherson.org/pc.htm (accessed 6 April 2017).

Knappenberger, B. (2014) *We Are Legion: The Story Of The Hacktivists* [*Video file*], 6 July [online] https://www.youtube.com/watch?v=bC1ex2zRCYA.

Olszewski, A. (2010) *Internet War Waged Against Hal Turner, Hudson County Hate Monger and FBI Informant*, 7 April [online] http://hudsoncountyfacts.com/hudsoncounty/2010/04/07/Internet-war-waged-hal-turner-hudsoncounty-hate-monger-fbi-informant/ (accessed 6 April 2017).

Rosenthal, R. (1979) 'The 'file drawer problem' and tolerance for null results', *Psychological Bulletin*, Vol. 86, No. 3, pp.638–641.

Sauter, M. and Zittrain, J. (2010) Everything you need to know about Wikileaks, 9 December [online] https://www.technologyreview.com/s/421949/everything-youneed-to-know-about-wikileaks/ (accessed 6 April 2017).

Schwartz, M.J. (2013) *Operation Payback: Feds Charge 13 on Anonymous Attacks*, 4 October [online] http://www.darkreading.com/attacks-and-breaches/operationpayback- feds-charge-13-on-anonymous-attacks/d/d-id/1111819 (accessed 6 April 2017).

Stanek, B. (2015) *How did Anonymous Start? The History Of The Mysterious 'Hacktivist' Group Began Quite Some Time Ago*, 20 February [online] http://www.bustle.com/articles/65444-how-did-anonymous-start-the-history-of-the-mysterioushacktivist-group-began-quite-some-time-ago (accessed 6 April 2017).

Techopedia (n.d.) *What is Hacktivism?* [online] https://www.techopedia.com/definition/2410/hacktivism (accessed 6 April 2017).