Anonymous: What do we have to fear from hacktivism, the lulz, and the hive mind?

A thesis presented to the

Program in Political and Social Thought at the
University of Virginia

by

Victoria McLaughlin

in partial fulfillment of the requirements for the degree of Bachelor of Arts with honors.

2 April 2012

Advisor(s): _____
Prof. Siva Vaidhyanathan

TABLE OF CONTENTS

Victoria McLaughlin

Anonymous: What do we have to fear from hacktivism, the lulz, and the hive mind?

In this thesis, I argue that the online collective Anonymous deserves serious attention as a hacktivist group. Anonymous has gotten a lot of press lately, but because the group is an amorphous online collective most famous for foreboding YouTube press releases and Guy Fawkes masks few people take the group seriously. However, Anonymous is more than just a trolling outfit and it is important to recognize the real consequences of hacktivism. Hacktivism, a portmanteau of hacking and activism, is the use of computers and/or hacking techniques towards political and social ends. Anonymous's main tool of hacktivism is distributed denial of services attacks (DDoS), an attack where a website is overloaded with traffic and shuts down for a period of time. Some, like anthropologist Gabriella Coleman, consider DDoS attacks to be a form of peaceful social protest. Coleman likens a DDoS attack to a digital sit-in. But, the FBI and international law enforcement agencies have arrested Anons around the globe that participated in DDoS attacks against public and private websites. I argue that, because DDoS attacks are not a national security concern, arresting and prosecuting attackers harms internet freedom and undermines the spirit of the internet.

The first chapter is a history of the hive mind and its origins on 4chan.org. Anonymous has a history of doing 'spectacularly stupid' things, but recent Anonymous Operations, such as Project Chanology, a protest again the Church of Scientology, and Operation Payback, an operation attacking anti-piracy outfits, indicate that the hacktivist collective is not only motivated by the lulz, a corruption of laugh out loud; the expression usually expresses joy in someone else's misfortune. The second chapter is a brief history of the internet and the hacker ethic, beginning in the 1980s. In the chapter, I elaborate on the open structure of the internet network and how this supported creativity and community among hackers. The chapter ends with a discussion of the end of the golden age of hacking and the rise of trolling, which I call the new nethic, or Net ethic. The third chapter describes Anonymous's transformation into a politically active group; I advocate that Anonymous's actions be assessed in terms of internet use and misuse, that is, does the hive mind support or undermine the founding principles, such as free access and free information, of the internet? The fourth chapter describes specific AnonOps and demonstrates that although Anonymous is an online collective, their actions have real consequences.

In the conclusion, I discuss the US State Department's Free Internet Agenda and the three challenges that the open internet poses to society. Namely, the open internet and hackers put our liberty and security at risk; however, legislating against such activities would be a greater infringement upon First Amendment rights. In the end, I agree with cybersecurity specialist Richard Forno that Anonymous, as of yet, has not caused any grave damage and it is therefore better to live with the threat of a raid than begin a preemptive strike.

Anonymous, the hacktivist online collective famous for donning Guy Fawkes masks and releasing ominous video press-releases alluding to the end of tyranny and the rise of a new, democratic world order, has received a lot of press as of late. Thanks to the group's attacks on major institutions like MasterCard, Visa, the United States Department of Justice, the Federal Bureau of Investigation, and even an attempt on the Vatican, maverick 'Anonymous' is now a sexy and provocative buzzword. The name 'Anonymous' did not always have such cache—in the early 2000s Anons[1] were nothing but internet trolls, people "who intentionally disrupt online communities,"[2] and rabble-rousers; Anons were most known in the internet community for trolling for entertainment and raiding, or launching an online attack, against various individuals for ambiguous reasons. The group first garnered national attention in 2008 when it targeted the Church of Scientology and became a household name once again last winter in the wake of WikiLeaks. In contrast to their pervasive presence in the media today, a few years ago, the 'digitized global brain' was only a blip on the radar.

CHAPTER 1

Introduction to Anonymous, the lulz, and the hive mind

"Ya dun goof'd"

In July of 2010, Anonymous launched a raid on 11-year-old Jessi Slaughter, real name Jessica Leonhardt, a self-professed 'scene queen' and loyal fan of the band Blood on the Dance Floor. Leonhardt was famous in an online gossip community for tweeners, Stickydrama, a site rife with middle school bathroom wall-type gossip. Gawker writer Adrian Chen describes Stickydrama as "a crowd-sourced gossip website for 13 year olds who loiter in mall food courts."[3] A few months before the raid, rumors about Slaughter and the lead singer of Blood on the Dance Floor, Dahvie Vanity, circulated on Stickydrama. Vanity, a twenty-something with 'coontails'[4] was (allegedly) engaged in a friends-with-benefits type relationship with Slaughter. However, Vanity was not the pedophilic front

[1] Participants in Anonymous Operations (AnonOps) or individuals who identify as Anonymous.
[2] Mattathias Schwartz, "Malwebolence," *The New York Times Magazine*, August 3, 2008. http://www.nytimes.com/2008/08/03/magazine/03trolls-t.html?pagewanted=all (accessed March 4, 2012).
[3] Adrian Chen, "How the Internet Beat Up an 11 Year Old Girl," *Gawker*, July 16, 2010, http://gawker.com/5589103/how-the-internet-beat-up-an-11+year+old-girl?skyline=true&s=I, (accessed March 4, 2012).
[4] 'Coontails' are horizontally died sections of hair, usually about 2 inches thick. They are supposed to be reminiscent of a raccoon's tail.

man to Slaughter's Lolita; instead, the anticipated roles were reversed—Vanity was her victim.[5] Slaughter's YouTube channel was also well known in the scene-tween community and her online persona garnered a lot of negative attention, especially from her peers. One Stickydrama user wrote, "If Dahvie were a pedophile, why would he pick her! Other than the fact she's a slut!"[6] To put it simply, Slaughter had haters.

Slaughter's notoriety peaked after a particularly vitriolic, profanity-laden YouTube video was posted on the "random" board, /b/, of popular image hosting website, or imageboard 4chan.org. /b/ is, more or less, the dregs of the internet; it is a haven for a handful of mischievous miscreants and a whole bunch of innocuous trolls—the rest of the internet proletariat calls them /b/tards.[7] /b/ is notorious for various reasons, among them: the genesis of Anonymous, hosting countless pictures of cats, and the posters that launch cruel and relentless attacks on individuals for no obvious reason at all. Slaughter gave the trolls no shortage of material. For example, Slaughter speaks to her webcam, "I'm happy with my life, okay, and if you can't, like, realize that and stop hating, then you know what? I'll pop a Glock in your mouth and make a brain slushie."[8] If you want to leave her more hating comments, don't, because she has like, *lots* of comebacks. Slaughter closes the speech throwing up her middle fingers to all of her haters. [9]

/b/tards organized and rallied around a shared hatred for the adolescent Slaughter, finding and her address, phone number, email address, and real name. They ordered dozens of pizzas to her home, sent call girls, and harassed her family with telephone calls. Slaughter eventually cried on webcam and gossip and news website Gawker eventually reported that she had been put under police

[5] "Jessi Slaughter," *Know your meme*, http://knowyourmeme.com/memes/events/jessi-slaughter, (accessed March 4, 2012).
[6] Chen, "How the Internet Beat Up an 11-Year-Old Girl."
[7] Schwartz.
[8] "Jessi Slaughter," *Know your meme*.
[9] "Jessi Slaughter," *Know your meme*.

protection. The hive mind ultimately got bored of harassing Slaughter and moved onto Vanity, 'Googlebombing'[10] his name so that Google web search results would imply he had raped a girl. One user wrote on Internet Relay Chat (IRC)[11] "we are like…some kind of internet hate machine."[12]

In a final exchange between Slaughter and the 'internet hate machine' she says, in between tears, "I just wanted to tell you guys that you ruined my life."[13] Only days before Slaughter had told her haters to "get AIDS and die," and now she was visibly distraught and emotionally devastated by complete strangers. Slaughter begged them to stop through raspy, uncontrolled sobs, "My household has been torn apart!" she cries.[14] Her father, Gene Leonhardt, enters the screen and disrupts Slaughter's almost touching moment. Instead of inspiring sympathy in viewers like his daughter did—like any crying 11- year-old girl can—Leonhardt launches a tirade against the trolls and births a very popular meme: "You will have to deal with the police, because *ya dun goof'd!*" he hollers. Leonhardt yells at his webcam again: the trolls have been reported to the cyberpolice. (They do not exist.) Their activities will be backtraced. (This is impossible if the user has blocked his or her IP address.) His video ends "And if you come near my daughter, guess what? Consequences will never be the same, ya lying bunch of pricks."[15]

———

[10] Googlebombing artificially increases the number of searches for a term in Google so that it ends up on the Hot Trends list, a continuously updated list of what people around the world are searching for using Google.
[11] Internet Relay Chat (IRC) is a protocol for online instant messaging. It supports both synchronous group chats and one and one chats via private messaging. Group chats occur on different channels, denoted by #. IRC is one of the places that trolls and Anons discuss and plan their raids; it better facilitates direct communication than /b/.
[12] Adrian Chen, "The Art of Trolling: Inside a 4chan Smear Campaign," *Gawker*, July 17, 2010, http://gawker.com/5589721/the-art-of-trolling-inside-a-4chan-smear-campaign (accessed March 4, 2012).
[13] Adrian Chen, "How the Internet Beat Up an 11-Year-Old Girl."
[14] Adrian Chen, "How the Internet Beat Up an 11-Year-Old Girl."
[15] Xeni Jardin, "4 chan 'backtraced,' reported to the 'cyberpolice' by mustachioed mad dad," *Boing Boing*, July 16, 2010, http://www.boingboing.net/2010/07/16/mad-mustachioed-dad.html (access March 4, 2012).

Leonhardt actually had very little recourse to identify the people who had been harassing his daughter. While the attacks against Jessi Slaughter unequivocally count as cyberharrassment, neither Leonhardt nor the authorities have the capabilities to trace the source of the pranks, especially because few of them were actually carried out online. Consider how easy it is to visit a webpage, get a phone number, and then make a phone call—the internet was the source of information, but not the tool of harassment. Anonymity, for many, is one of the major drawbacks of the internet and especially of online communities. People fear that without the accountability of reputation there is no reason for others not to troll. How do people behave when there aren't any consequences? In some cases, people are mean. In others, like the Slaughter case, they troll relentlessly. In exceptional cases, people use the privilege of anonymity to take the pranks way too far. Consider Megan Meier, a 13 year-old victim of cyberbullying. Meier committed suicide in 2007 after a boy she had been talking to on MySpace began sending her cruel messages. Further investigation revealed that it was not a boy at all, but a grown woman, Lori Drew, a classmate's mother. Drew later claimed that she only wanted to know if Meier had been gossiping about her daughter online.[16]

This kind of behavior, however, is an exception to the rule. The majority of people do not abuse anonymity online; instead, they enjoy anonymity in order to augment their real life in some way. There are advantages to anonymity; in particular anonymity allows the comfortable public expression personality or beliefs. Considering the advantages of anonymity, a misuse of the terms of service of a website or evidence of a mean spirit should not be grounds to entirely do away with the privilege of anonymity.[17] Mattathias Schwartz expands on this idea in a piece for *The New York Times Magazine*,

---

[16] Schwartz.
[17] Nancy Baym, *Personal Connections in the Digital Age*, (Malden, Massachusetts: Polity Press, 2010), 71.

> The difficulty is tracking down the perpetrators. In order to prosecute, investigators must subpoena sites and Internet service providers to learn the original author's IP address, and from there, his legal identity. Local police departments generally don't have the means to follow this digital trail, and federal investigators have their hands full with spam, terrorism, fraud and child pornography. But even if we had the resources to aggressively prosecute trolls, would we want to? Are we ready for an Internet where law enforcement keeps watch over every vituperative blog and backbiting comments section, ready to spring at the first hint of violence?[18]

Schwartz's (sage) answer is 'probably not', which I myself echo. It is important to remember that trolls, Anonymous, and /b/ are all memes: they snapshots of contemporary culture, and in case, snapshots of contemporary culture covered by a Guy Fawkes mask. As iterations of contemporary culture, these groups should be regarded as more than a bunch of bullies and considered as reflections of broader values; anonymity should not be the scapegoat for general bad behavior. So, however much anyone can ignore adults who emotionally attack adolescents, we should try, because something bigger is going on. What is the appeal of being anonymous, with a lowercase 'a'? And what of Anonymous proper, Anonymous with an uppercase 'A', the focus of this paper?

Thesis Statement & Overview

In the video "I Am One Anonymous," published on YouTube in July 2011 under a Creative Commons license, a self-identified Anon says,

> Hello Internet, I am One Anonymous. Anonymous is a collective of individuals united by an awareness. We promote the truth, promote free speech, stand up against human injustice, we fight corrupt corporations and protest governments who bastardize freedom… As one Anonymous, I question the solidarity of many reports stated back when Anonymous was young, emerging from 4chan /b/ in 2003 and spreading across the web. The infancy of Anonymous was wild, we were malicious hackers, we were frauds. We reportedly stole people's identities and used them for lulz. We attack racism; we brought a pedophile to justice; we stopped the abuse of a defenseless cat; we cyberattacked credit card companies. The name of Anonymous

[18] Schwartz.

> was known by the childish crimes and videos of many, but, to one Anonymous, all of this has become trivial.[19]

Today, Anonymous is a brand; Anonymous is not an 'online hate machine', it is the free speech vanguard of the 21st century. Or is it? The good that Anonymous has done, according to One Anonymous, outweighs the bad; Anonymous' higher moral ground today trivializes the 'wild infancy' of the group. As One Anonymous notes, there are many incarnations of Anonymous: Anonymous the vicious hacker; Anonymous the vigilante; Anonymous the cyberterrorist; Anonymous the freedom fighter. The group is notoriously hard to pin down because it intentionally cloaks itself in mystery. Furthermore, by virtue of being anonymous, there is no way to know what the Anonymous membership is really like. Gabriella Coleman, hacker anthropologist and McGill University professor notes that all the operations are sociologically distinct from one another: They were organized on different IRC networks and initiated largely by a different group of people.[20]

The hive mind, also known as collective consciousness, is the set of beliefs and attitudes that a group shares. It is also a type of shared awareness, defined by Clay Shirky a prominent author and commentator on the effects of the internet on society, as, "the ability of many different people and groups to understand a situation, and to understand who else has the same understanding…Shared awareness allows otherwise uncoordinated groups to begin to work together more quickly and effectively."[21] The hive mind's shared awareness, then, can be a tool to efficiently realize change because the multitude of voices amplifies the message. Do the words of One Anonymous overly romanticize the hive mind made up of thousands of anonymous users? One Anonymous' message

---

[19] FLSnag, "I Am One Anonymous," *Youtube*, July 23, 2011, http://www.youtube.com/watch?v=aEcvaoDIKtU (accessed March 5, 2012).
[20] Gabriella Coleman, "From the lulz to collective action," *The New Everyday*, April 6, 2011, http://mediacommons.futureofthebook.org/tne/pieces/anonymous-lulz-collective-action (accessed March 6, 2012).
[21] Clay Shirky, *Here Comes Everybody* (New York: Penguin Press, 2008), 163.

betrays unmitigated support for Anonymous—it claims that Anons trivial past should not tarnish its reputation today—because today, today Anonymous fights for freedom.

However, it is still important to recall that Anonymous *is* the hive mind; it is everyone and no one; it is a leaderless, amorphous group with imprecise membership subject to the caprice of whoever moderates the IRC channel. This background explains Anonymous' lulzy past, but can it really account for their alleged hacktivist present? Hacktivism, a portmanteau of 'hacker' and 'activism', is the use of computer networks for social or political ends. Hacktivism is just one example of how the tools of virtual trickery send the tangible world into a moral panic.
The lulz are a corruption of 'lol', an acronym for laugh-out-loud. A troll usually has the lulz and entertainment at someone else's misfortune.

Instead of trying to define Anonymous or suggest a 'why' for Anonymous, this thesis asks the question: what exactly is Anonymous doing? The birth of Anonymous is not like the Birth of Venus; Anonymous did not rise from the depths of the internet fully developed as Venus did from the sea. Anonymous emerges from a rich hacker culture and history; the rhetoric of Anonymous is reminiscent of the hacker ethic, founded on the principles of access, free information, and improving the quality of life, that developed in the '80s and '90s alongside the rise of personal computing. Like Anonymous, the hacker ethic has undergone numerous transformations since its inception. There are a number of debates going on today about Anonymous and its offshoots, LulzSec and AntiSec, chief among them: are their actions ethical? And, if they are not, what should be done about it?

Steven Mansfield-Devine, freelance journalist specializing in information security and editor of *Network Security*, writes, "most Anons are driven more by a desire for some anarchic cyber-fun

rather than any ideological conviction,"[22] Mansfield-Devine assumes that cyber-fun and ideological conviction are mutually exclusive, and thus concludes that Anons and Anonymous actions are of little consequence. However, I will argue that 'anarchic cyber-fun' and ideological conviction are not mutually exclusive and that both Anons and hacktivism should be taken very seriously because they do have real consequences.

Though many Anons do pursue anarchic cyber-fun, 'the lulz', to reduce all of Anonymous to anarchic cyber-fun alone is to discredit the importance of operations like Project Chanology, Operation Tunisia, Operation Egypt, and Operation Avenge Assange, all purportedly launched to protect free speech and dissidents everywhere. However, it is equally presumptuous to assume that, "Anonymous itself has 'come of age', transitioning from 'cyberpranksters' to full-blown 'hacktivists'",[23] as Angela Daly asserts. Any analysis of Anonymous requires a nuanced approach because even though the press releases say 'we', Anonymous is a collective of individuals and all views expressed reflect only a subset of the whole. Therefore, if membership drastically shifts, the hive mind's consciousness and spirit will as well. Anonymous' structure, dynamism, and aggressive actions make it indisputably a force to be reckoned with online, but it is not immediately obvious what the consequence of their operations is outside of the virtual world.

The remainder of Chapter 1 will discuss Anonymous' history and origins. In Chapter 2, I will discuss the structure and potential of the internet and challenge the supposition that the real and virtual worlds are entirely distinct. The two spheres are in fact complementary, and a discussion of the development and deterioration of the hacker ethic will show how online actions have very real

---

[22] Steven Mansfield-Devine, "Anonymous: serious threat or mere annoyance?" *Network Security*, Volume 11, Issue 1 (January 2011): 8.

[23] Angela Daly, "Private power and new media: the case of corporate suppression of WikiLeaks and its implications for exercise of fundamental rights on the Internet," (paper presented at the 4th international conference on Information Law, ICIL 2011, Thessaloniki, Greece, May 20-21, 2011), 13.

ramifications. Chapter 3 discusses Anonymous Operations (AnonOps) in light of Mansfield-Devine's assertion that Anons are driven by anarchic cyber-fun and not ideological conviction. Anonymous vigilante acts and Project Chanology will show that trolling is an expression not just of the lulz, but of principles too. The chapter will close with a discussion of different reactions to Anonymous praxis and principles. While some may place Anonymous somewhere on the hacktivism – cyberterrorism continuum, I argue that it is not only more appropriate, but more fruitful to instead consider AnonOps as 'use' and 'misuse' of the internet. Chapter 4 will examine specific AnonOps, specifically Operation Payback, Operation Avenge Assange, Operation Tunisia, Operation Egypt, Operation BART, and the hack on HBGary Federal, and their consequences. Chapter 4 will show that AnonOps do have real and important consequences. The final chapter asks the question: in light of all of this information, what should be done about groups like Anonymous? Lately, individuals, the media, and national governments have begun to pay great attention to Anonymous, but it is not clear that legislative action is the right reaction to AnonOps, especially considering the importance of internet freedom and of the free access to information.

In *Anonymous: From the Lulz to Collective Action*, Gabriella Coleman quotes an Anon, " 'I came for the lulz but stayed for the outrage'," [24] he says, wearing a Guy Fawkes mask and protesting against the Church of Scientology. Anonymous is one part troll, always in it for the lulz, but it is one part social and political conscious. This thesis will elucidate what inspired outrage within the Internet super-consciousness—and what they did about it.

[24] Coleman, "Anonymous: From the Lulz to Collective Action."

"/b/ will melt your brain"

Anonymous surfaced from the underbelly of the internet, the random board /b/ on website 4chan.org. /b/'s content is random so long as random means pornography—both the conventional and the avant-garde—, sexism, homophobia, and trolling with the intermittent nonsensical story or picture. One blogger describes /b/ as:

> A subset of 4chan, technically a "random image board," where completely anonymous — no login, no username — people try to shock, entertain, and coax free porn from each other. Encyclopedia Dramatica calls it the asshole of the Internet… /b/ has no rules; pretty much the only thing guaranteed to get a user banned is child porn, and even that gets constantly joked about. Reading /b/ will melt your brain, but sometimes you need that. It's like how I can't start a rough draft without a beer, but the analogy works better with heroin mixed with fiberglass.[25]

Of all the boards on 4chan.org, /b/ is the most well known as a haven for trolls. Trolling is a way of provoking strangers online; sometimes individuals do it by 'flaming', or posting blatantly incendiary comments on a forum or website. Trolls will also naïve questions to see who will take the bait, thus revealing themselves as a 'newbie' in the community. The goal of trolling is to embarrass the other person because they fell for the trick—online this usually means that the troll sits calmly and the victim types viciously and brutishly in caps lock. Schwartz quotes a guide to trolling, "If you don't fall for the joke, you get to be in on it."[26]

So what is Anonymous? No one really knows. In a 2008 letter to the public Anonymous writes: "We are the concerned public; facing a menacing threat from within. To use political terminology, we are a de-centralized grass-roots organization with members world-wide. We are not

[25] Nick Douglas, "What The Hell Are 4chan, ED, Something Awful, And 'b'?" *Gawker*, January 8, 2008, http://gawker.com/346385/what-the-hell-are-4chan-ed-something-awful-and-b (accessed 8 March 2012).
[26] Schwartz.

terrorists, we are not unruly upstarts."[27] Vanessa Grigoriadis describes the hacktivist collective in *Vanity Fair* as, "nobody and nothing and nowhere;"[28] Peter Ludlow, philosophy professor at Northwestern University, describes Anonymous' home 4chan as, "rowdy, transgressive, and scatological;"[29] Chris Landers of the *Baltimore City Paper* writes, "Anonymous is a phenomena…. [it is] the first internet-based superconsciousness;"[30] and Coleman settles for "ultra-coordinated motherfuckary."[31]

The website 4chan.org, an online imageboard, was launched in 2003 by Christopher Poole, better known by his handle 'moot', when he was only 15 years old. When Poole launched 4chan.org, he had intended to create a community similar to the Japanese 2chan.org where users congregated to discuss Japanese comics and anime. When Poole downloaded their publicly available code and launched 4chan.org, however, he started something much different. 4chan is unique among online communities because users do not have to register an account in order to read without participating, also known as lurking, or post on the various boards, which are organized by interest. 4chan also does not keep any information about its users. Poole says, "We began to see anonymity not just as an aspect or feature, but as a thing, as a principle, as an idea that we are one, we are a collective, we are Anonymous. People then came to the site who not only saw Anonymous as a principle, but started

---

[27] TheRealGothAlice, "I am Anonymous", January 29, 2008, *Youtube,* http://www.youtube.com/watch?v=WvPUxMZZiX0&feature=related (accessed December 9, 2011).
[28] Vanessa Grigoriadis, "4chan's Chaos Theory," *Vanity Fair*, April 2011, http://www.vanityfair.com/business/features/2011/04/4chan-201104 (accessed March 8, 2012).
[29] Peter Ludlow, "WikiLeaks and Hacktivist Culture," *The Nation*, October 4, 2011, 26.
[30] Chris Landers, "Serious Business: Anonymous Takes on Scientology (and Doesn't Afraid of Anything), *City Paper*, April 2, 2008, http://www2.citypaper.com/news/story.asp?id=15543 (accessed March 8, 2012).
[31] Gabriella Coleman, "Anonymous: From the Lulz to Collective Action."

to exploit anonymity as a new platform where they could be rebellious and no one knew who they were."[32] Currently, 4chan has 10 million users and 53 unique boards that users post on.

The 4chan 'culture' is amalgamation of different memes and cultural interests. The site seems foreign, but the content actually rings familiar to many, especially young people. Grigoriadis writes:

> If 4chan sounds trivial, that's because it is…In fact, you could say that 4chan has cornered the market on the trivial on the Internet, which is no small feat (the trivial usually spreads by accident on the Web, according to no logic.) Through the sheer force of its numbers, 4chan has somehow managed to establish the Internet's top memes—some of which are as important to the American consciousness at this point as Hollywood movies, and they've done it over and over.[33]

/b/tards are responsible for Lolcats, maybe the internet's most widely recognized meme. On 'Caturday', people used to post pictures of cats with cat-speak captioned in robust impact font; one user parlayed 'Caturday' into the notorious icanhazcheezburger.com where cats are not cats but 'kittehz' and they do not eat, they 'eated'. 'Rickrolling', the trick where a seemingly innocuous link redirects you to a video of Rick Astley's 'Never Gonna Give You Up', originated on /b/ as well. /b/tards rigged an online poll where Justin Bieber fans could vote on where he should visit on his world tour. Thanks to /b/tards and trolls worldwide, North Korea came in second to Israel; Beliebers cannot be thwarted.[34] 4channers also voted Poole to the number one spot in a Victoria's Secret beauty contest in 2009; the lingerie company disqualified him as a candidate.[35]

---

[32] Interview with Christopher 'Moot' Poole quoted in Aleks Krotowski, "The internet's cyber radicals: heroes of the web changing the world," *The Guardian*, November 27, 2010, http://www.guardian.co.uk/technology/2010/nov/28/internet-radicals-world-wide-web (accessed October 25, 2011).
[33] Grigoriadis.
[34] Grigoriadis.
[35] Sean Ridgely, "Gabe Newell and Christopher Poole ousted from Victoria's Secret beauty contest," *Neoseeker*, August 27, 2009. http://www.neoseeker.com/news/11654-gabe-newell-and-moot-ousted-from-victorias-secret-beauty-contest/ (accessed December 12, 2011).

When 4chan started, the majority of its users posted under the handle 'anonymous' by default. Seeing as each unique user was 'anonymous', the voice that emerged from 4chan seemed unanimous. The community that developed expressed the collective will, but only the ephemeral collective will. Everyone was equally anonymous and Anonymous, whether they had been there one year or one day or one hour. Membership is completely fluid, and so is memory on 4chan, which does not keep archives and has no search function, Vanessa Grigoriadis calls it "one of the last places on the Internet where you can really say anything you want and it won't come back to haunt you."[36]

A brief & incomplete history

The online collective has done some 'spectacularly stupid things'[37] while in pursuit of the lulz, but it has also been a politically active and socially relevant online collective with a proclivity for disruption. Even though Anonymous proper has, for the most part, left their /b/tard past behind, the collective it still inextricably linked to its troll legacy.

Coleman cites Operation Chanology, launched in 2008 against the Church of Scientology, as the political turning point for the group. In February 2008 after the church had tried to censor the internet, demanding that a leaked propaganda video be taken down, the Anonymous raid began: Anons flooded the church's offices with black faxes to waste toner, tied up phone lines, and as always, launched a distributed denial of service (DDoS) attack on their website. Anons even came out in person in Washington, DC to protest the church's practices and alleged violations of human rights. The physical protests mark the beginning of the iconic Guy Fawkes Anonymous mask—

[36] Grigoriadis.
[37] Joseph Menn, "They're watching. And they can bring you down," *The Financial Times*, September 23, 2011, http://www.ft.com/intl/cms/s/2/3645ac3c-e32b-11e0-bb55-00144feabdc0.html#axzz1gBiwxVlN (accessed December 9, 2011).

chosen for no reason besides the fact that it was the cheapest and most accessible mask available to preserve their anonymity.[38] Only a year before, however, Anonymous had offensively trolled Habbo, an online social networking site designed as a virtual hotel. Anons showed up on the site as identical avatars, all black men with Afros in gray suits, and blocked access to the hotel pool because it was 'full of AIDS'; they also formed swastika-like formations on the property and posted various indecent and absurd internet sayings.[39] When the group was banned from Habbo they called racism. Attacks like the one against Habbo encourage people to take Anonymous actions with a grain of salt, but subsequent operations showed that Anonymous was in fact promoting a serious agenda.

Since about 2010 Anonymous has been running Operation Payback. It was originally part of a protest against the software company that Bollywood companies hired to take down piracy websites hosting illegal content; the operation grew into an attack against the Motion Picture Association of America (MPAA) and snowballed to DDoS attacks on other websites and February 2012's Stratfor hack is another continuation of Operation Payback. The basic anatomy of an Anonymous raid is to do nothing except disrupt service; the only goal is to troll: raids should be as frustrating, attention grabbing, and infuriating as possible. Anyone is free to download the low orbit ion cannon (LOIC) which turns the user's computer into a war machine—if you accept that overloading a website with hits and disrupting service is tantamount to war, and some do. Operation Avenge Assange, the Anonymous response to the corporate reaction to WikiLeaks, is an extension of Operation Payback. In Operation Avenge Assange, Anons effectively shut down PayPal, MasterCard, and Visa websites after they froze WikiLeaks accounts—PayPal did eventually release

---

[38] Gabriella Coleman, "Hacktivism, Vigilantism, and Collective Action in the Digital Age" (panel discussion at The Brookings Institution, Washington, DC, December 9, 2011), 28.
[39] Ryan Single, "Palin Hacker Group's All-Time Greatest Hits," *Wired*, September 19, 2008, http://www.wired.com/threatlevel/2008/09/palin-hacker-gr/ (accessed March 20, 2012).

WikiLeaks's funds. Operation Avenge Assange is filled with rhetoric about the right to free speech; press releases make Anons sound like masked crusaders for justice in a wholly unjust world:

> **On the Internet, the only jury is that of the people. Anonymous has kept a watchful eye, and has decided that MasterCard's actions are unacceptable.**
>
> The free exchange of ideas and informaiton, no matter how inconvenient, is never illegal. Wikileaks has not acted in violation of law, and has won all prosecutions so far. MasterCard's and PayPal's words ring hollow, but their actions are obvious—**to punish WikiLeaks, most likely at the behest of the United States government.**
>
> **Punishing WikiLeaks because it has distributed information which embarrasses the powerful is a disgrace to the internet, and we will not accept it.**
>
> **ANONYMOUS IS LEGION.**
> **WE DO NOT FORGIVE. WE DO NOT FORGET.**
> **EXPECT US.**[40]

Despite press releases and costume and rhetoric, it is still difficult to speak about Anonymous, its message, or its goals, because it is not a cohesive group. There is no single membership base for Anonymous; it is fluid and changes daily. However the amorphous and anarchic nature of Anonymous is one of its strengths, and really, it makes Anonymous unbeatable because there is no clear place to strike. In the months after Operation Avenge Assange, the FBI arrested 16 people and more were arrested globally, but Anonymous' activities did not subside. If anything, the Anonymous voice has become louder.

Before Operation Avenge Assange, Anonymous had played an active role in the Arab Spring, DDoSing government websites and helping dissidents circumvent online censorship. In early 2011 Anonymous embarrassed the CEO of HBGary Federal, Aaron Barr, releasing his personal email correspondences and private documents relating to HBGary, pillaging their data, and vandalizing

[40] "MasterCard Manifesto," *Pastebin*, December 9, 2010, http://pastebin.com/AjVL9dNY (accessed April 1, 2012).

their webpage.[41] In August of 2011 Anonymous hacked and d0xed, or released private documents hackers mined from the San Francisco Bay Area Rapid Transit Service (BART) when cellphone service was disrupted in stations in response to reports of planned protest in reaction to the fatal shootings of a few passengers by transit officers. Throughout the fall of 2011 the Anonymous voice rang loud and clear during the Occupy Movement that inspired global protest. And since January 2012, the Anonymous voice has only resounded more loudly and resonated more strongly.

———

Many are quick to dismiss information coming from the internet as specious; we believe online representations are suspect—then Anonymous has to be irrelevant then, right? Steven Mansfield Devine dismisses the collective, writing, "And while Anonymous clearly has some degree of central control, even a little time spent in the IRC channels is enough to convince you that trying to organize Anons is like herding cats."[42] Generally speaking, we have drawn a bright line between what is virtual and what is real, and the bright line is determined by whether or not the information, interaction—what have you—is mediated by a screen. However, consider the Megan Meier story; the so-called 'virtual' world is not really virtual at all. The virtual and the real worlds are closely related, one always influencing, challenging, and changing the other.

There will always be people who believe online communities as unimportant or trivial. It is easy to think that online actions have no real-world consequences; after all, what exactly happened after Anonymous attacked Visa and MasterCard after WikiLeaks? Bradley Manning is, after all, still in jail. The United States Federal Bureau of Investigation and other security organizations still

[41] Peter Bright, "Anonymous speaks: the inside story of the HB Gary attack," *Ars Technica*, Spring 2011, http://arstechnica.com/tech-policy/news/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack.ars (accessed March 25, 2012).
[42] Mansfield-Devine, "Anonymous: serious threat or mere annoyance?" 8.

arrested the hackers that they could, targeting the assumed upper echelons of Anonymous. And the FBI kept going: in the beginning of March, Sabu, real name Hector Xavier Monsegur, suspected ringleader of Anonymous and its offshoot LulzSec, was arrested and outed as having been an FBI informant for months.[43] It is worth it to scrutinize statements like Mansfield-Devine's because, whether or not organizing Anons is like herding cats, the group is far from inconsequential.

Anonymous and its offshoots AntiSec and LulzSec can access and leak our information, crash our favorite websites, and disrupt our daily lives—they deserve our attention. Earlier I said that this paper would take a look at what inspired rage in the hacktivist collective and what Anons did about it; in addition, I also plan to explain just what exactly this behavior and activity means for the rest of us and not just whether we should care, but why we should care.

[43] Jana Winter, "EXCLUSIVE: Unmasking the world's most wanted hacker," *Fox News*, March 6, 2012, http://www.foxnews.com/scitech/2012/03/06/exclusive-unmasking-worlds-most-wanted-hacker/ (accessed March 13, 2012).

CHAPTER 2

The Promise of Open Networks

The internet: a generative platform

In 1958 the United States Department of Defense introduced a special agency, the Advanced Research Projects Agency (ARPA), intended to foster innovation in science and technology. ARPA "was founded in response to the surprise Sputnik launched in 1958 and fathered the Internet somewhere along the way."[44] On September 2, 1969, four ARPA engineers at the University of California, Los Angeles, made the first network connection between computers, creating Arpanet; by 1973, Bob Kahn and Vint Cerf had designed Transmission Control Protocol and Internet Protocol (TCP/IP), the basic tools for interconnecting networks, the foundation of the internet. In a 2008 interview with *Vanity Fair* Cerf says, "We absolutely knew what could happen if our work was successful. We knew about the mobile possibilities. We knew about satellite. We had some idea of how powerful this was,"[45] Cerf is now an executive at Google, 'chief Internet evangelist'.[46] Less than twenty years later, the European Organization for Nuclear Research (CERN), one of the largest physics laboratories in the world, launched the World Wide Web[47] and by 1994 there were more than 10,000 unique web servers and 10 million users.[48]

The network was developed in universities by scientists and scholars whose primary motivation was information sharing. The network is open; researchers and engineers evidenced little

[44] DARPA, www.darpa.mil (accessed December 2, 2011).
[45] Keenan Mayo and Peter Newcomb, "How the Web Was Won: An Oral History of the Internet," *Vanity Fair*, July 2008, http://www.vanityfair.com/culture/features/2008/07/internet200807?currentPage=1 (accessed December 2, 2011), 3.
[46] Mayo and Newcomb, 2.
[47] The World Wide Web is specifically a network of interlinked documents accessible through the Internet; the Internet, in contrast, is a 'network of networks', connecting various computer networks via TCP/IP.
[48] "How the Web Began," European Organization for Nuclear Research (CERN), http://user.web.cern.ch/public/en/About/WebStory-en.html (accessed December 2, 2011).

interest in controlling the structure of the network itself or in controlling how anyone else used the network. Designers rejected traditional hierarchical decision-making and instead made decisions by consensus; protocols of the network stayed relatively open in order to limit restrictions on future engineers and promote as much innovation as possible. Jonathan Zittrain, author of *The Future of the Internet—And How to Stop It*, writes,

> The point of building the network was not to offer a particular set of information or services like news or weather to customers, for which the network was necessary but incidental. Rather, it was to connect anyone on the network to anyone else. It was up to the people connected to figure out why they wanted to be in touch in the first place; the network would simply carry data between the two points.[49]

One of the most notable and revolutionary things about the network is that it welcomes unprecedented levels collaboration and creativity because it allows for rapid communication despite geographical distance. The network was designed to be open because its primary role was and still is facilitating information sharing and collaboration between people, not to regulate users. [50]

The actual value of the internet is not the physical network of connections between machines, but the still unrealized potential of said network connections. The network connects machines and the people behind machines: the internet is a network of wires, it is also a network of code, but most importantly it is a network of ideas. Zittrain calls the internet a *generative* technology, that is, one that has multiple uses that have yet to be realized or conceived. Generative technologies are platforms for other innovations; consider the adaptability of the PC compared to that of the iPhone. Anyone can write, run, and share code for a PC, but you cannot even open an iPhone and look at the inside of it. Change and development on a PC are user-driven; change and development on an iPhone are Apple-driven. Zittrain calls the iPhone and similar technologies appliances; they are

---

[49] Jonathan Zittrain, *The Future of the Internet—And How to Stop It* (New Haven: Yale University Press, 2008) 27.
[50] Barry M. Leiner, et. al., "Brief History of the Internet," *Internet Society*, 2011 http://www.internetsociety.org/internet/internet-51/history-internet/brief-history-internet (accessed March 15, 2012).

tethered technologies, "Whereas on a PC any user can write and share code in ways the manufacturer never imagined, on a tethered technology the consumer must use the product in the way specified by the manufacturer."[51] Anyone can design an application for the iPhone, but Apple has to approve it. There is no such central control over the internet.

The internet is revolutionary because it transforms how people share and receive information and because it transforms how people relate to each other. It is a collection of technological innovations and of communities. The technology has already transformed information sharing and interpersonal relationships, but by virtue of being generative technology the transformation is ongoing. Tim Berners-Lee, computer scientist, Massachusetts Institute of Technology professor, and inventor of the World Wide Web writes in *Weaving the Web*:

> If we end up producing a structure in hyperspace that allows us to work together harmoniously, that would be a metamorphosis. Though it would, I hope, happen incrementally, it would result in a huge restructuring of society. A society that could advance with intercreativity and group intuition rather than conflict as the base mechanism would be major change.[52]

Weaving the Web was published in 1999, before personal computers and internet access was as ubiquitous as it is today. Nearly 15 years later, it is fair to say that such an interactive community already exists online. In *Here Comes Everybody*, a book about the effect of the internet on group dynamics and organizing, author Clay Shirky discusses the interactive community that does exist online. The internet is home to infinite common-interest groups—infinite hive minds—that provide the social support and sense of belonging that many people desire. The popularity of online communities, however, does not mean that similar communities have ceased to exist in the real

---

[51] Jonathan Zittrain, "Glossary," *Future of the Internet,* http://futureoftheinternet.org/glossary (accessed March 18, 2012).
[52] Tim Berners-Lee, *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by its Inventor* (New York: Harper Collins, 1999), 206.

world. Cyber, or hyperspace, communities and real world communities complement each other. Shirky observes, "The idea of cyberspace made sense when the population of the internet had a few million users; in that world social relations online really were separate from offline ones…these worlds would rarely overlap."[53] However, today, in developed countries the majority of people are online and there is considerable overlap between online and real connections. It is difficult to say if there has been a 'huge restructuring of society' but it is fair to say that society is restructuring itself incrementally and that, "Instead of becoming a separate cyberspace, our electronic networks are becoming deeply embedded in real life."[54]

As Shirky discusses, the real and virtual worlds are not all that separate anymore. However, it is still very easy to slip back into the mindset that the real and the virtual are incompatible like oil and water. A hacker's online social capital cannot possibly be translated into real social capital, can it? Manuel Castells writes in his epilogue to *The Hacker Ethic*,

> While individual experiences may exist outside this hypertext, collective experiences and shared messages—that is, culture as a social medium—are by and large captured in this hypertext. It constitutes the source of real virtuality as the semantic framework of our lives. Virtual, because it is based on electronic circuits and ephemeral audiovisual messages. Real, because this is our reality, since the global hypertext provides most of the sounds, images, words, shapes, and connotations that we use in the construction of our meanings in all domains of experience.[55]

Castells reminds readers that technology and the web are integral parts of contemporary culture and that both are important parts of everyone's life. It is almost impossible to escape their reach because even those remote, isolated corners of the globe come to be digitized in photography, a blog post, or just a few typed notes. With so much of the world digitized, it is increasingly easy for social capital to move between the real world and hyperspace.

---

[53] Shirky, 195.
[54] Shirky, 196.
[55] Manuel Castells, epilogue to *The Hacker Ethic* by Pekka Himanen (New York: Random House, 2001), 170.

Consider the stock image of the internet addict. We generally imagine him to be someone relatively young, almost always male, probably unshowered, and wearing a flannel that Kurt Cobain would be jealous of. He sits in a dark basement, probably at his mother's house, surrounded by empty Big Gulps and bags of Cheetos. He might only consider himself an internet enthusiast. He has intimate knowledge of online subculture. We assume that he goes to sleep around dawn, not to wake until dinnertime, and that he rarely leaves the house. We expect him to be mischievous and poorly socially adjusted. We might assume that he is a hacker—if we do, we expect him to act with impunity. We imagine the hacker as vanguard, rogue, visionary, or all three. We expect a lot of the hacker though we cannot see him and really, we do not know anything about him. There is a stock image of the hacker, but we only need to consult the famous *New Yorker* cartoon to realize that the hacker can actually be anyone—even a dog.

We expect a lot of the hacker and, for the most part, we expect negative things. The hacker might have positive online social capital but when it gets converted to real social capital, he certainly isn't left with much.[56] The hacker probably isn't a dog—and he probably isn't malicious or maladjusted either. Hackers and zealous internet users are easily discounted even though their skillset and knowledge base are more relevant to the real world than many realize or imagine. This chapter will first define and discuss the hacker ethic and its eventual deterioration. Second, this chapter will explore troll culture. Finally, the chapter will show how hacker and troll culture pose a threat to today's information economy.

[56] David Auerbach, "Anonymity as Culture: Treatise," *Triple Canopy*, Issue 15, February 9, 2012, http://canopycanopycanopy.com/15/anonymity_as_culture__treatise (accessed March 18, 2012).

The Hacker Ethic

In the 1970s, when the term was first used, a hacker was an individual with exceptional programming abilities. Today, the definition varies; elite hackers, those with programming skills, are thought of as criminals with malicious desires to access and compromise computers and entire networks.[57] However, hacking does not require technical expertise; Robert Bickford, a 'cyberspace futurist', defines a hacker as "any person who derives joy from discovering ways to circumvent limitations."[58] Hacking, above all, is a mindset; it is curiosity and an interest in making things work better. The hacker ethic also places the individual at the center, not because hacking is solitary, but because the individual is important and should be afforded every opportunity to realize eudemonia however he or she wishes. Himanen writes, "The hacker ethic also reminds us, in the midst of all the curtailment of individual worth and freedom that goes on in the name of 'work,' that our life is here and now."[59]

The 'hacker ethic' is a turn of phrase first coined by Steven Levy, tech journalist and senior writer at *Wired*, in his book *Hackers: Heroes of the Computer Revolution*. Levy's six planks of the hacker ethic are:

1. First, access to computers should be unlimited and total: 'Always yield to the Hands-On Imperative!'
2. Second, all information should be free.
3. Third, mistrust authority and promote decentralization.
4. Fourth, hackers should be judged by their prowess as hackers rather than by formal organizational or otherwise irrelevant criteria.
5. Fifth, one can create art and beauty on a computer.
6. Finally, computers can change lives for the better.[60]

---

[57] Jim Thomas, "The moral ambiguity of social control in cyberspace: a retro-assessment of the 'golden age' of hacking," *New Media Society* 7: 599 (2005): 602.
[58] Robert Bickford, "Are You a Hacker?" 1989, http://www.textfiles.com/hacking/hacker.txt (accessed March 18, 2012).
[59] Himanen, 40.
[60] Steven Levy quoted in Thomas, 606.

The Hacker Ethic, a small volume written by Himanen, a philosopher, elaborates on the hacker ethic, contrasting it with the Protestant work ethic before Himanen finally identifies seven hacker values of his own. The book also has contributions from sociologist Manuel Castells, who writes an epilogue on the 'information age', and a prologue written by Linus Torvalds, creator of the Linux free operating system. According to Himanen, the modern Protestant work ethic places work at the center of our lives; work is represented as a good in and of itself with no regard for personal development or passion.[61] The idea of 'work' as inherently valuable goes against Linus's Law, named for Torvalds, which says that, "All of our motivations fall into three basic categories. More important, progress is about going through those very same things as 'phases' in a process of evolution, a matter of passing from one category to the next. The categories, in order, are 'survival,' 'social life,' and 'entertainment'."[62] Social life, writes Torvalds, is essentially social ties such as family, friends, country, or religion; they are all motivations for which people would be willing to risk their life. Entertainment, "is something intrinsically interesting and challenging,"[63] it is whatever leisure activities we pursue in order to avoid boredom. For some, it is just watching TV. For others it is playing chess or a video game, but for scientists, research could be entertainment—all entertainment is not guaranteed to be universally amusing. For hackers, the computer is now the source of social life and entertainment. Torvalds writes,

> That is how something like Linux comes about…The reason that Linux hackers do something is that they find it to be very interesting, and they like to share this interesting thing with others. Suddenly, you get both entertainment from the fact that you are doing something interesting, and you also get the social part. This is how you have this fundamental Linux networking effect where you have a lot of hackers working together because they enjoy what they do. Hackers believe that there is no higher stage of motivation than that.

---

[61] Himanen, 9.
[62] Linus Torvalds, introduction to *The Hacker Ethic* by Pekka Himanen (New York: Random House, 2001), xiv.
[63] Torvalds, xv.

The hacker ethic puts enjoyment at the center of life instead of work or money. Money, writes Torvalds, is not a primary motivation, instead it is a substitute for the things we really want. Money is a means of survival, social life, and entertainment, but it is not an end in itself.[64]

Himanen describes seven values of the hacker ethic: passion, freedom, social worth, openness, the nethic—or Net ethic—activity, and caring. Why is passion specific to a hacker? Well, passion, as Himanen describes it, is inspired by "some intrinsically interesting pursuit that energizes the hacker and contains joy in its realization,"[65] some call it 'geeking out'.[66] Freedom, as part of the hacker ethic, reflects the "dynamic flow between creative work and life's other passions, within which rhythm there is also room for play."[67] In the book, Himanen talks about how money really does not motivate hackers—projects motivate hackers. Projects with social worth motivate hackers even more, and they enjoy keeping said projects 'open' so that others can enjoy and further develop what had so excited and inspired him or her in the first place. There is the assumption that hacking is a solitary, lonely activity, but hackers might actually be more social than the average person who is consumed by work because hackers labor to create something socially valuable—together.

The 'nethic', or Net ethic, is hackers' philosophy of the network, and it is motivated by values of activity and caring. Himanen explains,

> Activity in this context involves complete freedom of expression in action, privacy to protect the creation of an individual lifestyle, and a rejection of passive receptiveness in favor of active pursuit of one's passion. Caring here means concern for others as an end in itself and a desire to rid the network society of the survival mentality that so easily results from its logic. This includes the goal of getting everybody to participate in the network and to benefit form it, to feel responsible for longer-term

[64] Torvalds, xv.
[65] Himanen, 139.
[66] Ito, et al., *Living and Learning with New Media: Summary of Findings from the Digital Youth Project*, (Chicago, Illinois: The MacArthur Foundation, 2008).
[67] Himanen, 140.

> consequences of the network society, and to directly help those who have been left on that the margins of survival.[68]

Do all hackers prescribe to this hacker ethic, exactly? No, of course not. But, many hackers—whether they are computer hackers or others—identify with its basic principles. The hacker ethic, ideally, promotes openness and free information; the hacker ethic, "is a challenge to our society and to each of our lives,"[69] and it encourages tinkering that catalyzes progress and inspires change that no one expected.

The hacker ethic described is exemplary of the 'golden age' of hacking, which coincided roughly with the rise of personal computing in the 1980s, lasting until 1990. In 1987 Apple Computer released the Apple II, designed by Steve Wozniak, who Levy lists as a 'true' hacker. The Apple II represented the hacker ethic because it was literally open. Anyone could lift up the hood, like a car, and tinker with the technology; anyone could reprogram it—experiment—and make it faster. The belief that computers and technology can make the world a better place sounds a little outdated today, because don't we most often hear that technology is making us dumber? More isolated? Lazier? In the 1970s when Wozniak was working on the computer and sharing it with the Bay Area's Homebrew computer club, that was not the case. Technology in the golden age of hacking was widely believed to bring unprecedented change for the good, " 'Everyone in the Homebrew Computer Club envisioned computers as a benefit to humanity—a tool that would lead to social justice'," Wozniak said.[70]

---

[68] Himanen, 140-1.
[69] Himanen, ix.
[70] Tim Wu, *The Master Switch*, (New York: Alfred A Knopf, 2010), 276.

The end of the 'golden age' of hacking

Hacking's 'golden age' could not last forever. The community of computer and Internet users was growing, and it was growing fast. It became harder to know if the hacker you were connecting with prescribed to the same ethic that you did. Jim Thomas, a sociology professor at Northern Illinois University, marks 1988 as the beginning of the end: computer science graduate student Robert Morris released the first computer worm online, immobilizing roughly 6,000 computers—an estimated 10% of all computers connected to the internet at the time. A computer worm is a type of malware that is self-replicating and, unlike a virus, does not need to attach itself to a specific program. Morris's program, though poorly programmed, was not created with bad intent; he claimed that he wanted to count the number of machines connected to the internet, not to disable them.[71] The worm, despite seeming innocuous, revealed the dark and destructive side of computer hacking when it forced the question: if this is what a computer science student could do by accident, what could he do on purpose? After the worm incident, the Internet Engineering Task Force released a 'request for comment' (RFC) document, RFC 1135, which concluded that it is important to promote and enforce an ethical standard, especially as new and inexperienced users signed on to the internet.[72] The security of the internet depended on a communal ethic that might have been disappearing.

The RFC however lacked any plan for implementation, which, upon further inspection, does make sense. Because there is no central control for the internet, there is no obvious way to enforce a universal ethical standard for network usage. Like other generative platforms, the internet is always being interpreted and reinterpreted and thus, will always be in beta. Unfortunately, because the

[71] Zittrain, 37.
[72] Zittrain, 37.

internet is forever incomplete it is also extremely vulnerable to attack. Zittrain discusses two philosophies that have directly contributed to both the vulnerability of the network and its supreme success: the procrastination principle and the trust-your-neighbor approach. The procrastination principle asserts that a problem with the network will be solved later and by someone else. Zittrain cites an engineering paper as an example, the paper says, "any features not universally useful should not be implemented, in part because not implementing these features helpfully prevents the generic network from becoming tilted toward certain uses,"[73] the procrastinators, therefore, are not just putting off the programming work, they are guaranteeing users freedom. Open networks allow for utmost creativity in design and for each user to tailor the network to his needs. The procrastination principle is in that respect another articulation of the hacker ethic. The second principle, the trust-your-neighbor approach based on trust, enables the procrastination principle. Internet architects and programmers did not need to secure the networks because they assumed users to be good-natured enough that they would not intentionally or carelessly disturb the flow of information across the network or to the computers at the network's endpoints.[74]

Overtime, the public has not proved itself to be so good-natured. Zittrain writes: "The idea of a Netwide set of ethics has evaporated as the network has become so ubiquitous. Anyone is allowed online if he or she can find a way to a computer."[75] The passage is tinged with panic: There is no ethic! The golden age is over! Not only are users less skilled now than they were during the golden age of hacking, but computers are much more powerful and the network more extensive; the potential damage of a virus or malicious user is greater than it was during the golden age, and it grows daily. A dystopian and hyperbolic interpretation of the end of the golden age of hacking

[73] Zittrain, 31.
[74] Zittrain, 31.
[75] Zittrain, 45.

means two things: first, malware is everywhere; second, users download and spread malware without realizing it. Zittrain claims that the ethic has 'evaporated'. However it is only the original hacker ethic of the golden age that has evaporated. A new ethic, characterized by trolling, anonymity, and activism, is emergent.

The new ethic, though, is unique: it is emerging in a completely different context from the one that inspired the original, productive hacker ethic. During the golden age, it was in everyone's interests to only produce good code, but now, "there is now a business model for bad code—one that gives many viruses and worms payloads for purposes other than simple reproduction."[76] Malware is not an expression of creativity or a test of cybersecurity, it is a business; malware makes money. Different types of malware, often viruses, harvest email addresses from users' address books for spam. They also harvest passwords and other sensitive information for profit.

In *Malwebolence: The Trolls Among Us*, Mattathias Schwartz investigates troll culture, the context of the new nethic. He describes imageboard /b/ as a "panopticon in reverse—nobody can see anyone, and everyone can claim to speak from the center,"[77] an appropriate metaphor to extend to today's nethic as well. The decline of the original hacker ethic and rise of this nebulous 'new' nethic means that we don't know what to expect from others online. By invoking the image of the panopticon, a circular prison with all cells and prisoners visible from a single post in the center, Schwartz taps into the insecurity of his readership. /b/ is still a prison, but users continue to evade surveillance. During the golden age of hacking, the fact that users, criminals in the metaphor, could remain anonymous and that each had equal voice was empowering because above all, it

[76] Zittrain, 45.
[77] Schwartz, "Malwebolence."

demonstrated that the internet was a unique and common space. But, since the fall of the golden age, it seems like anonymity does not connote individual security—anonymity undermines it.[78]

"Trolling is like internet eugenics."

"While reporting for this article," Schwartz writes in his piece for *The New York Times Magazine*, "I did everything I could to verify the trolls stories and identities, but I could never be certain. After all, I was examining a subculture that is built on deception and delights in playing with the media. If I had doubts about whether Fortuny was who he said he was, he had the same doubts about me."[79] *Malwebolence* was published in August of 2008, about two decades after the so-called 'golden age' of hacking. While Schwartz does prescribe to the standard demonization of the hacker, he also offers a surprisingly human profile of this group of people that enjoys ruining someone else's day.

The piece focuses on two prominent hackers, Jason Fortuny and a hacker who goes by the pseudonym Weev, both of whom Schwartz interviewed. Fortuny says that he is a "normal person who does insane things on the Internet,"[80] and he calls his trolling 'experiments'. In 2006 he launched "the Craigslist experiment'. Fortuny misrepresented himself in an ad as a woman looking for a 'str8 brutal dom muscular male.'[81] Over 100 men responded divulging personal information such as their real name, photograph, email address, physical address, and phone number, all of which Fortuny posted to his blog to 'expose' the men. In 2007, Fortuny's trolling was obscured by that of middle-aged woman, Lori Drew, who posed as a boy on MySpace and sent cruel messages to 13

---

[78] David Auerbach, "Anonymity as Culture: Treatise," *Triple Canopy*, Issue 15, February 9, 2012, http://canopycanopycanopy.com/15/anonymity_as_culture__treatise (accessed March 18, 2012).
[79] Schwartz.
[80] Schwartz.
[81] Schwartz.

year-old Megan Meier, one of her daughters classmates, resulting in her suicide. Days after the story went public, a blog "Megan Had It Coming" popped up. It had comments like, " 'Killing yourself over a MySpace boy? Come on!!! I mean yeah your fat so you have to what you can get but still nobody should kill themselves over it'," [82] and in the third comment, the author claimed to be Lori Drew herself. The blog was revealed to be another Fortuny experiment.[83]

The blog, Fortuny says, was meant "to question the public's hunger for remorse and to challenge the enforceability of cyberharassment laws like the one passed by Megan's town after her death," [84] and it only showed that the laws were unenforceable. Despite the fact that the county sheriff's department said it was investigating the identity of the fake Lori Drew, it never found or apprehended Fortuny. Furthermore, Fortuny is not convinced he even committed a crime. " 'What's he going to sue me for?' he asked. 'Leading on confused people? Why don't people fact-check where this stuff is coming from? Why do they assume it's true?'" [85] At some point during the interview, Schwartz asked Fortuny whether trolling hurt people, a question for which he had no solid answer. He replies:

> 'I'm not going to sit here and say, 'Oh God, please forgive me!' so someone can feel better…Am I the bad guy? Am I the big horrible person who shattered someone's life with some information? No! This is life. Everyone goes through it. I've been through horrible stuff too.'

In March of 2008 a group of trolls attacked the Epilepsy Foundation's Website, posting images with flashing lights and colors on forums. A few days later, more sophisticated trolls injected JavaScript into posts that would redirect users' browsers to seizure-inducing images.[86] Fortuny did not think

---

[82] Schwartz.
[83] Schwartz.
[84] Schwartz.
[85] Schwartz.
[86] Kevin Poulsen, "Hackers Assault Epilepsy Patients via Computer," *Wired*, March 28, 2008, http://www.wired.com/politics/security/news/2008/03/epilepsy (accessed March 18, 2012).

there was anything wrong with the attacks, "'Demonstrating these kinds of exploits is usually the only way to get them fixed.'"[87] According to Fortuny, attacks like the flashing gifs should be something the Epilepsy Foundation's website is able to protect itself form.

Weev, legendary troll and elite hacker, denounced the attack on the Epilepsy Foundation's website, calling it 'over the line': "'it's hacking peoples unpatched brains. we have to draw a moral line somewhere.'"[88] Weev, unlike Fortuny however, does not try to mollify online trolling by equating it to any standard social norms. He says to Schwartz,

> 'I hack, I ruin, I make piles of money…I make people afraid for their lives…Trolling is basically Internet eugenics. I want everyone off the Internet. Bloggers are filth. They need to be destroyed, Blogging gives the illusion of participation to a bunch of retards…We need to put those people in the oven!'[89]

Fast-forwarding about two decades since the golden age of hacking, we can see that the hacker ethic has deteriorated. Jon Postel, a computer scientist very influential in the creation and design of the internet, said with regard to internet protocol: "Be conservative in what you do; be liberal in what you accept from others,"[90] which is now known as Postel's Law. Postel's Law, meant to facilitate 'interoperability', that is, enable various computer systems to communicate with each other, has been dutifully exploited by hackers; consider the plethora of malware online today. As Weev's quotes indicate, modern day hackers and trolls do not prescribe to Postel's Law. Schwartz writes that instead, "Trolls embody the opposite principle. They are liberal in what they do and conservative in what they construe as acceptable behavior from others. You, the troll says, are not worthy of my understanding; I, therefore, will do everything I can to confound you."[91]

---

[87] Schwartz.
[88] Schwartz.
[89] Schwartz.
[90] Schwartz.
[91] Schwartz.

Trolling is often presented as a foreign concept, but as Gabriella Coleman writes in the *Social Text Journal*, trolls are not actually a new phenomenon. Trolls and hackers are the modern day incarnation of mythical 'tricksters' like the Native American coyote, Greek Hermes, the creole eshu spirits, or Norse Loki. Folklore paints tricksters as villainous for their unpredictability. For example, many are transformers that navigate the perils of their world using cunning and deceit. Tricksters may be things of literal myths, but there is certainly a certain mythos that surrounds hackers and trolls and augments the character they play.[92] Coleman writes,

> Many of these figures push boundaries of all sorts: they upset ideas of propriety and property; they use their sharpened wits sometimes for play, sometimes for political ends; they get trapped by their cunning (which happens ALL the time with tricksters! That is how they learn); and they remake the world, technically, socially, and legally and includes software, licensing and even forms of literature (think textfile[93], the Jargon File[94] or most dramatically, ED[95]).[96]

Like trolls, tricksters often navigate the perils of their world using unorthodox practices to achieve their desired goal.[97] During his interview with Schwartz, Weev also invokes historical tricksters, specifically Loki, "Loki was a hacker," he explains, "The other gods feared him, but they needed his tools."[98] Weev's other favorite trolls? Zeno of Elea, Socrates, Jesus, Coyote, and Kali, the Hindu goddess of destruction.[99]

---

[92] Gabriella Coleman, "Hacker and Troller as Trickster," *Social Text Jounal*, February 7, 2010, http://www.socialtextjournal.org/blog_dev/2010/02/hacker-and-troller-as-trickster.php (accessed March 18, 2012).
[93] http://www.textfiles.com/ is website focusing on mid 1980s textfiles and the "writers and artists bound by the 128 characters that the American Standard Code for Information Interchange (ASCII)".
[94] http://catb.org/jargon/ is a glossary of computer programmer slang.
[95] http://encyclopediadramatica.ch/Main_Page ED, or Encyclopedia Dramatica, is a troll's Wikipedia with the motto 'In lulz we trust'.
[96] Coleman, "Hacker and Troller as Trickster."
[97] Coleman, "Hacker and Troller as Trickster."
[98] Schwartz.
[99] Schwartz.

So, despite the fact that it is tempting, even convenient, to blame technology for destructive trolling, technology is probably not the root of the problem—troll-like figures have existed for centuries. Technology only makes their job easier. Schwartz writes,

> But while technology reduces the social barrier that keeps us from bedeviling strangers, it does not explain the initial trolling impulse. This seems to spring from something ugly—a destructive human urge that many feel but few act upon, the ambient misanthropy that's a frequent ingredient of art, politics and, most of all, jokes. There's a lot to hate out there, and a lot to hate as well.[100]

Schwartz suspects that the trolling impulse is universal but notes that only a minority of people actually acts on that trolling urge—a very visible minority. This is, perhaps, the root of the demonization of hackers; the vocal and destructive minority overshadows the quiet, in this case constructive, majority. Earlier Robert Bickford defined a hacker as anyone who enjoyed circumventing limitations. Hackers can be destructive, but they are also constructive and innovative. It is the responsibility of the hacker to come up with new and cunning ways to do an old thing—it should be expected that hackers would destroy the golden age and innovate their ethic as reality demanded.

In 1994 the head of the Internet Society warned that spam would destroy the network; however, the internet has remained (surprisingly, to some) resilient. While trolls and destructive hackers can be immoral, they do not pose a threat to the internet, Schwartz observes, "And yet the Internet is doing very well for a frontier town on the brink of anarchy. Its traffic is expected to quadruple by 2012. To say that trolls pose a threat to the Internet at this point is like saying that crows pose a threat to farming."[101] Trolls are an inconvenience to the graceful network of the web, but not a roadblock. The only way to end trolling, Fortuny says, is to stop taking the trolls seriously;

---

[100] Schwartz.
[101] Schwartz.

claiming that trolls and hackers might destroy the internet falsely inflates their power, thus inspiring them to take on bigger and better projects that may cause real destruction instead of a spattering of inconveniences.[102]

"Information wants to be free."

Schwartz writes about the trolls he interviewed saying, "That the Internet is now capacious enough to host an entire subculture of users who enjoy undermining its founding values is yet another symptom of its phenomenal success,"[103] but, do hackers and trolls really undermine the founding values of the internet? In his epilogue to *The Hacker Ethic* Manuel Castells describes the new technological paradigm of twenty-first century societies, informationalism, defined as the dependence upon information and knowledge to accumulate wealth and power.[104] Informationalism, however, requires that those with power control and restrict information; it requires that knowledge and information be transformed into scarce resources, which directly contradicts the internet's open structure, not to mention the vision of its founders. Trolls might terrorize some corners of the internet at times, but they certainly do not represent the same threat to its founding principles that the information economy does.

Before returning to informationalism and the network society, it is important to discuss the tensions between hackerism and capitalism. Hackerism depends on an open model for information—a common example is 'free' software, but it is free as in "*free speech*, not *free beer,*"[105]—whereas capitalism depends on a closed model. Himanen explains further:

---

[102] Schwartz.
[103] Schwartz.
[104] Castells, 157.
[105] Himanen, 59.

> Is the present company practice of restricting information really ethically tenable?...Any serious attempt should address many fundamental issues of our information age, including, for example, the paradoxical dependence of closed information on open information. This paradox is at the heart of our time: in fact, if one takes technology companies' dependence on research seriously, one might say that the ethical dilemma facing businesses in the new information economy is that capitalist success is possible only as long as most of the researchers remain 'communists'.[106]

The current model relies on researchers to produce information so that it can be privatized and commoditized, ignoring the traditional academic model that values collaboration and consensus, the model that fits the philosophy of the internet and its design. Informationalism as a technological paradigm undermines the founding principles of the internet because it is dependent on the very network that it exploits.

Informationalism is not unique because of the importance of knowledge or information in societies, Castells claims, because knowledge and information have been central to almost every society throughout history. Informationalism is unique specifically because of the information-technology revolution. Castells writes, "What is new is the technology of information processing and the impact of this technology on the generation and application of knowledge…[it is] a technological paradigm based on the augmentation of the human capacity in information processing around the twin revolutions in microelectronics and genetic engineering."[107] The information-technology revolution, like the internet itself, is notable for its generative features:

1. their self-expanding processing capacity in terms of volume, complexity, and speed,
2. their recombining ability, and
3. their distributional flexibility.[108]

---

[106] Himanen, 61.
[107] Castells, 159.
[108] Castells, 160.

The information-technology revolution ushered in a new technological paradigm because it fundamentally changed how we receive, store, and generate information. Information, in the new paradigm, seems to beget even more information.

Informationalism, Castells asserts, prompted the 'network society', the dominant form of social organization in the twenty-first century, "The network society is a social structure made of information networks powered by the information technologies characteristic of the informationalist paradigm."[109] The network society also directly mimics the structure of information networks: there is no center to it, rather, it is a set of interconnected nodes. Each node is necessary to the network, and if a node is superfluous it is likely to disappear and be replaced with a more productive node, thus making the network more efficient. Castells writes, "In a social structure, social actors and institutions program the networks. But once programmed, information networks, powered by information technology, impose their structural logic on their human components,"[110] informationalism, therefore, did not just 'prompt' the network society—it demanded it. The network society, however, is not flexible like information networks; the network society is closed and resistant to change.

The hacker criminal?

The article *The moral ambiguity of social control: a retroassessement of the 'golden age' of hacking* by Jim Thomas discusses how hacking for free information inspired a moral panic in law enforcement during the golden age of hacking. Hackers hacked, according to Thomas, for three main reasons: first, hackers are risk takers; second, to challenge dangerous and centralized

[109] Castells, 166.
[110] Castells, 167.

technological control; and third, to search for knowledge. They hacked because 'information wants to be free'. Thomas's narrative romanticizes hackers as part of a noble social revolution, comparing them to '60s youth, "creating what they perceived to be an ethical alternative culture,"[111] but ethics ran up against legality. Much of the hacker's behavior was illegal, and law enforcement treated it as such.

Thomas argues that law enforcement agents and the media unfairly demonized hackers because their abject difference and indifference inspired a moral panic. Thomas describes the challenge hackers posed to society and the ensuing 'witch hunt':

> Witch-hunts are about images and social control…Hackers represented a new type of social demon, as the techno-revolution seemed to challenge definitions of law, property rights, privacy and conventional social control strategies. The imagery of good against evil, which was portrayed in the media, political rhetoric and legislation, whipped the public into paranoid fear of teenage master criminals who allegedly could bring down the nation's E911 systems (enhanced emergency telephone service to facilitate urgent communication between the public and public safety agents), disrupt telecommunications or even launch military satellites. The urgent need to control them justified the extreme means in removing the scourge from the public midst.[112]

Few people understood hackers' tools, methods, or motivations and they were therefore treated as powerful and untrustworthy criminals. Thomas describes various raids where government officials abused their power. In 1990 US Secret Service agents barged into an Illinois teen's room and placed a gun to his head, threatening to shoot if he touched the keyboard. Law enforcement agents are also accused of illegal confiscation: during raids, agents would often take anything that might be associated with the suspected crime. They often confiscated not only computers and computer equipment, but also modems, notebooks, and in some instances, even homework.[113]

---

[111] Thomas, 607.
[112] Thomas, 607-8.
[113] Thomas, 609-610.

While hackers of the golden age might not have won the battle for free information, they did illuminate the dark side of social control, and they did challenge accepted social norms. "Rather than see hacking as simply unethical," Thomas proposes, "an alternative interpretation would be to view the participants as primitive rebels attempting to create dissonance in order to bring social meaning to what they perceived as an increasingly meaningless world."[114] Hackers actually bolster the founding principles of the internet because each hack reminds us that society is also a generative platform—it is just a lot harder to reconstruct than a piece of technology. Each hack is an attempt to rewire and reinterpret social norms and values.

———

Futurist Alvin Toffler said, "The future arrives too soon and in the wrong order." The information-technology revolution arrived, evolved, and matured before many realized it was even time to adapt. Thirty years later, the informationalist paradigm still has yet to completely replace the industrialist paradigm, and it is unlikely that the process will be entirely over soon. Berners-Lee's ideal society based on consensus instead of conflict still has yet to be fully realized, but we're making progress. What is worrisome is that the future is still coming and we are still not adapting; the hacker's greatest threat is their unknown potential, but hackers are still dismissed as inconsequential geeks, especially since it has been revealed that few hackers are elite programmers. Hackers' technological prowess will prove crucial in the future as the real and virtual worlds become more intertwined. The next chapter will show why the challenge that hackers pose to society is valuable by challenging the assumption that hackers, and Anons in particular, are unprincipled and thus a nuisance more than a social visionary.

---

[114] Thomas, 607.

CHAPTER 3

Trolling for Social Change

Man is least himself when he talks to you in his own person. Give him a mask and he will tell you the truth.
Oscar Wilde

The previous chapter showed that although the hacker stands on his platform of free access in direct opposition to the informationalist technological paradigm, hacking is not inherently a destructive activity. Hackers, and Anonymous in particular, are a constructive social force. In a panel entitled *Hacktivism, Vigilantism, and Collective Action in the Digital Age* hosted by the Brookings Institution, Richard Forno, director of the cybersecurity program at the University of Maryland, Baltimore, discusses Anonymous:

> I love the title of this panel. You know, hacktivism, vigilantism, and collective action, because it spans the gamut of possible ways of thinking about groups like Anonymous. And the true answer is, is that, in some instances it's hacktivism of a vicious sort, or vigilantism of an even more vicious sort. And then in some instances, it embodies collective action that has been a traditional core part of what we in America think of as free speech and political activity. [115]

Yes, Anonymous is obsessed with cats and Rickrolling, but that does not preclude the group from being an agent of social change. This chapter will use vigilante acts and Project Chanology to show that trolling is not just an expression of the lulz but of principles, namely the freedom of expression, as well.

The fact is, what Steven Mansfield-Devine called 'anarchic cyber fun' is a clever and effective guise for ideological conviction that is evinced in open letters and videos championing free speech, government transparency, and social justice. This chapter will first, show that Anonymous is a multi-

[115] Richard Forno, "Hacktivism, Vigilantism, and Collective Action in the Digital Age" (panel discussion at The Brookings Institution, Washington, DC, December 9, 2011), 22.

faceted, multi-dimensional group that is capable of more than schadenfreude. Second, it will show the power of online activism, noting the ripple effects of Project Chanology and specific acts of vigilantism. Third, the chapter will suggest that although the intersection of the lulz and ideological conviction online may prove to be ethically questionable activities, proper recourse is not legislation. It is important that individuals take the steps to protect themselves and their information online. Furthermore, as Forno says, online collective activism is an important part of contemporary American political culture and should enjoy the same credibility as traditional social activism.

BRB - CHURCH: Vigilantism & the Lulz

In 2007, two Anons posing as a 14-year-old girl in a chat room under the pseudonym 'serious' connected with Canadian Chris Forcand from Ontario. A quick Google search for 'Chris Forcand Anonymous' brings up an archived /b/ thread, called 'brb church – chris forcand' where the Anons posted screenshots of the explicit instant message chats between Forcand and the supposed teen. The first post by user Anonymous at 11:50 PM on October 14, 2007 says, "It's time to call a Pedo…have fun /b/ <3," followed by Forcand's full name, email address, physical address, and cell and home phone numbers.[116] Before reporting Forcand to the police, Anons called and harassed Forcand and sent copies of the chats to his church.[117] The archived /b/ thread is linked below in a footnote, but it should be viewed with caution. The content and images are adult and extremely NSFW, or not safe for work, and a better description might be repulsive.

[116] "brb church – chris forcand," *chanarchive.org*, October 14, 2007, http://chanarchive.org/4chan/b/1032/brb-church-chris-forcand, (accessed March 23, 2012).
[117] Jonathan Jenkins, "Man trolled web for girls:cops," *Canoe,* December 7, 2007, http://cnews.canoe.ca/CNEWS/Crime/2007/12/07/4712680-sun.html (accessed March 23, 2012).

The first image in the archive shows Forcand's chat with the girl, he writes in bold Comic Sans MS, "i want to show you my cock but my son is here right now and we are going out to church. can i show you later when he is back home?"[118] thus inspiring the title of the thread, 'brb – church'. The archive also includes pictures of Forcand's penis with a computer mouse and keyboard on top of it and solicitations for the girl's wet panties. As a result, one poster proposes: "Alright /b/tards; Do this: mail him some panties soaked in chloroform AND liquid laxative. He will pass out and shit himself, and his family will find him passed out, covered in shit, and eating panties. WIN!"[119] Anons and /b/tards continued their shaming rampage, calling and texting Forcand to remind him that he was a pervert, and that everyone knew. A quick map search of his address brought up four local churches and at 12:23 AM on October 15th, just half an hour after the original post went up, one Anon called for everyone to "print copies of all pictures and mail them to all four churches." One person asked, "Has anyone called the Toronto police or the [Royal Canadian Mounted Police] or the Canadian cyber tipline on this guy?"[120] Meanwhile another Anon implored, "DO NOT REPORT THIS MAN. DO NOT REPORT HIM. There is a chance to completely ruin his life here if we act tactfully."[121] The archived thread ends at 12:34 AM on October 15th. Forcand was reported to the authorities—it is unclear when exactly—and arrested on December 5, 2007.[122]

---

[118] Anonymuos, "It's time to call a Pedo," *chanarchive*.org, October 14, 2007, 23:50:0, http://chanarchive.org/4chan/b/1032/brb-church-chris-forcand, (accessed March 23, 2012).
[119] Anonymous, *chanarchive.org*, October 15, 2007, 00:10:0, http://chanarchive.org/4chan/b/1032/brb-church-chris-forcand (accessed March 22, 2012).
[120] Anonymous, *chanarchive.org*, October 15, 2007, 00:26:3, http://chanarchive.org/4chan/b/1032/brb-church-chris-forcand (accessed March 23, 2012).
[121] Anonymous, *chanarchive.org*, October 15, 2007, 00:24:3, http://chanarchive.org/4chan/b/1032/brb-church-chris-forcand (accessed March 23, 2012).
[122] Idkwhat, "Chris Forcand," *Oh Internet*, http://ohinternet.com/Chris_Forcand (accessed March 23, 2012).

"attn: newfags[123]," writes one Anonymous in the thread, "when oldfags like me complain that /b/ used to be so much better (yeah, i know /b/ was never good, but it WAS better.), this is what we are thinking of. this is how it used to be. enjoy it,"[124] implying a moral hierarchy of trolling. Trolling pedophiles to bring them to justice? Good. Trolling tweens because they're annoying? Not so good. While there may be some merit to the claim that ethically motivated trolling is preferable to non-ethically motivated trolling, the rationale is weak. However, it is notable that Anons take it upon themselves to enforce certain standards of conduct online. Anons are the self-appointed internet police; where authorities founder in bring about justice, Anon succeed, albeit by extralegal means.

In October of 2011 Anons waged war against pedophiles again, this time in the anonymous underground forum 'Lolita City'. Lolita City is a type of private, peer-to-peer file-sharing network called a darknet, where users enjoy anonymity because IP addresses are kept private. Systems like Tor, an acronym for 'The onion router', further guarantee anonymity by routing traffic through a worldwide network of encrypted servers concealing both location and web history from network surveillance. The tools are intended to protect users personal freedom and privacy and are often used by political dissidents and activists to protect themselves from oppressive governments. Tor and darknets are also extremely popular with a less savory bunch including "cybercriminals, hackers,

---

[123] /b/ and Anonymous have a very culturally specific vocabulary that to some extent encapsulates the troll philosophy. By using 'fag' as often as possible, Anons are baiting someone to start an argument with him or her about how offensive it is. But, because it is an offensive word, it also diminishes the individual towards which it is directed—another popular epithet is 'moralfag'. The perceived morality is unimportant as is the specific individual. Diminishing and disregarding the individual reinforces the hive mind because no single voice is louder or more respected than another. All users are equal; in the end, 'newfags' and 'oldfags' call themselves by the same derogatory word, a one-two punch: trolling while building the collective conscience.

[124] Anonymous, *chanarchive.org,* October 15, 2007, 00:23:4, http://chanarchive.org/4chan/b/1032/brb-church-chris-forcand (accessed March 23, 2012).

pedophiles and drugs dealers.[125] In October 2011 about six Anons launched OpDarkNet to go after the pedophiles and Freedom Hosting, which hosted one of the largest collections of child pornography on the internet on their servers. The press release of October 18, 2011 reads:

> The owners and operators at Freedom Hosting are openly supporting child pornography and enabling pedophiles to view innocent children, fueling their issues and putting children at risk of abduction, molestation, rape, and death. For this, Freedom Hosting has been declared #OpDarknet Enemy Number One. We will continue to not only crash Freedom Hosting's server, but any other server we find to contain, promote, or support child pornography.[126]

In addition to repeatedly crashing Freedom Hosting's servers, Anons trolled Lolita City: they uploaded clips of the popular hidden-camera reality show "To Catch a Predator" disguised as kiddie porn and leaked about 1,500 Lolita City usernames. In an interview with Chen, a hacker called Arson said, "We have been targeting them in secret for a while now, taking down their servers as much as possible…We decided to seek media attention for this operation so that we may get the resources needed to shut them down on a more permanent basis."[127] Notably, the hackers have not harassed the offenders; they have only pushed them out of the darknet and into the light.

Though little is sacred or serious to the hacker or the troll, child pornography crosses the moral line. There is no official reason why—it probably inspires the same revulsion that it does in the rest of the population. Additionally, online rings of child pornography are exactly the kinds of things that inspire moral panic amongst parents and lawmakers. Chen writes,

> On message boards and in chat rooms on the dark net, the hackers' crusade against Lolita City has sparked a firestorm. Many who use the dark net see it as a protected space for free speech and privacy, not for pedophiles. They despise child porn forums because it stains the reputation of the dark net and the TOR network it relies on, and

---

[125] Adrian Chen, "Vigilante Hackers Wage War on Underground Kiddie Porn," *Gawker*, October 21, 2011, http://gawker.com/5851459/vigilante-hackers-wage-war-on-underground-kiddie-porn (accessed 23 March 2012)
[126] OPDARKNET, "#OpDarknet Major Release & Timeline," *Pastebin*, October 18, 2011, http://pastebin.com/T1LHnzEW (accessed March 23, 2012).
[127] Chen, "Vigilante Hackers Wage War on Underground Kiddie Porn."

> they stage their own crusades against it. For years, computer experts have ben trying to build a system to track pedophiles on TOR. The OpDarkNet hackers say they're motivated by a similar wish to clean out the dark net. Child porn 'tarnishes the purpose of TOR…which was originally built to protect people in China and Iran from their government,' a hacker named Vicious told me.

David Auerbach, writer and software engineer, discusses anonymous culture, or 'A-culture' and ownership in his article, Anonymity as Culture: Treatise, for online magazine Triple Canopy. Anons see the internet as their own private space, and repugnant characters like pedophiles threaten that space and other freedoms. Child porn on Tor ruins Tor because it hints that, maybe, allowing complete freedom and anonymity is more negligent than it is responsible. But, the fact of the matter is that both the internet and Tor are unregulated and open to everyone; they are not 'owned' by Anons. The online world may be physically unreal, but, "Participants fill this void with their own pieces of reality and fiction… participants establish ownership; the world becomes their own because it is distinct and detached from the real one."[128] The space resists appropriation, but by imbuing it with personal touches, users become attached and see the space as their own. Sometimes this means that they troll a young girl like Jessi Slaughter—other times this means that they run out pedophiles.

Anonymous' moral outrage is not limited to pedophiles: they have also taken a stand against animal cruelty. In August of 2010 two videos went viral: one of a woman in Great Britain stuffing a cat into a trash bin[129] and the other of a teenage girl throwing puppies into a river.[130] Within a few hours of the video being posted /b/tards identified the woman as 45-year-old Mary Bale of Coventry England and launched a relatively standard raid publicly posting her personal identifying information on the internet and harassing her. Coventry was eventually forced into hiding, later

---

[128] David Auerbach, "Anonymity as Culture: Treatise."
[129] coventrytelegraph, "Women throws cat in wheelie bin," *Youtube*, August 25, 2012, http://www.youtube.com/watch?feature=player_embedded&v=zbMt82yVj24 (accessed March 23, 2012).
[130] Max Read, "4chan on the Hunt for Puppy-Throwing Girl," *Gawker*, August 31, 2010, http://gawker.com/5626105/4chan-on-the-hunt-for-puppy+throwing-girl?skyline=true&s=I, (accessed March 23, 2012).

confessing and publicly apologizing.[131] About a week later the second video went viral on the internet and inspired /b/tards to do something else principled. They quickly identified the owner of the YouTube account that the video was originally posted from and settled on a Bosnian girl as a culprit. After director Michael Bay volunteered a $50,000 reward for information that led to the arrest and prosecution of the unidentified girl, Bosnian police launched an investigation.[132] Police say that they apprehended the girl and that she is from Bugojno, the same town identified by 4chan.[133] It doesn't seem like anyone got Michael Bay's reward money, considering that the post was taken down shortly after it appeared and the only evidence that remains of the reward is a screencapture.[134]

Despite the fact that Anonymous vigilante raids are allegedly principled, Anonymous's fight to keep the internet open will be a pyrrhic battle because nothing goes away in the era of digitization. Anonymous will be remembered for trolling to intentionally induce epileptic seizures and cyberbullying adolescents, d*espite* its loud voice supporting the Occupy movement, Arab Spring, and WikiLeaks, not to mention open letters and videos championing free speech, government transparency, and social justice. The difficulty is that an Anonymous raid looks the same when it is inspired by moral outrage as it does when it is for the lulz, Forno says,

> And the final thing that really makes Anonymous a challenge and what makes it almost impossible to distinguish between hacktivism, vigilantism and collective action is that on the internet, the information flows are indistinct. It's all ones and zeroes, right? It would be as if, in air power, we couldn't tell the difference between commercial planes, spy planes and missiles that were coming across our aviation borders.[135]

---

[131] Adrian Chen, "How 4chan Brought the Evil British Cat Bin Woman to Justice," *Gawker*, August 25, 2010, http://gawker.com/5622237/how-4chan-brought-the-evil-british-cat-lady-to-justice (accessed March 23, 2012).
[132] Adrian Chen, "*Transformers* Director Michael Bay Offers $50,000 Bounty for Puppy-Throwing Girl," *Gawker*, September 1, 2010, http://gawker.com/5628051/transformers-director-michael-bay-offers-50000-bounty-for-puppy+throwing-girl (accessed March 23, 2012).
[133] Adrian Chen, "Puppy-Throwing Girl Caught in Bosnia," *Gawker*, September 3, 2010, http://gawker.com/5629513/puppy+throwing-girl-caught-in-bosnia (accessed March 23, 2012).
[134] Chen, "*Transformers* Director Michael Bay Offers $50,000 Bounty for Puppy-Throwing Girl."
[135] Forno, "Hacktivism, Vigilantism, and Collective Action in the Digital Age," 23.

Anonymous's attacks are nuanced—like the group itself—and deserve close scrutiny. If we continue to ignore Anonymous, or simply arrest its leaders, we will never be able to tell if an online attack by Anonymous or any other group is a commercial plane, spy plane, or missile.

Vigilantism, granted, has its own problems. But the fact of the matter is that Anonymous's vigilante efforts to bring pedophiles and animal abusers to justice demonstrate that Anons do have principles. The next section will discuss Anonymous's crusade against Scientology, which began as a lulzy raid on the Church of Scientology, and culminated in a real-life protest.

"Wise Beard Man is Wise. His words are wise, his face is beard." or, Project Chanology

In 2008, a video of celebrity Scientologist Tom Cruise passionately praising the practices and beliefs of the Church of Scientology meant only for internal church viewing was leaked. The Church of Scientology threatened all publishers with legal action, citing the Digital Millennium Copyright Act.[136] Music from Mission: Impossible plays in the background and Cruise, Freedom Medal of Valor winner says,

> I think it's a privilege to call yourself a Scientologist and it's something that you have to earn. And because a scientologist does. He, or she has the ability to create new and better realities and improved conditions…Being a scientologist you look at someone and know absolutely that you can help them…When you're a Scientologist, and you drive by an accident, you know you have to do something about it, because you know you're the only one who can really help... We are the way to happiness. We can bring peace and unite cultures.[137]

After receiving legal notice, many video publishers took the video down, including YouTube. Gawker Media, however, refused to take the video down. Nick Denton, founder of Gawker media,

---

[136] Gabriella Coleman, "Anonymous: From the Lulz to Collective Action," *The New Everyday*, April 6, 2011, http://mediacommons.futureofthebook.org/tne/pieces/anonymous-lulz-collective-action (accessed March 23, 2012).
[137] Aleteuk, "Tom Cruise Scientology Video – (Original UNCUT), *Youtube*, January 17, 2008, http://www.youtube.com/watch?v=UFBZ_uAbxS0, Accessed 24 March 2012.

responded to the church saying, "Gawker is now hosting a copy of the video; it's newsworthy; and we will not be removing it."[138] Anonymous followed Gawker's lead and responded to the church's attempts at secrecy and censorship by declaring war against the Church of Scientology. Between January 15, 2008 and January 27, 2008, Anonymous raided the church with DDoS attacks, black faxes, and prank calls in order to disrupt the church's daily operations, calling the attack Project Chanology.

On January 21, 2008, Anonymous released its formal declaration of war against the Church of Scientology in the form of a video on YouTube. A computerized voice speaks over footage of clouds passing over buildings:

> Hello, Leaders of Scientology. We are Anonymous.
>
> Over the years, we have been watching you. Your campaigns of misinformation; your 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 have come to trust you as their leaders, 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, and for our own enjoyment, we shall proceed to expel you from the Internet and systematically dismantle the Church of Scientology in its present form. We recognize you as serious opponents and do not expect our campaign to be completed in a short time. However, you will not prevail forever against the angry masses of the body politic. Your choice of methods, your hypocrisy, and the general artlessness of your organization have sounded its death knell.
>
> You have nowhere to hide; we are everywhere. You will find no recourse in attack because for each of us that falls, ten more will take his place. We are cognizant of the many who may decry our methods as parallel to those of the Church of Scientology. Those who espouse the obvious truth that your organization will use the actions of Anonymous as an example of the persecution of which you have for so long warned your followers. This is acceptable to Anonymous, in fact, it is encouraged. We are your SPs; over time, as we begin to merge our pulse with that of your church, the suppression of your followers will become increasingly difficult to maintain. Believers will become aware that salvation needn't come at the expense of their livelihood; they

[138] Nick Denton, "The Cruise Indoctrination Video Scientology Tried to Suppress," *Gawker*, January 15, 2008, http://gawker.com/5002269/the-cruise-indoctrination-video-scientology-tried-to-suppress (accessed March 24, 2012).

> will become aware that the stress and the frustration that they feel is not due to us, but a source much closer to them. Yes, we are SPs[139] but the sum of suppression we could ever muster is eclipsed by that of your own RTC.[140]
>
> Knowledge is free.
> We are Anonymous.
> We are Legion.
> We do not forgive.
> We do not forget.
> Expect us.[141]

The so-called declaration of war is interesting for two reasons. First, it demonstrates Anonymous's unadulterated commitment to freedom of speech, especially for marginalized persons. Anonymous's battle against the church might attract criticism in the short term, but the criticism will be worth it because Anonymous is serving the greater good: freeing captive Scientologist from the oppression of the church. Second, it expresses great solidarity with oppressed Scientologists. Anonymous identifies itself as a suppressive person regardless of whether Anons and protestors are affiliated with the church. One protestor described Anonymous, "It's multinational, multicultural, multidenominational. You have Jewish people, atheists, Mormons, Christians, Hindus, Buddhists, wiccans, Unitarians, whatever, who are all coming together, who are basically the collective mass…the collective mass of the internet,"[142] the group is everyone but no one in particular; one person's struggle for freedom is all of ours.

Considering the hacker maxim that information wants to be free, it logically follows that Anonymous would target the Church of Scientology for holding it captive. The Tom Cruise video leak and ensuing efforts of censorship exemplify the informationalist paradigm because the Church

---

[139] SP is the Scientology acronym for 'Suppressive Person', or someone who the church considers an enemy.
[140] RTC is the acronym for Religious Technology Center that monitors and controls the use of all Scientology trademarks as well as the use of Scientology texts and symbols.
[141] Church0fScientology, "Message to Scientology," *Youtube*, January 21, 2008, http://www.youtube.com/watch?feature=player_embedded&v=JCbKv9yiLiQ (accessed March 24, 2012).
[142] Landers, "Anonymous Takes On Scientology."

of Scientology relies on internal information and secret rituals to maintain itself. Scientologists paid to hear Tom Cruise speak; they pay for auditing, or counseling by the Church, and coursework necessary to reach higher levels in the church; they pay and work for little to no wages so that the church can file lawsuits to protect its monopoly of information. Today's Church of Scientology is founded entirely on the assumption that knowledge is a scarce resource.

Gabriella Coleman explains another reason that Anonymous might have been attracted to the Church of Scientology as part of the Brookings Institution Panel, Hacktivism, Vigilantism, and Collective Action. She explains her time researching, "I was like, oh, I see why geeks and hackers love to battle the Church of Scientology. It's their evil doppelganger, you know, the perfect nemesis. It's the bizarre comic world, right? It's extremely offensive because it's not simply religion, but one of science and technology that's false,"[143] Anonymous versus the Church of Scientology is a bit like a real life version of the comic Spy vs. Spy: though superficially different, they use the same tools to try and destroy each other. (A graphic in Wired describing the feud chooses nut versus nut, one with sharpie'd devil horns and the other a sharpie'd halo.) The difference between Anonymous and the Church of Scientology, at least from the Anonymous perspective, is that Anonymous's transgressions are just not that grave. On Why We Protest, a website run by a few Anons, the Church of Scientology is charged with*:* "suspicious deaths, torture, coerced abortions, the deliberate separation of families, and human trafficking," harassment and slander towards individuals who publicly challenge the church, and fraudulent activities, most notably the church's tax exempt status despite being a commercial enterprise.*[144]*

---

[143] Coleman, "Hacktivism, Vigilantism, and Collective Action in the Digital Age," 35.
[144] "Scientology Dangers," *Why We Protest*, https://whyweprotest.net/anonymous-scientology/scientology/scientology-dangers/ (accessed March 29, 2012).

The most obvious difference between Anonymous and the Church of Scientology is that, while the Church takes itself very, very seriously, Anonymous, one part troll and one part collective conscious really does not. In a news article, "Serious Business: Anonymous Takes on Scientology (and Doesn't Afraid of Anything)," for Baltimore's City Paper, Chris Landers discusses the church's attempts to "maintain control over the uncontrollable," [145] that is, manage and supervise its brand and representations online. The lawsuit that the church filed against YouTube, Gawker, and other content publishers was standard behavior on behalf of the church. The church has also forced eBay to end all auction for e-meters, the tool used to identify an individual's bad memories, or engrams, during auditing sessions. In fact, no infraction, large or small, gets past the Church of Scientology. At the end of the leaked video, Tom Cruise walks across a stage in a rather shiny suit and a writer at US Weekly wrote a little snark on the fashion statement; Scientologist Kirstie Alley demanded that the writer be fired. The church requires that individuals leaving the church sign non-disclosure agreements and usually classifies them at 'suppressive persons', excommunicating them from the church entirely.[146] Anonymous, in contrast, does not take itself seriously at all. Landers describes the group using equal parts gravity and humor:

> Anonymous is legion. Anonymous does not forgive. Anonymous does not forget. Anonymous only undertakes Serious Business. Anonymous: because none of us is as cruel as all of us. Anonymous has seen Fight Club too many times. Anonymous is not your personal army. Anonymous delivers. Anonymous' real name is David. Anonymous hates dogs. Anonymous likes Mudkips.[147] Anonymous is in it for the lulz.[148]

[145] Landers.
[146] Landers.
[147] Mudkip is a Pokemon character and popular meme on /b/.
[148] Landers.

However, on February 10, 2008, Project Chanology took an interesting turn. Some Anons abandoned the lulz in favor of an organized, multi-city "RL raid",[149] or real life protest.[150] The issues were serious.

Days after the raid started, Mark Bunker, long-time critic of the Church of Scientology, issued a public request to Anonymous. He lauds Anonymous for taking a stand, but asks that they stop trolling the church. Taking down the church's websites will lead to Anons' arrest before it leads to any real change. He warns that the church is merciless in pursuing its critics. He asks that Anons act legally and peacefully against the Church of Scientology. [151] Anonymous listened. In Wired, Julian Dibbell calls the move to public protest, "unprecedented in the annals of not just trolling but online activism in general."[152] Anons explained their reasoning for taking to the streets this way, "Wise Beard Man is Wise. His words are wise, his face is beard."[153] Bunker, a heavily bearded man, would be 'Wise Beard Man'. The February 10th protests, according to Anonymous, drew about 8,300 people worldwide; the protest in D.C. alone, about 200. Anons came out publicly but still refused to abandon their anonymity, the majority wearing Guy Fawkes masks, and one protestor donned a full Burger King costume. Different organizing, coordinating, and support websites popped up and the protests and raid were widely covered by the media.

There were more protests against the Church of Scientology throughout the spring, with numbers matching the original protest. On March 15th, protesters marched to the action site across the street from the Church of Scientology in D.C. while Rick Astley's "Never Gonna Give You Up,"

---

[149] Julian Dibbell, "The Assclown Offensive: How to Enrage the Church of Scientology," *Wired*, September 21, 2009, http://www.wired.com/culture/culturereviews/magazine/17-10/mf_chanology?currentPage=all, (accessed March 29, 2012).
[150] Dibbell.
[151] xenutv1, "Scientology: XENU TV Speaks to Anonymous," *Youtube*, January 27, 2008, http://www.youtube.com/watch?feature=player_embedded&v=zW466xcM0Yk (accessed March 24, 2012).
[152] Dibbell.
[153] Landers.

the Rickroll anthem, played through speakers.[154] The Church of Scientology was also organizing—with law enforcement—to press charges against as many people as they could who had participated in the coordinated raids against their websites. Dibbell also reports that individual Scientologists, handlers, have taken it upon themselves to monitor the most active Anons engaged in protest, sometimes even videorecording them in order to immortalize any incriminating or embarrassing activity.[155] Tommy Davis, a church spokesperson, told Dibbell, "They are a terrorist organization. Their intention is to instill fear and incite hate. There is no other explanation."[156] One woman at the protest in D.C. had a differing opinion; she said to Landers:

> Scientology is seen at the moment, as far as the internet is concerned, the most egregious infection that's keeping it from being as smoothly operating as it needs to be, so we sort of turn our attention to it. But what's started to happen is that then you see the real effect it's had on real people, beyond the free speech angle. And this is what draw peoples in and makes them physically appear at a protest on the birthday of a woman who died because of this cult, or organization, or whatever you want to call it.[157]

The protests against the Church of Scientology fall squarely into the realm of activism. Even a 2009 protest against the church, called Operation Slickpubes where a man covered himself in petroleum jelly, pubic hair trimmings, and toenail clippings, before walking into the Church of Scientology in New York, isn't terrorism; it inspires headshaking, eye rolls, and bewilderment, but not fear.[158] However, there is still debate surrounding the ethics of other Anonymous tactics, most notably DDoS attacks. The next section will discuss DDoSing, internet use, misuse and what it has to do with the future of Anonymous.

---

[154] Landers.
[155] Dibbell.
[156] Dibbell.
[157] Landers.
[158] Dibbell.

From hacktivism to cyberterrorism

In her 2001 article, Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, Dorothy E. Denning, an information security researcher and professor in the Department of Defense Analysis at the Naval Postgraduate School in Monterey, California, discusses the different categories of online action. Activism, Denning writes, is "normal, non-disruptive use of the Internet in support of an agenda or cause,"[159] such as routine use of email or social media to organize or spread awareness. Hacktivism is the fusion of hacking and activism, "It covers operations that use hacking techniques against a target=s Internet site with the intent of disrupting normal operations but not causing serious damage. Examples are Web sit-ins and virtual blockades, automated e-mail bombs, Web hacks, computer break-ins, and computer viruses and worms."[160] Hacktivism is not destructive, it is only inconvenient. *The* third class of digital political activity, according to Denning, is cyberterrorism, or hacking operations that are intended to cause significant harm such as extensive loss or life or economic ruin.[161] In Denning's 2000 testimony before the United States Congress's House Armed Services Committee she said:

> Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a cost nuisance would not.[162]

---

[159] Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," Nautilus Institute, June 8, 2001, http://faculty.nps.edu/dedennin/publications/Activism-Hacktivism-Cyberterrorism.pdf (accessed 23 March 2012).
[160] Denning, 2.
[161] Denning, 2.
[162] Denning in "Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet," by Maura Conway, *First Monday* 7:11 (2002), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/1001/922 (accessed April 1, 2012).

There is no bright line test for cyberterrorism, instead, acts need to satisfy requirements for both intent and consequence. The fact that there is no universal definition for cyberterrorism underscores the need for prudence: because cyberterrorist acts must satisfy certain requirements, they can only be recognized in retrospect.[163]

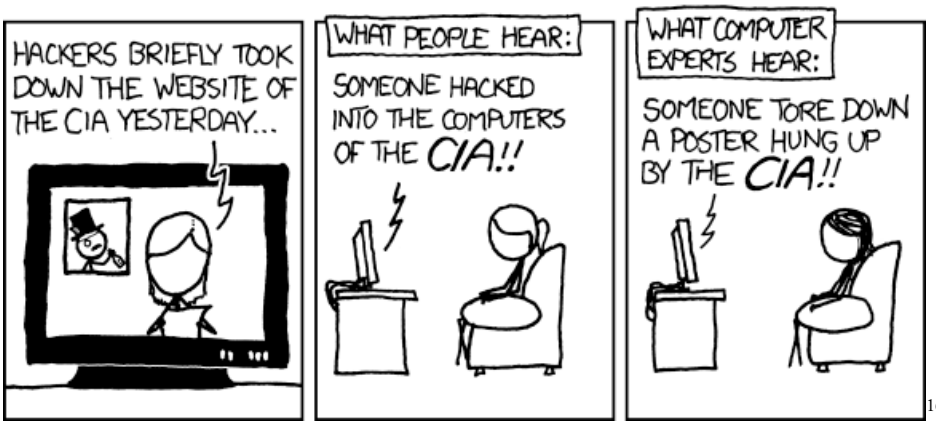
Activism, hacktivism, and cyberterrorism are all political terms that describe actions with political or social ends in mind. Terms like activism, hacktivism, and cyberterrorism, though, presuppose politics, forcing Anonymous into a binary of political and apolitical that it does not fit. Furthermore, 'hacktivism' and 'cyberterrorism' are especially troublesome identifiers because there is no universally accepted definition for either. It is therefore preferable to discuss Anonymous and its tools, specifically DDoS attacks and d0xing, in terms of internet 'use' and 'misuse'. That is: are Anons using the tools of the computer and the internet in productive ways that align with the general spirit of the internet, or, do their practices undermine the spirit of the internet, as Schwartz claims?

A DDoS attack is distributed denial of service attack, what Coleman calls "gumming up a server by bombarding it with too many requests."[164] Hacking, in contrast, is an actual computer break-in and considered trespassing. Coleman likens a DDoS attack to a digital sit-in and argues that it should be considered a non-violent protest on a virtual medium.[165] To launch a DDoS attack, digital activists download the Low Orbit Ion Cannon (LOIC), a denial of service attack application, which turns the computer into a 'bot', repeatedly requesting a website, "No skill is required to use LOIC. The Javascript version just needs the user to enter a target address and click the 'fire'

---

[163] Conway.
[164] Coleman, *The Ethics of Direct Digital Action*.
[165] Coleman, *The Ethics of Direct Digital Action*.

button."[166] An average internet user becomes a hacktivist just by searching for LOIC in Google. It is important to take away from this discussion that DDoS does not require elite programming skills and they do not compromise information stored on the side or the site code; DDoS attacks only make a website inaccessible. Recently, when Anonymous DDoS'd the Central Intelligence Agency, the site was inaccessible and an image replaced the home page. The web comic xkcd put up a comic that summarizes the attack:



[167]

The image that came up instead of the CIA homepage was vandalism, not a hack. The front page of the website was defaced with Anonymous's image and text until the attack was over and everything returned to normal.

Despite the fact that DDoS attacks are 'unambiguously illegal' in the United States and likely illegal in the majority of countries, LOIC does not pretend to hide the IP address of the attacker, making it very easy for law enforcement to carry out arrests—which they do not hesitate to do. Interpol recently apprehended 25 individuals associated with Anonymous;[168] in July 2011, the FBI arrested 16 individuals associated with Anonymous's attacks against PayPal, MasterCard, and

---

[166] Steven Mansfield-Devine, "Anonymous: Serious Threat or Mere Annoyance?" 5.
[167] xkcd, "CIA," http://xkcd.com/932/ (accessed March 23, 2012).
[168] Greg Keller, "Interpol: 25 Suspected Anonymous Hackers Arrested in New Crackdown," *Huffington Post*, February 28, 2012, http://www.huffingtonpost.com/2012/02/28/interpol-anonymous-hackers_n_1306630.html (accessed March 23, 2012).

Visa;[169] in January 2011, 5 individuals associated with the attacks against PayPal, MasterCard, and Visa were arrested in the United Kingdom.[170] Josh Holiday reports for The Guardian,

> The arrests were co-ordinated by the Metropolitan police in conjunction with other UK forces and international agencies. "They are part of an ongoing investigation into Anonymous which began last year following criminal allegations of DDoS attacks by the group against several companies," Scotland Yard said. "This investigation is being carried out in conjunction with international law enforcement agencies in Europe and the US."[171]

DDoS attacks, according to anthropologist Coleman and information security specialist Denning, may be a digital sit-in—a form of civil disobedience—but the attacks are still apparently a matter of international concern, not to mention a threat to international security. Coleman argues that if DDoS action is always intolerable and considered a tactic of chaos, the consequences of prosecution will jeopardize First Amendment rights online. She writes, "This is damaging to the overall political culture of the internet, which must allow for a diversity of tactics, including mass action, direct action, and peaceful of protests, if it is going to be a medium for democratic action and life."[172] Hastily criminalizing DDoS attacks and other tools of online action without carefully considering their value as forms of protest threatens the internet's potential to be a center for truly democratic speech and action.

d0xing, or the online release of private and sensitive documents or personal information such as name, phone number, address, or photographs, is another common feature of an AnonOp. Whereas DDoS attacks and real-life protests have clear parallels, d0xing is an unambiguous violation of individual privacy. The hacker maxim 'information wants to be free' might encourage such release

---

[169] Adrian Chen, "These are the Faces of Anonymous," *Gawker*, September 9, 2011, http://gawker.com/5838756/these-are-the-pale-faces-of-anonymous/gallery/1 (accessed March 23, 2012).
[170] Josh Halliday, "Police arrest five over Anonymous WikiLeaks attacks," *The Guardian*, January 27, 2011, http://www.guardian.co.uk/technology/2011/jan/27/anonymous-hacking (accessed March 23, 2012).
[171] Halliday.
[172] Coleman, *The Ethics of Direct Digital Action.*

of information, but the consequences of such an interpretation are enormous. If all information were freed and publicized, privacy and security would fall like dominoes. Information like my home address may be 'public' but that does not mean that it should be publicized; 'information wants to be free' is an adage, not an ethical imperative. d0xing to reveal security gaps, as Anonymous did to Sony's PlayStation Network in 2011, acquiring user data for more than 75 million customers, is similarly unethical.[173] In a 1989 article, *Are Computer Hacker Break-ins Ethical?* Gene Spafford, a leading computer security expert and computer science professor at Purdue University, writes:

> People wishing to report a problem with the security of a system need not exploit it to report it. By way of analogy, one does not set fire to the neighborhood shopping center to bring attention to a fire hazard in one of the stores, and then try to justify the act by claiming that firemen would otherwise never listen to report of hazards.[174]

d0xing is a misuse of technology: it treats computers and the internet as exercises in security, instead of tools and resources crucial for learning, communicating, and connecting.

d0xing and DDoS attacks may be unethical and misuses of technology, but we should still be hesitant to describe either practice using inflammatory language like hacktivism and cyberterrorism because it only politicizes and dramatizes the issues further. Hacktivism and cyberterrorism deserve careful attention because they are issues of freedom, security, and privacy—not because they are political Mark Manion and Abby Goodman elaborate in *Terrorism of Civil Disobedience: Towards a Hacktivist Ethic*: "Moreover, labeling the hacktivist as a national security threat provides further legitimation for the erasure of individual privacy at the hands of the national security state, which

---

[173] Kim Zetter, "FBI Arrests U.S. Suspect in LulzSec Sony Hack; Anonymous Also Targeted," *Wired*, September 22, 2011, http://www.wired.com/threatlevel/2011/09/sony-hack-arrest/ (accessed March 30, 2012).
[174] Spafford.

compiles and stores vast databases on hundreds of thousands of citizens each year,"[175] rhetoric of hacktivism and cyberterrorism, they argue, distracts us from the real issues at hand.

Hackers may be a threat to privacy and security, but so is the moral panic that legitimizes severe legislation at the expense of freedom of expression. Spafford addresses different rationales for justifying break-ins and vandalism, one of which is the so-called 'social protector argument'. The social protector argument claims that hackers are actually protecting society from surveillance by breaking in because they hacks force transparency. Spafford reacts,

> However, it is not clear that breaking into those systems will aid in righting the wrong. If anything, it will cause those agencies to become even more secretive and use the break-ins as an excuse for more restricted access. Break-ins and vandalism have not resulted in new open-records laws, but they have resulted in the introduction and passage of new criminal statutes.[176]

Break-ins and vandalism do not align with the democratic agenda put forth by alleged activists, and in fact, the actions work against them because they are illegal and unethical. The social protector argument results in fewer, not more freedoms. Towards the end of his article, Spafford suggests that it is the role of professionals to make recommendations to the public on how to deal with cybercrime and information security, not lawmakers. Internet use and misuse, hacktivism and cyberterrorism, should remain questions of ethics for the time being, and not be legislated over.

The question of whether or not DDoS attacks are really the equivalent of a digital sit-in remains unresolved. It could be that (temporarily) taking down the websites of PayPal, MasterCard, Visa, the Motion Picture Association of America, Sony, the Department of Justice, the Federal Bureau of Investigation, among others, threatens safety and security in such a way that charging

---

[175] Mark Manion and Abby Goodrum, "Terrorism or Civil Disobedience: Towards a Hacktivist Ethic," *Computers and Society* 30:2 (June 2000): 17.

[176] Eugene H. Spafford, *Are Computer Hacker Break-ins Ethical?* Department of Computer Science, Purdue University, 1989, http://webcache.googleusercontent.com/search?q=cache:fYGDDVF0DG0J:spaf.cerias.purdue.edu/tech-reps/994.ps+&cd=2&hl=en&ct=clnk&gl=us (accessed March 30, 2012).

Anons with felony crimes is the only way to guarantee social stability. But, it is also interesting to take a close look at the list of DDoS attack victims because many of the attacks are against private firms. The fact that the government takes such a strong stance against these attacks is indicative of today's information economy and the close relations between the government and large private enterprise. The health of private companies is of great public interest, potentially at the expense of the free and open internet if the Stop Online Piracy Act (SOPA), Protect IP Act (PIPA) and attacks on network neutrality are any indication. Anonymous itself may be a politically destabilizing force, but the real question is whether or not Anonymous as a group should be destabilized in turn.

Anonymous is not an irrelevant group of pranksters. The hacktivist collective publicly takes on big issues and challenges structures and institutions that many take for granted. The next chapter *will discuss different AnonOps through the present and show that the consequences of the collective's operations are not only relevant in obscure online forums; AnonOps have very real consequences.*

CHAPTER 4

AnonOps: unprecedented change for the good?

"Who would have thought a bunch of /b/tards from 4chan's chaotic recesses would have grown up to change the world?
Anonymous, @YourAnonNews, March 29, 2012

Anonymous's crusades against pedophiles, animal abusers, and the Church of Scientology challenge Steven Mansfield-Devine's assertion that "trying to organize Anons is like herding cats,"[177] because although Anonymous is anarchic, it is not chaotic. Anonymous is anarchic in the original sense of the word: the group challenges traditional political authority in favor of meritocracy and a hyper-democratic process. Hierarchy exists in Anonymous based on your merited reputation: you earn authority when you demonstrate exceptional capability in a certain area. Decisions are consensus based and regardless of reputation, each person has a say. Anonymous, by challenging the colloquial definition of anarchy, which brings to mind lawless rebels and barbarity, also challenges accepted ideas about power. The Chris Forcand raid showed that power does not always arrive in uniform; the raid showed that individuals have the ability to exercise power remotely. The raid against Lolita City furthers the theme of individual empowerment: when individuals exercise power, they assume the responsibility of reforming their world, thus chipping away at the formal power of the state. Project Chanology, instead of challenging the power of the state, challenged the power of a private institution over individuals.

The last chapter showed that even though Anonymous is a lulzy, sometimes brutish, group of cyberpunks, the raids evidence a general ideological commitment to mankind. Anons endeavor to create a safe internet space for activists as well as children, and decry violence against animals and

[177] Mansfield-Devine, "Anonymous: serious threat or mere annoyance?" 8.

people, as noted in the list of grievances against the Church of Scientology. Anonymous's attacks did bring pedophiles and animal abusers to justice, though the jury is still out with regard to the Church of Scientology. This chapter will explore the inspiration for and consequences of five specific AnonOps: Operation Payback, Operation Avenge Assange, Operation Tunisia, Operation Egypt, and Operation BART. The chapter will close with a discussion of the attack on HBGary Federal, carried out by Anonymous offshoot Lulz Security. Although the mythos surrounding Anonymous makes it seem like the hive mind is deeply entrenched in the virtual world; it is a group with its own vocabulary, cultural currency, and organizational structure that make sense only in the virtual context. However, this chapter will demonstrate that Anonymous is not limited to cyberspace: AnonOps involve real world action and have real world consequences.

Operation Payback

Operation Payback, full name Operation: Payback is a Bitch, is Anonymous's longest-running operation. The operation began in September 2010 as an attack against anti-piracy groups and lasted for nearly three months, culminating with the notorious December 2010 attacks against MasterCard, Visa, and PayPal in the wake of WikiLeaks. Operation Payback began on September 17, 2010, when India-based AiPlex Software, at the behest of Bollywood studios launched a DDoS attack against popular peer-to-peer file-sharing website The Pirate Bay. The company is contracted by the Motion Pictures Association of America (MPAA) to deliver copyright notices to websites that have violated copyright laws and then launch a DDoS attack against the website if the notice is ignored. Anonymous's original plan was to DDoS the AiPlex Software website on September 17th, but another individual already had. The collective quickly remodeled the attack, choosing to instead

target the MPAA and International Federation of the Phonographic Industry (IFPI), causing over 30 hours of combined downtime; two days later the attacks targeted other copyright stringent organizations, the Recording Industry Association of America (RIAA) and the British Phonographic Industry (BPI).[178][179] On September 19th, Anonymous released the following statement:

To whom it may concern:

> This is to inform you that we, Anonymous, have for the last few days been involved in an Operation called "Payback is a Bitch".
>
> This was begun in retaliation for denial of service attacks perpetrated by AIPLEX against The Pirate Bay's servers on behalf of the RIAA (Recording Industry Association of America) and the MPAA (Motion Pictures Association of America). Anonymous has successfully engaged in its own DDoS against AIPLEX's servers and ahs expanded its operations against the MPAA and the RIAA, which at the time of writing were also unreachable.
>
> Anonymous is sick and tired of these corporations seeking to control the internet in their pursuit of profit. Anonymous cannot sit by and do nothing while these organizations stifle the spread of ideas and attack those who wish to exercise their rights to share with others. Anonymous will not just watch while others are attacked. Their servers have been shut down and they will remain so for as long as there is no true freedom of information and data. These successful attacks on the MPAA and RIAA's servers shall continue. An injury to one is an injury to all.
>
> Anonymous,
>
> We are legion.
> We do not forgive.
> We do not forget.

[178] Ernesto, "Behind the Scenes at Anonymous' Operation Payback," *Torrent Freak*, November 15, 2010, http://torrentfreak.com/behind-the-scenes-at-anonymous-operation-payback-111015/ (accessed March 30, 2012).
[179] Luis Corrons, "4chan Users Organize Surgical Strike against the MPAA," *PandaLabs*, September 17, 2010, http://pandalabs.pandasecurity.com/4chan-users-organize-ddos-against-mpaa/ (accessed March 30, 2012).

The operation, like nearly every Anonymous operation, was organized on IRC. On one channel, #command, there was a group of organizers, and on another, #operationpayback, was a group of individuals there to fire on targeted websites; both channels were open to anyone who wanted to join. The DDoS attack received substantial media attention, inspiring the group to continue its attacks, targeting two anti-piracy law firms and United Kingdom anti-piracy firm ACS:Law.[180] Anonymous took ACS:Law's website down with a DDoS attack and d0xed the firm.[181] When asked about the attack, owner Andrew Crossley feigned indifference even though the d0x included a confidential list of individuals involved in lawsuits, "It was only down for a few hours. I have far more concern over the fact of my train turning up 10 minutes late or having to queue for a coffee than them wasting my time with this sort of rubbish,"[182] despite Anonymous's theatrics, the media attention dissipated quickly and Anonymous chose to revamp its strategy.

Operation Payback began as an attack against groups that targeted the Pirate Bay and eventually snowballed into an attack against anyone engaged in anti-piracy efforts.[183] In October Anonymous targeted Portugal's ministry of Culture, the Associação do Comércio Audiovisual de Portugal (ACAPOR), because ACAPOR had filed a lawsuit against The Pirate Bay that September. Anonymous d0xed ACAPOR and redirected all requests for the website to thepiratebay.org.[184] In the same month, Anonymous targeted KISS member Gene Simmons after he had encouraged victims of Anonymous's attacks to be litigious and put the offenders in jail; Anonymous's DDoS attacks against

---

[180] Ernesto, "Behind the Scenes at Anonymous' Operation Payback."
[181] Enigmax, "ACS:Law Anti-Piracy Law Firm Torn Apart by Leaked Emails," *Torrent Freak*, September 25, 2010, http://torrentfreak.com/acslaw-anti-piracy-law-firm-torn-apart-by-leaked-emails-100925/ (accessed March 30, 2012).
[182] Christopher Williams, "Piracy Lawyer Mocks 4chan DDoS Attack," *The Register*, September 22, 2010, http://www.theregister.co.uk/2010/09/22/acs_4chan/ (accessed March 30, 2012).
[183] Ernesto, "Behind the Scenes at Anonymous' Operation Payback."
[184] Ernesto, "Movie Rental Outfit Hacked, Emails Leaked, Redirected to The Pirate Bay," October 18, 2010, http://torrentfreak.com/movie-rental-outfit-hacked-emails-leaked-redirected-to-the-pirate-bay-101018/ (accessed March 30, 2012).

both simmonsrecords.com and genesimmons.com lasted for over 24 hours. After the attack, Simmons trolled Anonymous right back saying, "Some of you may have heard a few popcorn farts re: our sites being threatened by hackers…First, they will be punished. Second, they might find their little butts in jail, right next to someone who's been there for years and is looking for a new girl friend,"[185] threats that led to even more downtime for his websites. In November, Anonymous targeted the US Copyright Office website, its first attack against a .gov site; this attack motivated an FBI investigation into Anonymous activities.[186]

One Anon told *Torrent Freak*, "I fight with anonops because I believe that the current political system failed, and that a system based on anarchy is the only viable system,"[187] however, Operation Payback's demands were not anarchic; they were actually surprisingly banal. Anonymous demanded that copyright and patent laws change, but not that they be done away with entirely. Another Anon explains,

> What we are now trying to do, is straighten out our ideals, and trying to make them both heard and accepted. Nobody would listen to us if we said piracy should be legal, but when we ask for copyright lifespans to be reduced to 'fair' lengths, that would sound a lot more reasonable.[188]

Anons wanted Operation Payback to lead to real change, and it was thus important for their demands to realistic so that they would be considered seriously. Demanding that copyrights and patents be done away with and all file sharing legalized would have eroded their broad base of supporters.[189] Though Operation Payback has not resulted in any specific legislative changes to date,

---

[185] Nate Anderson, "Gene Simmons vs. Anonymous: Who's the bigger tool?" *Ars Technica*, October 2010, http://arstechnica.com/tech-policy/news/2010/10/gene-simmons-vs-anonymous-whos-the-bigger-asshole.ars (accessed March 30, 2012).
[186] Ernesto, "Behind the Scenes at Anonymous' Operation Payback."
[187] Ernesto, "Behind the Scenes at Anonymous' Operation Payback."
[188] Ernesto, "Behind the Scenes at Anonymous' Operation Payback."
[189] Ernesto, "Behind the Scenes at Anonymous' Operation Payback."

Anonymous's broad support base was instrumental in lobbying against the Stop Online Piracy Act (SOPA) and Protect IP Act (PIPA) this past fall and winter.[190]

Operation Avenge Assange

The final leg of Operation Payback, Operation Avenge Assange, arrived December 2010 in the wake of WikiLeaks. In November 2010, *The New York Times*, *The Guardian*, *Der Spiegel*, *Le Monde*, and *El País* began to publish a number of the quarter-million stolen cables between the US State Department and various diplomatic outposts. The cables had been distributed by the Australian Julian Assange's nonprofit organization WikiLeaks, a project intended to counter government secrecy by making information free.[191]

Shortly after the release of the cables, many corporations suspended business with WikiLeaks, including: MasterCard, Visa, PayPal, Amazon.com, Apple, Bank of America, EveryDNS, the WikiLeaks US hosting provider, and Tableau Software.[192] Angela Daly, doctoral candidate at the European University Institute in Florence, Italy and International Legal Fellow at the Electronic Frontier Foundation, speculates that the corporate response to WikiLeaks may have been heavily influenced by politics in Washington, DC; she argues that there is an 'invisible handshake' between governments and corporations:

> This state of affairs has come about due to the policies of the governments of various developed countries, particularly in North America and Europe, in adopting the role of regulator regarding the communications infrastructure, directing private behavior through the use of rules, and thus in practice allowing the emergence of private entities in this environment, which exercise control over parts of the network. When

---

[190] Weisman, Jonathan, "After an Online Firestorm, Congress Shelves Antipiracy Bills," *The New York Times*, January 20, 2012, http://www.nytimes.com/2012/01/21/technology/senate-postpones-piracy-vote.html?_r=1 (accessed March 30, 2012).
[191] Angela Daly, "Private power and new media: the case of the corporate suppression of WikiLeaks add its implications for the exercise of fundamental rights on the Internet."
[192] Daly, parts 2-4.

> the State wants to exert control over the network, it co-opts these pre-existing privately-managed nodes.[193]

In the informationalist paradigm, state and corporate interests merge because each depends on the other for survival: the state uses legislative means to control private information, often in the name of national security, and corporations have incentive to comply with state demands, namely because the incentives facilitate the accumulation of still more information, and thus wealth.[194] The convergence of state and corporate interests efficiently transforms information and knowledge into scarce resources, maximizing the benefits of the informationalist paradigm for both parties.

Daly suspects that the 'invisible handshake' factored into the corporate reaction to WikiLeaks because, at the time, WikiLeaks was innocent. Many of the companies that suspended services to WikiLeaks purported to do so because WikiLeaks was engaged in illegal activity or violated their terms of service, "However," writes Daly,

> these claims of illegality or lack of rights over the content are mere allegations since there has been no authoritative legal pronouncement on the matters, and the claims regarding the jeopardisation of the safety of individuals are also mere speculation. Furthermore, even if an illegal act was committed by the person who leaked the information to WikiLeaks, it would seem that WikiLeaks in disseminating that information enjoys the protection of the First Amendment vis-à-vis prosecution by the US Government.[195]

The parallel interests did not escape Anonymous: the group released the following manifesto, lambasting the companies that kowtowed to American government interests:

> **On the Internet, the only jury is that of the people. Anonymous has kept a watchful eye, and has decided that MasterCard's actions are unacceptable.**
>
> MasterCard Worldwide stated its policy is to 'prohibit customers form directly or indirectly engaging in or facilitating any action that is illegal.' PayPal state: 'Paypal has permanenty restricted the account used by WikiLeaks due a violation of the

[193] Daly, 3.1.
[194] Daly, 3.1.
[195] Daly, 3.2.

> PayPal Acceptable Use Policy, which states that our payment sevice cannot be used for any activities that encourage, promote, facilitate or instruct others to engage in illegal activity. We've notified the account holder of this action.'
>
> The free exchange of ideas and informaiton, no matter how inconvenient, is never illegal. Wikileaks has not acted in violation of law, and has won all prosecutions so far. MasterCard's and PayPal's words ring hollow, but their actions are obvious—**to punsih WikiLeaks, most likely at the behest of the United States government.**
>
> **False allegations have been made that Wikileaks has engaged in illegal activity.** We vaguely remember learning in school that courts decide what is illegal and what is not. It is unacceptable that a corporate entity such as MasterCard has the ability to financial disadvantage Wikileaks as an organisation., thus crippling the ability and the possibility for people to be informed.
>
> **Corporate entities should not be engaged in suppressing speech, nor assist governments in silencing dissidents.**
>
> In attacking Wikileaks, these organizations have revealed their hypocrisy. **MasterCard accepts payments going ot the KKK and other less than savory political organisations**—why then do they block donations to Wikileaks? In 1870, a federal grand jury determined that the Klan was a terrorist organization, and many government bodies have since agreed. **Yet, MasterCard still willingly collects funds for them, while WikiLeaks, which does nothing illegal, has been shut out.**
>
> We have come a long way. **PayPal has agreed to submit to our termsa nd we have shown the power of Anonymous.** We thank PayPal for doing the right thing.
>
> Moreover, we expect that companies such as Mastercard and Visa will have the same decency. **Wikileaks is not a criminal organisation, it serves solely the people of the free world and the users of the Internet.**
>
> **Punishing WikiLeaks because it has distributed information which embarrasses the powerful is a disgrace to the internet, and we will not accept it.**
>
> ANONYMOUS IS LEGION.
> WE DO NOT FORGIVE. WE DO NOT FORGET.
> EXPECT US.[196]

On December 7, 2010 Anonymous launched DDoS attacks against the websites of PayPal, MasterCard, and Visa, shutting them down for hours—not a small feat considering the amount of

[196] MasterCard Manifesto.

traffic that those websites are designed to handle. Anonymous also targeted Amazon.com for a bit, but it became obvious that there were not enough bots engaged to overwhelm Amazon's servers. After the DDoS attack, PayPal did release WikiLeak's funds.

Operation Payback began simply as an operation to save The Pirate Bay, a very popular file-sharing website, but became symbolic of Anonymous's commitment to free speech. Anonymous continued to exercise its voice through January when Anons played an important role in uprisings of the Arab Spring.

The Arab Spring: Operation Tunisia & Operation Egypt

On Sunday, January 2, 2010, Anonymous began Operation Tunisia (OpTunisia), launching successful DDoS attacks against several Tunisian government websites, including that of the president, the prime minister, the Ministry of Industry, the Ministry of Foreign Affairs, the stock exchange, and ironically the government internet agency that had been censoring online dissidence, popularly known as Ammar 404[197] Like many Anonymous Operations, the attack was announced through a press release on YouTube.[198]

The operation was borne out of the WikiLeaks scandal and Operation Avenge Assange; the government's censorship of WikiLeaks Tunisia had directed Anonymous's attention to the government's pervasive online censorship campaign. Internet freedom in Tunisia is severely limited as a result of the government's very sophisticated phishing, or password-stealing, operation. The government internet agency steals users' passwords to blogs, emails, social networking sites—

[197] Yasmine Ryan, "Tunisia's bitter cyberwar," *Al Jazeera*, January 6, 2011, http://www.aljazeera.com/indepth/features/2011/01/201116141458393 62.html (accessed March 30, 2012).
[198] Anonymousworldwar3, "ANONYMOUS – OPERATION TUNISIA – A Press Release," *Youtube*, January 5, 2011, http://www.youtube.com/watch?v=BFLaBRk9wY0 (accessed March 30, 2012).

anything—to spy on its citizens and delete posts that criticize the government or express dissent. One Tunisian web activist, Azyz Amamy said to *Al Jazeera*, "Here we don't really have Internet, we have a national intranet."[199]

In "Tunisia's bitter cyberwar," *Al Jazeera's* Yasmine Ryan reports that there were an estimated 50 Tunisians in the IRC channels where OpTunisia was planned, one of whom was Slim Amamou, Tunisian blogger and former Secretary of State for Sport and Youth.[200] Anons provided Amamou, who used the handle 'slim404', and other Tunisians with an 'online care package' that included Tor software and Greasemonkey script, a web browser extension, to help Tunisians circumvent governmental restrictions on privacy. Amamou and other Tunisian activists in the channels shared the software with people on the ground.[201] One Anon (now famously) wrote,

> This is *your* revolution. It will neither be Twittered nor televised or [sic] IRC'ed. You *must* hit the streets or you *will* lose [sic] the fight. Always stay safe, once you got [sic] arrested you cannot do anything for yourself or your people. Your government *is* watching you.[202]

Both Amamy and Amamou were taken in by authorities on Thursday, January 6th, but only eight days later Ben Ali left power. Anons had little time to celebrate the success of the Tunisian Revolution before beginning Operation Egypt (OpEgypt).

OpEgypt, like OpTunisia, was a reaction to government censorship. On Wednesday, January 26, 2011, Anonymous launched DDoS attacks on the websites of the Egyptian cabinet, the Ministry of the Interior, and the Ministry of Communications and Information Technology. As is customary, Anonymous announced their plans in a press release on YouTube in which Anonymous

---

[199] Ryan.
[200] Ryan.
[201] Quinn Norton, "2011: The Year Anonymous Took On Cops, Dictators, and Existential Dread," *Wired*, January 11, 2012, http://www.wired.com/threatlevel/2012/01/anonymous-dicators-existential-dread/ (accessed March 30, 2012).
[202] Norton.

charges the Egyptian government with being criminal for imposing censorship on its people, violating the Universal Declaration of Human Rights by denying their right to freedom of expression, freedom of association, and the free access of information.[203] Anonymous's characteristic computerized voice continues,

> Anonymous wants you to offer free access to uncensored media in your entire country. When you ignore this message, not only will we attack your government websites, Anonymous will also make sure that the international media sees the horrid reality you impose upon your people. Anonymous will not spare anybody who supports this suppression.[204]

Anonymous continued its DDoS attacks against all top government websites for days, and similar to OpTunisia, provided Egyptians with an online care package available for download from their Facebook group page.[205]

The real effects of Anonymous's hacktivism in the Arab Spring will never be entirely clear, however it is fair to say that their online care package was helpful to many Tunisians and Egyptians, if not directly instrumental to the revolution itself. In a time when the government tried to assert its dominance over the people by denying them free expression and access to the internet, citizens were able to counter, accessing blocked sites and organizing clandestinely online, showing that the emperor in fact, had no clothes.

---

[203] Paul Wagenseil, "Anonymous 'hacktivists' attack Egyptian websites," *Security News Daily*, January 26, 2011, http://www.msnbc.msn.com/id/41280813/ns/technology_and_science-security/#.T3bs0r9SR7E (accessed March 30, 2012).
[204] mmxanonymous, "OPERATION EGYPT: ANONYMOUS PRESS RELEASE – 26/01/2011," *Youtube*, January 26, 2011, http://www.youtube.com/watch?v=yOLc3B2V4AM (accessed March 30, 2012).
[205] Jesse Emspak, "Update: Egyptian Gov't Web Sites Under Attack," *International Business Times*, January 26, 2011, http://www.ibtimes.com/articles/105329/20110126/update-egyptian-gov-t-web-sites-under-attack.htm (accessed March 30, 2012).

Operation BART

Operation BART (OpBART), in contrast to the previous operations discussed, was primarily a real-life protest. Though OpBART had a virtual component, the core of the operation was a protest scheduled for August 15, 2011. Anonymous launched OpBART in response to actions that authorities of San Francisco's Bay Area Rapid Transit (BART) took on August 11th, when they turned off cell phone service temporarily as a reaction to a planned peaceful protest that day. The planned protest was in response to the fatal shooting of Charles Hill by BART police in July 2011; police allegedly shot the 45-year-old man three times at close proximity.[206] The action attracted criticism from the American Civil Liberties Union and the Electronic Frontiers Foundation, and tech website *Ars Technica* asked, "Did San Francisco's subway pull a Mubarak?"[207]

The cell phone shut off caught Anonymous's attention, and the group quickly planned three days of action. On the first day, August 13th, Anonymous raided BART offices with copies of its message; on August 14th, Anonymous attempted to take the BART website down using DDoS, but the attack was unsuccessful because BART uses cloud hosting, insusceptible to DDoS attacks. Anons did, however, manage to vandalize the BART webpage by inserting their own image.[208] When the DDoS attack failed, Anonymous chose to release the personal data of at least 2,400 BART customers in order to embarrass BART, demonstrating that it did not keep its customers information safe.[209]

The third day of planned action was an August 15th protest at the Civic Center. In its press release Anonymous requests that everyone wear red to remember those killed by the BART police.

---

[206] Michael Stone, "Operation BART: Anonymous protests San Fran cell phone censorship," August 14, 2011, *Examiner.com*, http://www.examiner.com/anonymous-in-national/operation-bart-anonymous-protests-san-fran-cell-phone-censorship (accessed March 30, 2012).
[207] Matthew Lasar, "Scenes from an Anonymous protest: Did San Francisco's subway 'pull a Mubarak'?" *Ars Technica*, August 2011, http://arstechnica.com/tech-policy/news/2011/08/did-bart-pull-a-mubarak-in-san-francisco.ars (accessed March 30, 2012).
[208] Ragan.
[209] Ragan.

The group also says in the press release, "We also encourage you to bring cameras to record any further abuse by police, and to legitimize the protest. Remember to bring your mask, and remember that this is a peaceful protest,"[210] the protest went smoothly, and cell phone service remained on the whole time. OpBART shows that Anonymous actions do not only happen online; Anonymous broad support base and sizable virtual presence actually gives it a unique platform upon which to draw support for real world protests and redress real world grievances.

HBGary Federal

The attack on HBGary Federal, a technology security company that sells its products to the US government, was not a typical AnonOp. It was not an AnonOp at all; it was a raid to embarrass the CEO, Aaron Barr. In 2010, Barr claimed that he could use data from social media sites to learn the real life identities of high profile Anons. Barr began his experiment, and in early 2011 he announced in an interview with *The Financial Times* that he planned to release the identities he had discovered. The day after the article was published, Anonymous launched a DDoS attack on the HBGary Federal website; by the next day Anons had successfully infiltrated the website and accessed the email server. After watching Barr's communications for 30 hours, Anonymous released over 40,000 emails from HBGary Federal on The Pirate Bay and deleted one terabyte of backup data just for good measure. The new homepage of HBGary Federal read, "now the Anonymous hand is bitch-slapping you in the face."[211]

---

[210] anonyops, "Anonymous: Operation BART," *Youtube*, August 13, 2011, http://www.youtube.com/watch?feature=player_embedded&v=o10k3M0-L9E (accessed March 30, 2012).
[211] Nate Anderson, "How one man tracked down Anonymous—and paid a heavy price," *Ars Technica*, February 2011, http://arstechnica.com/tech-policy/news/2011/02/how-one-security-firm-tracked-anonymousand-paid-a-heavy-price.ars/3 (accessed March 30, 2012).

The attack against HBGary Federal was motivated by vengeance more than it was any moral outrage. Barr had threatened to out Anonymous, with false intel no less, and Anonymous took the opportunity to embarrass Barr and the company. Anonymous d0xed HBGary Federal and Barr, releasing their supposed identities as well as Barr's own personal correspondences. Barr's method for verifying identity, detailed in Nate Anderson's article "How one man tracked down Anonymous—and paid a heavy price," for *Ars Technica*, was revealed to be not only inaccurate, but also entirely pedestrian. Anderson also reports that that even the coder Barr worked with also had serious reservations about Barr's 'analysis' because it was based completely on speculation; it involved no algorithms and not a single line of code. The HBGary Federal hack was a chance for Anons to prove their hacking prowess as well as demonstrate the very real consequences of virtual action: after the hack, many companies were less inclined to contract HBGary for technology security projects. [212] Similarly, after Anons hacked and d0xed the BART website, BART had to not only beef up its website security but also issue a statement to assure customers that their data was in fact safe.

The HBGary Federal attack is unique from the AnonOps presented earlier because the group behind the colossal d0xing endeavor was not Anonymous, but Lulz Security (LulzSec), an offshoot hacker-troll organization that delights in disruption. LulzSec is made up of six Anons, including storied Anonymous leader 'Sabu', who was recently revealed to be an FBI informant. (Sabu, also known as Hector Xavier Monsegur is a computer security specialist living in New York City and was not known to the FBI during the HBGary attack.) This summer the group went on a 50-day tour of

[212] Anderson, "How one man tracked down Anonymous—and paid a heavy price."

mayhem, taking down government websites like CIA.gov and exposing passwords.[213] At the end of their tour, LulzSec issued a statement:

> For the past 50 days we've been disrupting and exposing corporations, governments, often the general population itself, and quite possibly everything in between, just because we could. All to selflessly entertain others – vanity, fame, recognition, all of these things are shadowed by our desire for that which we all love. The raw, uninterrupted, chaotic thrill of entertainment and anarchy. It's what we all crave, even the seemingly lifeless politicians and emotionless, middle-aged self-titled failures. You are not failures. You have not blown away. You can get what you want and you are worth having it, believe in yourself.
>
> Let it flow…
>
> Lulz Security – our crew of six wishes you a happy 2011, and a shout-out to all of our battlefleet members and supporters across the globe.[214]

After LulzSec disbanded, members of LulzSec joined forces with Anonymous to form Operation AntiSec, devoted to stealing and leaking any classified information, emails, and documentation from the government, banks, or other significant institutions.[215]

LulzSec and AntiSec are anarchic, tempestuous operations in unabashed pursuit of the lulz; they stand in stark contrast with today's Anonymous, which more often than not takes on 'big' operations with moral significance. As evidenced by Operation Payback, Operation Avenge Assange, OpTunisia, OpEgypt, and OpBART, today's Anonymous is a positive social force, whereas LulzSec and AntiSec are destabilizing ones. Anonymous and AntiSec though, are not that different: both show spectators that authority is a social construct. Anonymous does so by encouraging people to re-envision and recreate their world; AntiSec does so by mercilessly revealing the powers that be as

---

[213] Joe Weisenthal, "Notorious Hacker Group LulzSec Just Announced That It's Finished," *Business Insider*, June 25, 2011, http://www.businessinsider.com/lulzsec-finished-2011-6 (accessed March 30, 2012).
[214] Weisenthal, "Notorious Hacker Group LulzSec Just Announced That It's Finished."
[215] Nick Ross, "Lulzsec teams up with Anonymous," *ABC Australia*, June 20, 2011, http://www.abc.net.au/technology/articles/2011/06/20/3248520.htm (accessed March 30, 2012).

frauds. They are two sides to the same coin: trolls and moral crusaders hacking a new global power structure.

———

Josh Corman, research director at The 451 Group, an information technology analysis and research firm, describes the people behind hacks like the one at HBGary, "These are ideological insiders that have access; this is more like Fight Club; they do your laundry, they work in the mailroom. This is a whole counterculture thing; especially in a time when people feel powerless. They find this empowering."[216] Operation Payback and Avenge Assange was for free access to information; Operation Tunisia and Egypt were for freedom for mankind; the HBGary hack was for individual empowerment. Whether or not you agree with the actions taken by Anonymous and LulzSec, it is undeniable that they are of major consequence and will continue to reveal their significance at time goes on. Anonymous actions may well prove that technology can "bring unprecedented change for the good."[217]

[216] Jerome Taylor, "Who are the group behind this week's CIA attack?" *The Independent*, June 16, 2011, http://www.independent.co.uk/news/world/americas/who-are-the-group-behind-this-weeks-cia-hack-2298430.html (accessed March 30, 2012).
[217] Wu, 276.

CHAPTER 5

Conclusion: What do we have to fear from hacktivism, the lulz, and the hive mind?

On February 15, 2011, Secretary of State Hillary Clinton gave a speech at George Washington University on the US Department of State's "Internet Freedom Agenda." In the speech, Clinton championed what she labels the 'freedom to connect': the freedom of expression, association, and assembly online. Clinton addresses the audience, "The Internet has become the public space of the 21st century—the world's town square, classroom, marketplace, coffeehouse, and nightclub. We all shape and are shaped by what happens there, all 2 billion of us and counting."[218] Today's internet represents the marketplace of ideas: it is the ultimate library and represents the ultimate democracy because everyone has a voice. The internet has great potential to revolutionize our world, however, Clinton cites three challenges we face in ensuring that the internet operates at its full potential and "delivers the greatest possible benefits to the world."[219]

The problem that Clinton identifies is one discussed in Chapter 2 of this thesis: there is no agreement on the principles or ethics of internet usage. The open structure of the internet was invaluable to creating the internet that we had today because the architecture is customizable and interactive. Anyone was able to turn the technology into what they needed or wanted it to be and then share their creation publicly; the open internet fostered creativity and community. However, today the open internet faces a number of obstacles that we as its users must be invested in overcoming. The internet is a generative technology, but it cannot generate anything on its own. It is the job of internet users to make it the public space that we want it to be.

---

[218] Hillary Clinton, "Internet Rights and Wrongs: Choices & Challenges in a Networked World," *US Department of State*, Speech at George Washington University, Washington, DC, February 15, 2011, http://www.state.gov/secretary/rm/2011/02/156619.htm (accessed April 2, 2012).
[219] Clinton.

Clinton identifies three challenges that the open internet presents: first is the challenge to achieve both liberty and security online. "Without security," she reminds, the audience, "liberty is fragile. Without liberty, security is oppressive," and both security and liberty are necessary to ensure our basic freedoms. The internet's structure is highly customizable and it is important to remember that it can be used for good, but it can just as easily be used towards nefarious ends that threaten security and liberty. The second challenge she identifies is one to protect both transparency and confidentiality. The internet democratizes knowledge and information and encourages government transparency, making them more accessible to the people. However, as discussed in Chapter 4 of this thesis, information is not always secure online, especially when hackers are involved. If we cannot be sure that our private information will remain confidential, we cannot fully enjoy security and basic freedoms. The third challenge is one discussed in Chapters 1 and 3 of this thesis, how to protect "free expression while fostering tolerance and civility."[220] Chapters 1 and 3 showed that the only way to protect free expression while fostering tolerance and civility is self-regulation; the community must choose and enforce its own standards. Like in the real world, there is no good way to restrict offensive speech, "Instead, as it has historically been proven time and time again, the better answer to offensive speech is more speech."[221]

For all of the challenges that the open internet presents to us today, it is still a tool for profound positive social change; Clinton discusses the revolution in Egypt. Egyptians had been organizing on Twitter and Facebook; everyone had the power to be a journalist, posting news worthy photos and videos online; the whole world was watching on January 28, 2011, when the

[220] Clinton.
[221] Clinton.

internet went dark because the Egyptian government had blocked access.[222] Now, it's interesting because even when the internet was turned off in Egypt, the revolution went on. In this thesis I have discussed the role of the internet as a vehicle for social change at length, but Egypt's example challenges the assumption that the internet is critical to a successful social movement. Evgeny Morozov, a commentator on the political consequences of the internet and the author of *Net Delusion: The Dark Side of Internet Freedom*, argues that the internet is overestimated as a positive influencer for social movements. There were social movements and revolutions before the internet. Furthermore, free internet effects many other things besides social movements: the internet facilitates organization, but it also has a profound potential effect on peoples thoughts and opinions, which are equally important to revolution as organization, if not more so.

The internet is a vehicle for social change in part because it makes possible the rapid spread of information and efficient social organization. However, the internet is also important because of how it connects people, Clay Shirky says, "One of the places I think the debate has gone awry is in overestimating the importance of the value of access to information, and we've underestimated the importance of access of value to people. This is a mistake that dates from the dawn of the Internet."[223] The internet, begun as a government research project, is recognized primarily for its wealth of information and that makes it a revolutionary technology. However the internet is really revolutionary as a tool that connects people and empowers them to value or not value what they access online. The advent of the internet led to an unprecedented amount of public information, but it also brought about an unprecedented level of interconnectivity between people that might be more important.

---

[222] Clinton.
[223] Clay Shirky quoted in "Digital Power and its Discontents," *Edge*, April 12, 2010, http://edge.org/3rd_culture/morozov_shirky10/morozov_shirky10_index.html (accessed April 2, 2012).

In this thesis, I have argued that the hive mind Anonymous famous for online pranks poses a serious challenge to contemporary society and should be taken very seriously. Anonymous is accused of being devoid of ideological conviction, however AnonOps like Project Chanology and Operation Payback show that Anons are in fact motivated by higher principles, especially the freedom of expression. What makes Anonymous so hard to grasp is that it is an online collective of individuals, not an expression of a singular ideology. When Anonymous raids in the name of freedom of expression, Anonymous raids for people, not for the idea. Anonymous utilizes the internet as a tool to help people self-actualize. Anonymous does not overestimate the importance of the value of access of information because as a collective of individuals, its value is based on the connections between people. People are the ones who produce information. This is why groups like Anonymous, LulzSec, and AntiSec go after big corporations and government agencies—it is to challenge our preconceptions of who actually produces and controls information.

Anonymous poses an important challenge to society. But, much of what Anonymous does is also misuse of the tools of technology; while the Stratfor hack certainly challenged authority, it is not obvious that the challenge was necessary. In this thesis I argued that Anonymous, while in pursuit of the lulz, anarchic cyber-fun, is not ipso facto devoid of ideological conviction; however I did not argue that the ideological conviction was not malevolent. The group is too decentralized for there to be an obvious spirit to its motivations: sometimes, like in the case of OpBART, the praxis and principles both seem virtuous. Other operations, like the Statfor hack, seem malevolent.

Regardless of whether or not what Anonymous is doing is virtuous, ethical, malevolent—what have you—it is undeniable that the group is relevant. In Chapter 2 I demonstrated how cyberspace has become a part of our daily lives, and that groups like Anonymous therefore affect

everybody. Chapters 3 and 4 explore the consequences of Anonymous actions, showing that the operations are serious and have real consequences. Groups like Anonymous encourage discussion and exemplify a commitment to the marketplace of ideas; groups like Anonymous rely on the open network. If Anonymous is perceived as a threat it is more important that experts engage in dialogue around how to secure your computer and network from a hack instead of irresponsibly limiting the network, a valuable and necessary resource for freedom of expression.

No matter whether or not groups like Anonymous exist, it is important that, in the age of informationalism, we are net savvy. This thesis originally asked the question: what do we have the fear from hacktivism, the lulz, and the hive mind? The answer is nothing really. Hacktivism, the lulz, and the hive mind are not inherently dangerous, they are actually important tools for realizing social change. During the Brookings Institution panel discussion, "Hacktivism, Vigilantism, and Collective Action in a Digital Age," Richard Forno said:

> But, for policymakers, at least those with a degree of humility, I would say before we enable a large set of massive changes of government policy and restructuring of the internet, because I sort of think the candid answer is that though Anonymous generates a great deal of fear and a great deal of media attention, the true scope of the harm that it ahs caused is relatively modest; certainly not existential, at least not yet. And perhaps you fear that they might become an existential threat down the road, but at least, as a first approximation right now, it's kind of like crime, right? You can't eradicate it, you just kind of worry about it. You try and reduce it a little, but we're never going to reach a world in which there are no murders. And I suspect that absent massive change, we'll never reach a world in which there are no Anonymouses; period, full stop. So maybe we just live with it.

So, maybe we should just live with hacktivism, the lulz, and the hive mind. The future has already arrived after all.

AFTERWORD

I would like to thank Diet Coke for giving me life force, Mariah Carey for reminding me that I can make it through the rain, and the internet for inspiring this thesis and making sure that I never felt lonely.

I would also like to thank Professor Vaidhyanathan for his guidance throughout the thesis process and Professor Smith, for being an amazing professor and always giving the most unique advice.

WORKS CITED

4chan.org. Accessed October 25, 2011.

Aleteuk. "Tom Cruise Scientology Video – (Original UNCUT)." *YouTube*. Online Video Clip. January 17, 2008. http://www.youtube.com/watch?v=UFBZ_uAbxS0 (accessed 24 March 2012).

Anderson, Nate. "Gene Simmons vs. Anonymous: Who's the bigger tool?" *Ars Technica*. October 2010. http://arstechnica.com/tech-policy/news/2010/10/gene-simmons-vs-anonymous-whos-the-bigger-asshole.ars (accessed March 30, 2012).

———"How one man tracked down Anonymous—and paid a heavy price." *Ars Technica*. February 2011. http://arstechnica.com/tech-policy/news/2011/02/how-one-security-firm-tracked-anonymousand-paid-a-heavy-price.ars/3 (accessed March 30, 2012).

Anonymousworldwar3. "ANONYMOUS – OPERATION TUNISIA – A Press Release." *YouTube*. Online Video Clip. January 5, 2011. http://www.youtube.com/watch?v=BFLaBRk9wY0 (accessed March 30, 2012).

anonyops. "Anonymous: Operation BART." *YouTube*. Online Video Clip. August 13, 2011. http://www.youtube.com/watch?feature=player_embedded&v=o10k3M0-L9E (accessed March 30, 2012).

Auerbach, David. "Anonymity as Culture: Treatise." *Triple Canopy*, Issue 15 (February 9, 2012). http://canopycanopycanopy.com/15/anonymity_as_culture__treatise (accessed March 18, 2012).

Baym, Nancy. *Personal Connections in the Digital Age*. Malden, Massachusetts: Polity Press, 2010.

Berners-Lee, Tim. *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by its Inventor.* New York: Harper Collins, 1999.

Bickford, Robert. "Are You a Hacker?" 1989. http://www.textfiles.com/hacking/hacker.txt (accessed March 18, 2012).

"brb church – chris forcand." *chanarchive.org*. October 14, 2007. http://chanarchive.org/4chan/b/1032/brb-church-chris-forcand, (accessed March 23, 2012).

Bright, Peter. "Anonymous speaks: the inside story of the HB Gary attack." *Ars Technica*. Spring 2011. http://arstechnica.com/tech-policy/news/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack.ars (accessed March 25, 2012).

Church0fScientology. "Message to Scientology." *YouTube*. Online Video Clip. January 21, 2008. http://www.youtube.com/watch?feature=player_embedded&v=JCbKv9yiLiQ (accessed March 24, 2012).

Chen, Adrian. "The Art of Trolling: Inside a 4chan Smear Campaign." *Gawker*. July 17, 2010. http://gawker.com/5589721/the-art-of-trolling-inside-a-4chan-smear-campaign (accessed March 4, 2012).
———"How 4chan Brought the Evil British Cat Bin Woman to Justice." *Gawker*. August 25, 2010. http://gawker.com/5622237/how-4chan-brought-the-evil-british-cat-lady-to-justice (accessed 23 March 2012).
———"How the Internet Beat Up an 11-Year-Old Girl." *Gawker*. July 16, 2010. http://gawker.com/5589103/how-the-internet-beat-up-an-11+year+old-girl?skyline=true&s=I, (accessed March 4, 2012).
———"Puppy-Throwing Girl Caught in Bosnia." *Gawker*. September 3, 2010. http://gawker.com/5629513/puppy+throwing-girl-caught-in-bosnia (accessed March 23, 2012).
——— "These are the Faces of Anonymous." *Gawker*. September 9, 2011. http://gawker.com/5838756/these-are-the-pale-faces-of-anonymous/gallery/1 (accessed March 23, 2012).
———"*Transformers* Director Michael Bay Offers $50,000 Bounty for Puppy-Throwing Girl." *Gawker*. September 1, 2010, http://gawker.com/5628051/transformers-director-michael-bay-offers-50000-bounty-for-puppy+throwing-girl (accessed 23 March 2012).
———"Vigilante Hackers Wage War on Underground Kiddie Porn." *Gawker*. October 21, 2011. http://gawker.com/5851459/vigilante-hackers-wage-war-on-underground-kiddie-porn (accessed 23 March 2012).

Clinton, Hillary. "Internet Rights and Wrongs: Choices & Challenges in a Networked World." *US Department of State*. Speech at George Washington University, Washington, DC. February 15, 2011. http://www.state.gov/secretary/rm/2011/02/156619.htm (accessed April 2, 2012).

Coleman, Gabriella, and Alex Golub. "Hacker practice: Moral genres and the cultural articulation of liberalism." *Anthropological Theory* Vol. 8, 3 (2008): 255-277.

Coleman, Gabriella. "Anonymous: From the Lulz to Collective Action." *The New Everyday*. April 6, 2011. http://mediacommons.futureofthebook.org/tne/pieces/anonymous-lulz-collective-action (accessed March 6, 2012).
———"The Anthropology of Hackers." *The Atlantic*. September 21, 2010.
———"Hacker and Troller as Trickster." *Social Text Journal*. February 7, 2010. http://www.socialtextjournal.org/blog_dev/2010/02/hacker-and-troller-as-trickster.php (accessed March 18, 2012).
———"Our Weirdness is Free." *Triple Canopy*, Issue 15 (February 9, 2012). http://canopycanopycanopy.com/15/our_weirdness_is_free (accessed February 12, 2012).

Conway, Maura. "Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet." *First Monday* 7:11 (November 2002). http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/1001/922 (accessed April 1, 2012).

Corrons, Luis. "4chan Users Organize Surgical Strike against the MPAA." *PandaLabs*. September 17, 2010. http://pandalabs.pandasecurity.com/4chan-users-organize-ddos-against-mpaa/ (accessed March 30, 2012).

coventrytelegraph. "Women throws cat in wheelie bin." *YouTube*. Online Video Clip. August 25, 2012. http://www.youtube.com/watch?feature=player_embedded&v=zbMt82yVj24 (accessed March 23, 2012).

Daly, Angela. "Private power and new media: the case of the corporate suppression of Wikileaks and its implications for the exercise of fundamental rights on the Internet." Paper presented at the 4th international conference on Information Law, ICIL 2011, Thessaloniki, Greece, May 20-1, 2011.

DARPA. www.darpa.mil (Accessed December 2, 2011).

Denning, Dorothy. "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy." *Nautilus Institute*. June 8, 2001. http://faculty.nps.edu/dedennin/publications/Activism-Hacktivism-Cyberterrorism.pdf (accessed March 23, 2012).

Denton, Nick. "The Cruise Indoctrination Video Scientology Tried to Suppress." *Gawker*. January 15, 2008. http://gawker.com/5002269/the-cruise-indoctrination-video-scientology-tried-to-suppress (accessed March 24, 2012).

Dibbell, Julian. "The Assclown Offensive: How to Enrage the Church of Scientology." *Wired*. September 21, 2009. http://www.wired.com/culture/culturereviews/magazine/17-10/mf_chanology?currentPage=all (accessed March 29, 2012).

Douglas, Nick. "What The Hell Are 4chan, ED, Something Awful, And 'b'?" *Gawker*. January 8, 2008, http://gawker.com/346385/what-the-hell-are-4chan-ed-something-awful-and-b (accessed March 8, 2012).

Emspak, Jesse. "Update: Egyptian Gov't Web Sites Under Attack." *International Business Times*. January 26, 2011. http://www.ibtimes.com/articles/105329/20110126/update-egyptian-gov-t-web-sites-under-attack.htm (accessed March 30, 2012).

Enigmax. "ACS:Law Anti-Piracy Law Firm Torn Apart by Leaked Emails." *Torrent Freak*. September 25, 2010. http://torrentfreak.com/acslaw-anti-piracy-law-firm-torn-apart-by-leaked-emails-100925/ (accessed March 30, 2012).

Ernesto. "Behind the Scenes at Anonymous' Operation Payback." *Torrent Freak*. November 15, 2010. http://torrentfreak.com/behind-the-scenes-at-anonymous-operation-payback-111015/ (accessed March 30, 2012).

Ernesto. "Movie Rental Outfit Hacked, Emails Leaked, Redirected to The Pirate Bay." October 18, 2010. http://torrentfreak.com/movie-rental-outfit-hacked-emails-leaked-redirected-to-the-pirate-bay-101018/ (accessed March 30, 2012).

FLSnag. "I Am One Anonymous." *YouTube*. Online Video Clip. July 23, 2011. http://www.youtube.com/watch?v=aEcvaoDIKtU (accessed March 5, 2012).

Friedman, Allan A. et. al. "Hacktivism, Vigilantism and Collective Action in the Digital Age," *The Brookings Institution*. Panel Discussion. Washington, DC, December 9, 2011.

Goodrum, Abby, and Mark Manion. "Terrorism or Civil Disobedience: Toward a Hacktivist Ethic." *Computers and Society* 30: 2 (June 2000): 14-19.

Grigoriadis, Vanessa. "4chan's Chaos Theory." *Vanity Fair*. April 2011.

Halliday, Josh. "Police arrest five over Anonymous WikiLeaks attacks." *The Guardian*. January 27, 2011. http://www.guardian.co.uk/technology/2011/jan/27/anonymous-hacking (accessed March 23, 2012).

Halupka, Max, and Cassandra Star. "The Utilisation of Direct Democracy and Meritocracy in the Decision Making Process of the Decentralised Virtual Community Anonymous." Paper presented at the Australian Political Studies Association Conference 2011, Canberra, Australia, September 26-28, 2011.

Himamen, Pekka. The Hacker Ethic. New York: Random House, 2001.

"How the Web Began." European Organization for Nuclear Research (CERN). http://user.web.cern.ch/public/en/About/WebStory-en.html (Accessed December 2, 2011).

Idkwhat. "Chris Forcand." *Oh Internet*. http://ohinternet.com/Chris_Forcand (accessed March 23, 2012).

Ito, et al. *Living and Learning with New Media: Summary of Findings from the Digital Youth Project*. Chicago, Illinois: The MacArthur Foundation, 2008.

Jardin, Xeni. "4 chan 'backtraced,' reported to the 'cyberpolice' by mustachioed mad dad." *Boing Boing*. July 16, 2010. http://www.boingboing.net/2010/07/16/mad-mustachioed-dad.html (access March 4, 2012).

Jenkins, Jonathan. "Man trolled web for girls:cops."*Canoe*. December 7, 2007. http://cnews.canoe.ca/CNEWS/Crime/2007/12/07/4712680-sun.html (accessed March 23, 2012).

"Jessi Slaughter." *Know your meme*. http://knowyourmeme.com/memes/events/jessi-slaughter (accessed March 4, 2012).

Keller, Greg. "Interpol: 25 Suspected Anonymous Hackers Arrested in New Crackdown." *Huffington Post*. February 28, 2012. http://www.huffingtonpost.com/2012/02/28/interpol-anonymous-hackers_n_1306630.html (accessed March 23, 2012).

Krotoski, Aleks. "The internet's cyber radicals: heroes of the web changing the world." *The Guardian*. November 27, 2010. http://www.guardian.co.uk/technology/2010/nov/28/internet-radicals-world-wide-web. Accessed October 25, 2011.

Landers, Chris. "Serious Business: Anonymous Takes on Scientology (and Doesn't Afraid of Anything)." *Baltimore City Paper*. April 2, 2008. http://www2.citypaper.com/columns/story.asp?id=15543 (accessed October 23, 2011).

Lasar, Matthew. "Scenes from an Anonymous protest: Did San Francisco's subway 'pull a Mubarak'?" *Ars Technica*. August 2011. http://arstechnica.com/tech-policy/news/2011/08/did-bart-pull-a-mubarak-in-san-francisco.ars (accessed March 30, 2012).

Leiner, Barry M., et. al., "Brief History of the Internet." *Internet Society*. 2011. http://www.internetsociety.org/internet/internet-51/history-internet/brief-history-internet (accessed March 15, 2012).

Ludlow, Peter. *Crypto Anarchy, Cyberstates, and Pirate Utopias.* Cambridge, Massachusetts: The MIT Press, 2001.
———"Wikileaks and Hacktivist Culture." *The Nation*. October 4, 2010.

Mansfield-Devine, Steven. "Anonymous: serious threat or mere annoyance?" *Network Security* Volume 2011, Issue 1 (January 2011): 4-10.
———"Hacktivism: Assessing the Damage." *Network Security* Volume 2011, Issue 8 (August 2011): 5-13.

Menn, Joseph. "They're watching. And they can bring you down." *The Financial Times*. September 23, 2011. http://www.ft.com/intl/cms/s/2/3645ac3c-e32b-11e0-bb55-00144feabdc0.html#axzz1gBiwxVlN (accessed December 9, 2011).

mmxanonymous. "OPERATION EGYPT: ANONYMOUS PRESS RELEASE – 26/01/2011." *YouTube*. Online Video Clip. January 26, 2011. http://www.youtube.com/watch?v=yOLc3B2V4AM (accessed March 30, 2012).

Morozov, Evgeny and Clay Shirky. "Digital Power and its Discontents." *Edge*. April 12, 2010. http://edge.org/3rd_culture/morozov_shirky10/morozov_shirky10_index.html (accessed April 2, 2012).

Newcomb, Peter, and Keenan Mayo "How the Web Was Won: An Oral History of the Internet." *Vanity Fair*, July 2008. http://www.vanityfair.com/culture/features/2008/07/internet200807?currentPage=1 (Accessed December 2, 2011).

Norton, Quinn. "2011: The Year Anonymous Took On Cops, Dictators, and Existential Dread." *Wired*. January 11, 2012. http://www.wired.com/threatlevel/2012/01/anonymous-dicators-existential-dread/ (accessed March 30, 2012).

OPDARKNET. "#OpDarknet Major Release & Timeline." *Pastebin*. October 18, 2011. http://pastebin.com/T1LHnzEW (accessed March 23, 2012).

Poulsen, Kevin. "Hackers Assault Epilepsy Patients via Computer." *Wired*. March 28, 2008. http://www.wired.com/politics/security/news/2008/03/epilepsy (accessed March 18, 2012).

Read, Max. "4chan on the Hunt for Puppy-Throwing Girl." *Gawker*. August 31 2010. http://gawker.com/5626105/4chan-on-the-hunt-for-puppy+throwing-girl?skyline=true&s=I (accessed 23 March 2012).

TheRealGothAlice. "I am Anonymous". January 29, 2008. *YouTube.* Online Video Clip. http://www.youtube.com/watch?v=WvPUxMZZiX0&feature=related (accessed December 9, 2011).

Ridgely, Sean. "Gabe Newell and Christopher Poole ousted from Victoria's Secret beauty contest." *Neoseeker*. August 27, 2009. http://www.neoseeker.com/news/11654-gabe-newell-and-moot-ousted-from-victorias-secret-beauty-contest/ (accessed December 12, 2011).

Ross, Nick. "Lulzsec teams up with Anonymous." *ABC Australia*. June 20, 2011. http://www.abc.net.au/technology/articles/2011/06/20/3248520.htm (accessed March 30, 2012).

Ryan, Yasmine. "Tunisia's bitter cyberwar." *Al Jazeera*. January 6, 2011. http://www.aljazeera.com/indepth/features/2011/01/20111614145839362.html (accessed March 30, 2012).

Schwartz, Mattathias. "The Trolls Among Us." *New York Times*. August 3, 2008.

Shirky, Clay. *Here Comes Everybody* New York: Penguin Press, 2008.

Single, Ryan. "Palin Hacker Group's All-Time Greatest Hits." *Wired*. September 19, 2008. http://www.wired.com/threatlevel/2008/09/palin-hacker-gr/ (accessed March 20, 2012).

Spafford, Eugene H. "Are Computer Hacker Break-ins Ethical?" *Department of Computer Science, Purdue University*. 1989. http://webcache.googleusercontent.com/search?q=cache:fYGDDVF0DG0J:spaf.cerias.purdue.edu/tech-reps/994.ps+&cd=2&hl=en&ct=clnk&gl=us (accessed March 30, 2012).

Stone, Michael. "Operation BART: Anonymous protests San Fran cell phone censorship." August 14, 2011. *Examiner.com*. http://www.examiner.com/anonymous-in-national/operation-bart-anonymous-protests-san-fran-cell-phone-censorship (accessed March 30, 2012).

Taylor, Jerome. "Who are the group behind this week's CIA attack?" *The Independent*. June 16, 2011. http://www.independent.co.uk/news/world/americas/who-are-the-group-behind-this-weeks-cia-hack-2298430.html (accessed March 30, 2012).

Thomas, Jim. "The moral ambiguity of social control in cyberspace: a retro-assessment of the 'golden age' of hacking." *New Media Society* 7: 599 (2005): 599-624.

Vaidhaynathan, Siva. *The Anarchist in the Library.* New York: Basic Books, 2004.

Wagenseil, Paul. "Anonymous 'hacktivists' attack Egyptian websites." *Security News Daily*. January 26, 2011. http://www.msnbc.msn.com/id/41280813/ns/technology_and_science-security/#.T3bs0r9SR7E (accessed March 30, 2012).

Wark, McKenzie. *A Hacker Manifesto*. United States of America: Harvard University Press, 2004.

Weisenthal, Joe. "Notorious Hacker Group LulzSec Just Announced That It's Finished." *Business Insider*. June 25, 2011. http://www.businessinsider.com/lulzsec-finished-2011-6 (accessed March 30, 2012).

Weisman, Jonathan. "After an Online Firestorm, Congress Shelves Antipiracy Bills." *The New York Times*. January 20, 2012. http://www.nytimes.com/2012/01/21/technology/senate-postpones-piracy-vote.html?_r=1 (accessed March 30, 2012).

Why We Protest. https://whyweprotest.net/anonymous-scientology/scientology/scientology-dangers/ (accessed March 29, 2012).

Williams, Christopher. "Piracy Lawyer Mocks 4chan DDoS Attack." *The Register*. September 22, 2010. http://www.theregister.co.uk/2010/09/22/acs_4chan/ (accessed March 30, 2012).

Wu, Tim. *The Master Switch*. New York: Alfred A Knopf, 2010.

Winter, Jana. "EXCLUSIVE: Unmasking the world's most wanted hacker." *Fox News*. March 6, 2012. http://www.foxnews.com/scitech/2012/03/06/exclusive-unmasking-worlds-most-wanted-hacker/ (accessed March 13, 2012).

xkcd. "CIA." http://xkcd.com/932/ (accessed March 23, 2012).

xenutv1. "Scientology: XENU TV Speaks to Anonymous." *YouTube*. Online Video Clip. January 27, 2008. http://www.youtube.com/watch?feature=player_embedded&v=zW466xcM0Yk (accessed March 24, 2012).

Zetter, Kim. "FBI Arrests U.S. Suspect in LulzSec Sony Hack; Anonymous Also Targeted." *Wired*. September 22, 2011. http://www.wired.com/threatlevel/2011/09/sony-hack-arrest/ (accessed March 30, 2012).

Zittrain, Jonathan. *The Future of the Internet—And How to Stop It*. New Haven: Yale University Press, 2008.

Computer 'hacktivists' cause havoc targeting the websites of governments, companies and the police but who they are and what motivates them?Â Image caption 'V for Vendetta' Guy Fawkes masks are known as the symbol of Anonymous. Computer 'hacktivists' cause havoc targeting the websites of governments, companies and the police but who they are and what motivates them? The internet is not some playground that corporations and governments can take basic civil liberties with and destroy them and get away with it. Dr Steelhammer, Online activist. It is 4 o'clock in the morning and I'm waiting for a Skype call from a computer hacker on the run in Canada. With respect to hacktivism and cyberterrorism, those who engage in such activity are less likely to accomplish their foreign policy objectives than those who do not employ disruptive and destructive techniques. They may feel a sense of empowerment, because they can control government computers and get media attention, but that does not mean they will succeed in changing policy.Â They decide what is said and how. They do not have to rely on the mass media to take notice and tell their story "right." During the Kosovo conflict, organizations and individuals throughout the world used their Web sites to publish information related to the conflict and, in some cases, to solicit support.