Phreaks, Hackers, and Trolls

The Politics of Transgression and Spectacle

E. GABRIELLA COLEMAN

Among academics, journalists, and hackers, it is common to define hackers not only by their inquisitive demeanor, the extreme joy they garner from uninterrupted hacking sprints, and the technological artifacts they create but also by the “hacker ethic.” Journalist Steven Levy first defined the hacker ethic in Hackers: Heroes of the Revolution, published in 1984. The hacker ethic is shorthand for a mix of aesthetic and pragmatic imperatives: a commitment to information freedom, a mistrust of authority, a heightened dedication to meritocracy, and the firm belief that computers can be the basis for beauty and a better world.

In many respects, the fact that academics, journalists, and many hackers refer to the existence of this ethic is testament not only to the superb account that Levy offers—it is still one of the finest and most thoroughgoing accounts on hacking—but to the fact that the hacker ethic in the most general sense can be said to exist. For example, many of the principles motivating free and open-source software (F/OSS) philosophy reinstantiate, refine, extend, and clarify many of those original precepts.

However, over the years, the concept has been overly used and has become reified. Indeed as I learned more about the contemporary face of hacking and its history during the course of my fieldwork on free and open-source software hacking, I started to see significant problems in positing any simple connection between all hackers and an unchanging ethic. Falling back on the story of the hacker ethic elides tensions and differences that exist among hackers. Although hacker ethical principles may have a common core—one might even say a general ethos—further inquiry soon demonstrates that, similar to any cultural sphere, we can easily identify variance, ambiguity, and, at times, even serious points of contention.
Take for instance the outlandish and probably not entirely serious (but not entirely frivolous) accusation launched by a hacker bearing a spectacular and provocative name, the “UNIX Terrorist.” He is featured in the hacker e-zine Phrack, which reached its popular zenith in the late 1980s and the early 1990s. The UNIX Terrorist claims that a class of so-called hackers, those who write free and open-source software, such as the Linux operating system and the enormously popular Firefox browser, are not deserving of the moniker “hacker”:

Nowadays, it is claimed that the Chinese and even women are hacking things. Man, am I ever glad I got a chance to experience “the scene” before it degenerated completely. And remember, kids, knowing how to program or wanting really badly to figure out how things work inside doesn’t make you a hacker! Hacking boxes makes you a “hacker”! That’s right! Write your local representatives at Wikipedia/urban dictionary/OED and let them know that hackers are people that gain unauthorized access/privileges to computerized systems! Linus Torvalds isn’t a hacker! Richard Stallman isn’t a hacker! Niels Provos isn’t a hacker! Fat/ugly, maybe! Hackers, no! And what is up with the use of the term “cracker”? As far as I’m concerned, that term applies to people that bypass copyright protection mechanisms. Vladimir Levin? hacker. phiber optik? hacker. Kevin Mitnick? OK maybe a gay/bad one, but still was a “hacker.” Hope that’s clear.

Hackers do not universally invoke this type of policing between “good” and “bad” or “authentic” and “inauthentic.” Some hackers recognize the diversity of hacking and also acknowledge that, despite differences, hacking hangs together around a loose but interconnected set of issues, values, experiences, and artifacts. For instance, hackers tend to uphold a value for freedom, privacy, and access; they tend to adore computers—the cultural glue that binds them together; they are trained in highly specialized and technical esoteric arts, including programming, systems administration, and security research; some gain unauthorized access to technologies, though the degree of illegality greatly varies (and much of hacking is fully legal). Despite a parade of similarities, if we are to understand the political and cultural significance of hacking and its role in shaping and influencing segments of contemporary Internet cultures—such as Internet trolling—every effort must be made to address its ethical and social variability.

While Levy, and countless others, locate the birth of hacking at MIT and similar university institutions during the late 1950s, it may be more accu-
rate to identify MIT as the place where one variant of hacking got its start. Another variant began in the 1950s with telephone phreakers, who were the direct ancestors to underground hackers like the UNIX Terrorist. Phreakers studied, explored, and entered the phone system by re-creating the audio frequencies that the system used to route calls. Quite distinct from university-bred hackers whose ethical commitments exhibit a hyperextension of academic norms such as their elevation of meritocracy, these phone explorers exhibited other ethical and aesthetic sensibilities rooted in transgression (often by breaking the law or duping humans for information) and spectacle (often by mocking those in power). The institutional independence of phreakers, in combination with some early political influences, such as the Yippies (Youth International Party), made for a class of technologists whose aesthetic sensibilities and linguistic practices proved to be more daring, vivacious, audacious, and brash than what is commonly found in other genres of hacking, such as F/OSS.

As phreaking morphed into computer hacking in the late 1970s and early 1980s, this brash aesthetic tradition and the politics of transgression continued to grow in visibility and importance, especially evident in the literary genres—texts, files, and zines—produced by the hacker underground. In recent times, the aesthetics of audaciousness has veritably exploded with Internet trolls—a class of geek whose raison d'être is to engage in acts of merciless mockery/flaming or morally dicey pranking. These acts are often delivered in the most spectacular and often in the most ethically offensive terms possible.²

The behavior of trolls cannot, of course, be explained only by reference to the hacker underground or phreakers; nonetheless, as this essay will illustrate, there is a rich aesthetic tradition of spectacle and transgression at play with trolls, which includes the irreverent legacy of phreakers and the hacker underground. This aesthetic tradition demonstrates an important political attribute of spectacle: the marked hyperbole and spectacle among phreakers, hackers, and trolls not only makes it difficult to parse out truth from lies; it has made it difficult to decipher and understand the cultural politics of their actions. This evasiveness sits in marked contrast to other genealogies of hacking that are far easier to culturally decipher.

This drive toward cultural obfuscation is common to other edgy youth subcultures, according to cultural theorist Dick Hebdige. One of his most valuable insights, relevant to phreakers, hackers, and trolls, concerns the way that some subcultural groups have “translate[d] the fact of being under scrutiny into the pleasures of being watched, and the elaboration of..."
surfaces which takes place within it reveals a darker will toward opacity, a drive against classification and control, a desire to exceed.” This description, which Hebdige used to describe the “costers,” young and impoverished British boys who sold street wares and who flourished a century ago, could have just as well been written about phreakers, hackers, and trollers nearly a century later.

As the example of the UNIX Terrorist exemplifies, and as we will see below with other examples, these technologists “make a ‘spectacle’ of themselves, respond to surveillance as if they were expecting it, as if it were perfectly natural.” Even if they may vilify their trackers, they nonetheless take some degree of pleasure in performing the spectacle that is expected of them. Through forms of aesthetic audacity, a black hole is also created that helps shield these technologists from easy comprehension and provides some inoculation against forms of cultural co-optation and capitalist commodification that so commonly prey on subcultural forms.10

In the rest of the essay, I narrow my analysis to phreakers, underground hackers, and Internet trolls. The point here is not to fully isolate them from other types of hacking or tinkering, nor is it to provide, in any substantial manner, the historical connections between them. Rather it provides in broad strokes a basic historical sketch to illustrate the rich aesthetic tradition of spectacle that has existed for decades, all the while growing markedly in importance in recent years with Internet trolling.

1950–1960s: The Birth of Phone Exploration, Freaking, and Phreaking

Currently, the history of phone exploring, freaking, and phreaking exists only in fragments and scraps, although basic details have been covered in various books, public lectures, and Internet sites.11 Most accounts claim Joe Engressia, also known as Joy Bubbles, as their spiritual father, although others were already experimenting with the phone network in this period. Blind since birth and with perfect pitch, Engressia spent countless hours playing at home with his phone. In 1957, at the age of eight, he discovered he could “stop” the phone by whistling at a certain pitch, later discovered to be a 2600 hertz tone, into the receiver. Eventually, the media showcased this blind whiz kid, and local coverage most likely inspired others to follow in his footsteps.

In the late 1950s, the first glimmerings of phone explorations thus flickered, although only sporadically. Largely due to a set of technological changes, phreaking glimmered more consistently in the 1960s, although it
was still well below general public view. By 1961, phreakers—although still not named as such—no longer had to rely on perfect pitch to make their way into the phone system. They were building and using an assortment of small electrical boxes, the most famous of these being the Blue Box. This device was used to replicate the tones used by the telephone switching system to route calls, enabling Blue Box users to act as if they were a telephone operator, facilitating their spelunking of the phone system and, for some, free phone calls. Phreakers drew up and released schematics, or detailed “Box plans,” allowing others to construct them at home. Eventually, further technical discoveries enabled phreakers to set up telephone conferences, also known as “party lines,” where they congregated together to chat, gossip, and share technological information. By the late 1960s, a “larger, nationwide phone phreak community began to form,” notes historian of phreaking Phil Lapsely, and “the term ‘phone freak’ condensed out of the ambient cultural humidity.” Its codes of conduct and technical aesthetics were slowly but surely boiling, thickening into a regularized set of practices, ethics, commitments, and especially jargon—a sometimes impenetrable alphabet soup of acronyms—that no author who has written on phreakers and subsequently hackers has ever left without remark.

Hello World! The 1970s

In was only in the 1970s when phone freaking made its way out of its crevasse and into the public limelight through a trickle of highly influential journalistic accounts that also worked to produce the very technologists represented in these pieces. Thanks in particular to “Secrets of the Little Blue Box,” a provocative account published in 1971, mainstream Americans were given a window into the spelunkers of the phone system. The article, authored by Ron Rosenbaum, who coined the term “phreaker” was an instant sensation, for it revealed, in astonishingly remarkable detail, the practices and sensual world of phreaking. It focused on a colorful cast of characters with “strange” practices, names, and obsessions, who, according to Rosenbaum, were barely able to control their technological urges: “A tone of tightly restrained excitement enters the Captain’s voice,” wrote Rosenbaum, “when he starts talking about Systems. He begins to pronounce each syllable with the hushed deliberation of an obscene caller.” Rosenbaum wrote such a compelling account of phreaking that it inspired a crop of young male teenagers and adults (including two Steves: Wozniak and Jobs) to follow in the footsteps of the phreakers he showcased. The most famous of the featured phreakers was

Phreaks, Hackers, and Trolls
Captain Crunch, whose name references a toy whistle packaged in the sugary Cap'n Crunch brand cereal. Captain Crunch discovered that this whistle emitted the very 2600 hertz tone that provided one entryway into the phone system.

If journalists were spreading the word about these “renegade” technological enthusiasts throughout the 1970s, many phreakers and eventually hackers also took on literary pursuits of their own. In the 1980s they produced a flood of writing, often quite audacious in its form and content. In the early 1970s, however, the volume was only a steady trickle. In 1971, phreakers published a newsletter as part of their brief affiliation with an existing and well-known countercultural political movement, the Yippies. Founded in 1967, the Yippies, who resided on the far left of the political spectrum, became famous for promoting sexual and political anarchy and for the memorable and outrageous pranks they staged. Originally bearing the title YIPL (Youth International Party Line), the newsletter was later renamed TAP (the Technical Assistance Program). Over time, the editors of TAP dropped the overt politics, instead deriving “tremendous gut-level satisfaction from the sensation of pure technical power.”

For a number of years, however, YIPL blended technological knowledge with a clear political call to arms. For instance, the first issue, published in 1971, opens with a brief shout-out of thanks to the phreakers who contributed the technical details that would fill the pages of this DIY/rough-and-tumble newsletter: “We at YIPL would like to offer thanks to all you phreaks out there.” And it ends with a clear political statement:

YIPL believes that education alone cannot affect the System, but education can be an invaluable tool for those willing to use it. Specifically, YIPL will show you why something must be done immediately in regard, of course, to the improper control of the communication in this country by none other than bell telephone company.”

Published out of a small storefront office on Bleecker Street in Manhattan’s then seedy East Village neighborhood, the YIPL newsletter offered technical advice for making free phone calls, with the aid of hand-drawn schematics on pages also peppered with political slogans and images. For instance, these included a raised fist, a call to “Strike the War Machine,” and, important for our purposes here, the identification of AT&T as “Public Enemy Number 1.” A group of phreakers, who by and large had pursued their exploitations and explorations in apolitical terms, got married, at least for a brief period of
time, to an existing political movement. Although the marriage was brief, the Yippies nonetheless left their imprint on phreaking and eventually hacking.

Although phreakers were already in the habit of scorning AT&T, they had done so with at least a measure of respect. The zines YIPL, TAP, and eventually 2600 signaled a new history of the phreakers' (and eventually hackers') scornful crusade against AT&T. For example, in 1984, when TAP ceased to be, the hacker magazine and organization 2600 got its start. Largely, although not exclusively, focusing on computers, 2600 paid homage to its phone-phreaking roots in choosing its name and spent over two decades lampooning and critiquing AT&T (among other corporations and the government) with notable vigor.

1980s: “To Make a Thief, Make an Owner; to Create Crime, Create Laws”—Ursula Le Guin

Arguably one of the most influential legacies of the Yippies was their role in amplifying the audacious politics of pranking, transgression, and mockery that already existed among phreaks. However, it took another set of legal changes in the 1980s for the politics of transgression and spectacle to reach new, towering heights. By the 1980s, phreaking was still alive and kicking but was increasingly joined by a growing number of computer enthusiasts, many of them preteens and teens, who extended the politics of transgression into new technological terrains. During this decade, the mainstream media also closely yoked the hacker to the figure of the criminal—often in spectacular terms as well—an image buttressed by legal changes that outlawed for the first time certain classes of computer intrusions.

As in the past, other media representations also proved central in sparking the desire to hack, and few examples illustrate this better than the blockbuster 1983 movie War Games. Many hackers I interviewed, for example, recounted how watching the movie led to a desire to follow in the footsteps of the happy-go-lucky hacker figure David, whose smarts lead him to unwittingly hack his way into a government computer called WOPR, located at the North American Aerospace Defense Command Center (NORAD). After initiating a game of chess with the computer, David (unintentionally, of course) almost starts World War III. Most of the movie concentrates on his effort to stop the catastrophic end of the world by doing what hackers are famous for: subduing a recalcitrant and disobedient computer.

Apparently the movie appealed to a slew of nerdy types across Europe, Latin America, and the United States, leading them to incessantly demand
from their parents a PC and modem, which once they got, commanded their attention while they were logged on for hours on Bulletin Board Systems (BBSes). A BBS is a computerized meeting and announcement system where users could upload and download files, make announcements, play games, and have discussions. BBSes housed a wildly diverse mixture of information, from government UFO coverups to phreaking box schematics, as well as software to ingest. They also functioned like virtual warehouses filled with vast amounts of stand-alone texts, including genres like textfiles and zines, both of which significantly expanded the reach of the hacker underground, often broadcasting their message in audacious tones.

Textfiles, which were especially popular among underground hackers, spanned an enormously versatile subject range: anarchism, bomb building, schematics for electronics, manifestos, humorous tirades, UNIX guides, proper BBS etiquette, anti-Scientology rants, ASCII (text-based) porn, and even revenge tactics. A quite common type of textfile was box plans, schematics for electronics that showed how to use the phone system or other communication devices for unexpected (and sometimes illegal) purposes. Each textfile bears the same sparse aesthetic stamp: ASCII text, at times conjoined with some crude ASCII graphics. This visual simplicity sharply contrasts with the more audacious nature of the content. Take for example a textfile from 1984: “the code of the verbal warrior, or, [sic] barney’s bitch war manual,” which offered (quite practical) advice on the art of bitching.

```
the glue ball bbs------312-465-hack
barney badass’s b-files

/\///////\\/b-file #1\\///////\\//\\
the code of the verbal warrior, or,
barney’s bitch war manual
```

so you log onto a board and make a bee-line for your favorite sub-board, some people love pirate boards, some people like phreak boards. my passion is the trusty old standby, the bitch board.

so you get in the ‘argument den’, or ‘discussion board’, or ‘nuclear bitch-fare’ and start looking around for someone who you think you can out-rank. you know, insult, cut down, and generally verbally abuse. and so you
post, and, next thing you know, somebody appears to hate your guts. You’ve got an enemy. Now what?

The main problem with 85% of all bitching that goes on on boards today, is that people just don’t know how to handle the answer to that question. Now what? Do I keep it up? Do I give up? Do I insult his mother?

Barney’s bitch tip #1—Make up your mind. Either take the bitching completely seriously, or do not take it seriously at all. If you find yourself grinning at insults thrown at you by your opponent, then either cut it out immediately, or try grinning even wider when you’re typing your reply. The benefit of this is that you can’t be affected one way or the other by any thing that your opponent says. If you’re taking it seriously, then you just keep glaring at your monitor, and remain determined to grind the little filth into submission. If you’re using the lighthearted approach, then it’s pretty difficult to get annoyed by any kind of reference towards your mother/some chains and the family dog, because, remember, you’re not taking this seriously!

During the 1980s and through the 1990s, hackers were churning out these literary and political texts at rates that made it impossible for any individual to keep up with all of them. As cultural historian of hacking Douglas Thomas has persuasively argued, there was one publication, the electronic zine *Phrack*, that produced a shared footprint of attention among an otherwise sprawling crew of hackers and phreakers. Phrack was particularly influential during its first decade of publication, and its style honored and amplified the brash aesthetics of hacking/phreaking as it spread news about the hacker underground.

One of the most important sections of the zine was the hacker “Pro-Phile,” an example of which is the UNIX Terrorist’s Pro-Phile that appears at the beginning of this essay. Thomas explains its importance in the following terms:

The Pro-Phile feature was designed to enshrine hackers who had “retired” as the elder statesmen of the underground. The Pro-Philes became a kind of nostalgic romanticizing of hacker culture, akin to the write-up one expects in a high school yearbook, replete with “Favorite Things” and “Most Memorable Experiences.”

This material was not simply meant for the hacker public to ingest alone. In the case of *Phrack*, the audience included law enforcement, for this was

Phreaks, Hackers, and Trolls
the period when hackers were being watched closely and constantly. Like Hebdige’s costers, hackers conveyed the message that they too were watching back. The cat-and-mouse game of surveillance and countersurveillance among underground hackers and law enforcement amplified the existing propensity for hyperbole and trash talking that existed among phreakers and hackers. Their mockery of law enforcement, for example, not only abounded in the content featured in Phrack but was reflected in the very form of the zine. For instance, the structure of the Pro-Phile mirrors (and mocks) the FBI’s “Most Wanted” poster, listing such attributes as date of birth, height, eye color, and so on.25

Hackers’ expert command of technology, their ability to so easily dupe humans in their quest for information, and especially their ability to watch the watchers made them an especially subversive force to law enforcement. With society unable to pacify hackers through mere representation or traditional capitalist co-optation, a string of hackers were not simply legally prosecuted but also persecuted, with their punishment often exceeding the nature of their crime.27

1990s: “In the United States Hackers Were Public Enemy No. 1.”—Phiber Optik

Throughout the 1990s, the hacker underground was thriving, but an increasing number of these types of hackers were being nabbed and criminally prosecuted.28 Although there are many examples to draw on, the most famous case and set of trials concerns hacker and phone phreaker Kevin Mitnick.29 Throughout the 1980s and 1990s, he was arrested and convicted multiple times for various crimes, including computer fraud and possessing illegal long-distance access codes. Eventually the FBI placed him on the FBI’s “Most Wanted” list before they were able to track him down and arrest him in 1995, after a three-year manhunt. He was in jail for five years, although he spent over four of those as a pretrial detainee, during which time he was placed in solitary confinement for a year.30 Mitnick explained in an interview why this extreme measure was taken: “because a federal prosecutor told the judge that if I got to a phone I could connect to NORAD (North American Aerospace Command) and somehow launch an ICBM (Intercontinental Ballistic Missile).”31 Mitnick was unquestionably guilty of a string of crimes, although he never gained anything financially from his hacks. The extreme nature of his punishment was received as a warning message within the wider hacker community. “I was the guy
pinned up on the cross,” Kevin Mitnick told a packed room of hackers a couple of years after his release, “to deter you from hacking.”

At the time of Mitnick’s arrest, hackers took action by launching a “Free Kevin” campaign. Starting in the mid-1990s and continuing until Mitnick’s release in January 2002, the hacker underground engaged in both traditional and inventively new political activities during a vibrant, multiyear campaign: they marched in the streets, wrote editorials, made documentaries, and publicized his ordeal during the enormously popular hacker conference HOPE (Hackers on Planet Earth), held roughly every two years in New York City since 1994.

2000–2010: Good Grief! The Masses Have Come to Our Internet

Although the Internet was becoming more accessible throughout the 1990s, it was still largely off-limits, even to most North American and European citizens. By 2000, the floodgates started to open wide, especially with the spread of cheaper Internet connections. A host of new social media technologies, including blogs, wikis, social networking sites, and video-sharing sites, were being built and used by geeks and nongeeks to post messages, to share pictures, to chatter aimlessly, to throw ephemeral thoughts into the virtual wind, and to post videos and other related Internet memes. Internet memes are viral images, videos, and catchphrases under constant modification by users, and with a propensity to travel as fast as the Internet can move them.

During the period when large droves of people were joining the Internet, post-9/11 terrorism laws, which mandated stiff punishments for cybercrimes, and the string of hacker crackdowns of the 1980s and 1990s most likely made for a more reserved hacker underground. Without a doubt, cultural signs and signals of the hacker underground were and are still visible and vibrant. Hacker underground groups, such as Cult of the Dead Cow (CDC), continued to release software. Conferences popular among the underground, such as DEFCON and HOPE, continue to be wildly popular even to this day. Free from jail after two years, Kevin Mitnick delivered his humorous keynote address to an overflowing crowd of hackers at the 2004 HOPE conference, who listened to the figure who had commanded their political attention for over ten years.

Yet, with a few exceptions, the type of hacker Kevin Mitnick represents has become an endangered species in today’s North American and European cultural landscape. Trolls, on the other hand, have proliferated beyond their more limited existence prior to this decade. Trolls have transformed what
were more occasional and sporadic acts, often focused on virtual arguments called flaming or flame wars, into a full-blown set of cultural norms and set of linguistic practices. These codes are now so well established and documented that many others can, and have, followed in their footsteps.

Trolls work to remind the “masses” that have lapped onto the shores of the Internet that there is still a class of geeks who, as their name suggests, will cause Internet grief, hell, and misery; examples of trolling are legion. Griefers, one particular subset of troll, who roam in virtual worlds and games seeking to jam the normal protocols of gaming, might enact a relatively harmless prank, such as programming flying phalluses to pay a public visit in the popular virtual world Second Life during a high-profile CNET interview. Other pranks are far more morally dicey. During a virtual funeral held in the enormously popular massively multiplayer online game World of Warcraft, for a young player who had passed away in real life, griefers orchestrated a raid and mercilessly killed the unarmed virtual funeral entourage.

In the winter of 2007 and 2008, one group of trolls, bearing the name Anonymous, trolled the Church of Scientology after the church attempted to censor an internal video featuring Tom Cruise that had been leaked. (Eventually what was simply done for the sake of trolling grew into a more traditional protest movement.) One participant in the raids describes the first wave of trolling as “ultra coordinated motherfuckary [sic],” a description fitting for many instances of trolling:

The unified bulk of anonymous collaborated though [sic] massive chat rooms to engage in various forms of ultra coordinated motherfuckary [sic]. For very short periods of time between Jan 15th and 23rd Scientology websites were hacked, DDosed to remove them from the Internet, the Dianetics [sic] telephone hot line was completely bombarded with prank calls . . . and the “secrets” of their religion were blasted all over the internet, I also personally scanned my bare ass and faxed it to them. Because fuck them.

If hackers in the 1980s and 1990 were “bred by boards,” as Bruce Sterling has aptly remarked, trolls have been partly bred in one of the key descendants of boards: wildly popular image forums, like 4chan.org, which was founded in 2003. 4chan houses a series of topic-based forums where participants—all of them anonymous—post and often comment on discussions or images, many of these being esoteric, audacious, creative, humorous, heavily Photoshopped, and often very grotesque or pornographic. In contrast to many websites, the
posts on 4chan, along with their commentary, images, and video, are not archived. They are also posted at such an unbelievably fast pace and volume that much of what is produced effectively vanishes shortly after it is posted and viewed. These rapid-fire conditions magnify the need for audacious, unusual, gross, or funny content. This is especially true on the most popular and infamous of 4chan boards, /b/, the “random” board whose reigning logic combines topical randomness with aesthetic, linguistic, and visual extremity. “If you like the upbeat metaphor of the Internet as hive mind,” explains Rob Walker, “then maybe /b/ is one of the places where its unruly id lives.”

This board is a haven for most anything and thus has birthed many acts of trolling.

Like phreakers and hackers, some trolls act as historical archivists and informal ethnographers. They record and commemorate their pranks, trivia, language, and cultural mores in astonishing detail on a website called Encyclopedia Dramatica (ED). ED is written in a style and genre that, like Phrack, pays aesthetic homage and tribute to the brashness that the trolls it chronicles constantly spew out. Take for example, the definition of “troll” and “lulz,” a plural bastardization of laughing out loud (“lol”); lulz are often cited as the motivating emotional force and consequence of an act of trolling:

A troll is more than the embodiment of the internet hate machine, trolls are the ultimate anti-hero, trolls fuck shit up. Trolls exist to fuck with people, they fuck with people on every level, from their deepest held beliefs, to the trivial. They do this for many reasons, from boredom, to making people think, but most do it for the lulz.

Lulz is laughter at someone else’s expense. . . . This makes it inherently superior to lesser forms of humor. . . . The term lulz was coined by Jameth, and is the only good reason to do anything, from trolling to consensual sex. After every action taken, you must make the epilogic dubious disclaimer: “I did it for the lulz.” Sometimes you may see the word spelled as luls but only if you are reading something written by a faggot. It’s also Dutch for cock.”

As one will immediately notice, the very definition of “lulz” is a linguistic spectacle—one clearly meant to shock and offend through references to “cocks” and “faggots.” Trolls have taken political correctness, which reached its zenith in the 1980s and the 1990s, by the horns and not only tossed it out the window but made a mockery of the idea that language, much like everything virtual, is anything that should be taken seriously.
Clearly, trolls value pranking and offensiveness for the pleasure it affords. But pleasure is not always cut from the same cloth; it is a multivalent emotion with various incarnations and a rich, multifaceted history. Common to F/OSS developers, hacker pleasure approximates the Aristotelian theory of eudaimonia described by philosopher Martha Nussbaum as “the unimpeded performance of the activities that constitute happiness.”\(^4\) Hackers, in pushing their personal capacities and technologies to new horizons, experience the joy of what follows from the self-directed realization of skills, goals, and talents—more often than not achieved through computing technologies.

The lulz, on the other hand, celebrates a form of bliss that revels and celebrates in its own raw power and thus is a form of joy that, for the most part, is divorced from a moral hinge—such as the ethical love of technology. If underground hackers of the 1980s and 1990s acted out in brashness often for the pleasure of doing so, and as a way to perform to the watching eyes of the media and law enforcement, it was still largely hinged to the collective love of hacking/building and understanding technology. There was a balance between technological exploration and rude-boy behavior, even within the hacker underground that held an “elitist contempt” for anyone who simply used technological hacks for financial gain, as Bruce Sterling has put it.\(^4\)

At first blush, it thus might seem like trolls and griefers live by no moral code whatsoever, but among trolls and griefers, there is a form of moral restraint at work. However naive and problematic it is, this morality lies in the “wisdom” that one should keep one’s pranking ways on the Internet. Nothing represents this better than the definition for “Chronic Troll Syndrome,” also from Encyclopedia Dramatica. This entry uses the characteristically offensive and brash style to highlight the existence of some boundaries, although in reality this advice is routinely ignored:

Chronic Troll Syndrome (CTS) is an internet disease (not to be confused with Internet Disease) that is generally present in trolls. It causes the given troll to be unable to tell the difference between internet and IRL [in real life] limits.

As a result, the troll is no longer able to comprehend what is appropriate to say and do when dealing with IRL people in contrast with the Internets. Symptoms include being inconsiderate and generally asshatty to friends and family, the common offensive use of racial epithets, and a tendency to interfere in other people’s business uninvited “for the laughs.”\(^4\)

As so many Internet scholars insist, one should question any such tidy division between the virtual world and meatspace; further trolling often exceeds
the bounds of speech and the Internet when trolls “dox” (revealing social secu-
ritvity numbers, home addresses, etc.) individuals and send unpaid pizzas to tar-
get’s home, for instance. However problematic their division is, I would like
to suggest that when trolls draw this cultural line in the sand, they are also com-
menting on the massification of the Internet—a position that is quite con-
temptuous of newcomers. Although trolling has existed in some form since
people congregated online, trolling proliferated and exploded at the moment
the Internet became populated with non-technologically-minded people. The
brash behavior of trolls is especially offensive to people unfamiliar with this
world, and even for those familiar with this world, it can still be quite offensive.
Their spectacle works in part as a virtual fence adorned with a sign bearing the
following message: “keep (the hell) out of here, this is our Homeland.”

This geeky commentary on the masses is not entirely new. Take, for
instance, “September That Never Ended,” an entry from an online glossary of
hacker terms, the Jargon File:

All time since September 1993. One of the seasonal rhythms of the Usenet
used to be the annual September influx of clueless newbies who, lacking any
sense of netiquette, made a general nuisance of themselves. This coincided
with people starting college, getting their first internet accounts, and plun-
ging in without bothering to learn what was acceptable. These relatively small
drafts of newbies could be assimilated within a few months. But in Septem-
ber 1993, AOL users became able to post to Usenet, nearly overwhelming the
old-timers’ capacity to acculturate them; to those who nostalgically recall the
period before, this triggered an inexorable decline in the quality of discus-
sions on newsgroups. Syn. eternal September. See also AOL. 45

Already by 1993 geeks and hackers who considered the Internet as their partic-
ular romping grounds were remarking on the arrival of newcomers. This tradition
of lamenting the “lame” behavior of “noobs” continues today; however, the tac-
tics have changed among a class of technologists. Instead of reasoned debate, as is
common with university and F/OSS hackers, among trolls, the preferred tactic of
performing their “eliteness” is shocking spectacle and the creation of highly spe-
cialized and esoteric jargon: argot. As noted folklorist David Maurer has argued,
argot functions primarily in three capacities: to encode technical expertise, to cre-
ate boundaries between insiders and outsiders, and to maintain secrecy. 46

The behavior of trolls, of course, cannot be explained only by their con-
tempt of newcomers; as this essay has argued, there are multiple sources and
a rich historical tradition at play, including the aesthetic legacy of phreakers
and the underground, who provided a rich, albeit less shocking, tradition of spectacle and brashness from which to draw on, extend, and reformulate. We must also give due weight to the condition of collective anonymity, which, as the psychosocial literature has so long noted, fans the fire of flaming and rude behavior. Finally, with a number of important exceptions, their antics, while perhaps morally deplorable, are not illegal. The hacker crackdown of the 1980 and 1990s may have subdued illegal hacks, but it certainly did not eliminate the rude-boy behavior that often went along with them; in fact, it might have created a space that allowed trolling to explode as it has in the past few years.

How have underground hackers reacted to this class of technologists? Although there is no uniform assessment, the UNIX Terrorist, who opened this piece, ends his rant by analyzing “epic lulz.” Engaging in the “lulz,” he notes, provides “a viable alternative” both to the hacker underground and to open-source software development:

Every day, more and more youngsters are born who are many times more likely to contribute articles to socially useful publications such as Encyclopedia Dramatica instead of 2600. Spreading terror and wreaking havoc for “epic lulz” have been established as viable alternatives to contributing to open source software projects. If you’re a kid reading this zine for the first time because you’re interested in becoming a hacker, fucking forget it. You’re better off starting a collection of poached adult website passwords, or hanging out on 4chan. At least trash like this has some modicum of entertainment value, whereas the hacking/security scene had become some kind of fetid sinkhole for all the worst kinds of recycled academic masturbation imaginable. In summary, the end is fucking nigh, and don’t tell me I didn’t warn you... even though there’s nothing you can do about it.

Good night and good luck,
the unix terrorist

One obvious question remains: do trolls even deserve any place in the historical halls of hacking? I cannot answer this question here, for it is at once too early to make the judgment and not entirely my place to do the judging. One thing is clear: even if trolls are to be distinguished from underground hackers, they do not reside entirely in different social universes; trolling was common on BBSes, Usenet, and other Internet arenas where underground hacking thrived. There is a small class of the most elite griefers and trolls who use hacking as a weapon for their merciless mockery. Most telling may be the...
UNIX Terrorist himself, and especially his rant; as the UNIX Terrorist’s final words so clearly broadcast: underground hacking is notoriously irreverent and brash and thus helped to light an aesthetic torch that trolls not only have carried to the present but have also doused with gasoline.

Conclusion: Informational Tricksters or Just “Scum of the Earth Douchebags”?

Even while some of the actions of phreakers, hackers, and trolls may be ethically questionable and profoundly disquieting, there are important lessons to be drawn from their spectacular antics.53 As political theorist and activist Stephen Duncombe has so insightfully argued, if carried out responsibly, a politics of spectacle can prove to be an invaluable and robust political tactic: “spectacle must be staged in order to dramatize the unseen and expose associations elusive to the eye.”54 The question that remains, of course, is whether there is any ethical substance to these spectacular antics, especially those of the troll, whose spectacle is often generated through merciless mocking, irreverent pranking, and at times, harassment.

If we dare consider these informational prankers in light of the trickster, then perhaps there may be some ethical substance to some, although certainly not all, of their actions. The trickster encompasses a wide range of wildly entertaining and really audacious mythical characters and legends from all over the world, from the Norse god Loki to the North American coyote. Not all tricksters are sanitized and safe, as Disney has led us to believe. Although clever, some are irreverent and grotesque. They engage in acts of cunning, deceitfulness, lying, cheating, killing and destruction, hell raising, and as their name suggests, trickery. Sometimes they do this to quell their insatiable appetite, to prove a point, at times just to cause hell, and in other instances to do good in the world. Tricksters are much like trolls: provocateurs and saboteurs. And according to Lewis Hyde, tricksters help to renew the world, in fact, to renew culture, insofar as their mythological force has worked to “disturb the established categories of truth and property and, by so doing, open the road to possible new worlds.”55

The mythical notion of the trickster does seem to embody many of the attributes of the phreaker, hacker, and especially the contemporary Internet troll. But is it reasonable to equate the mythical trickster figure Loki and the tricksters in Shakespeare with figures that do not reside in myth (although Internet trolls certainly create myths), do not reside in fiction, but reside in the reality of the Internet? Given that trolls, in certain instances, have
caused mayhem in people’s lives, does the moniker “trollster” act as an alibi, a defense, or an apology for juvenile, racist, or misogynist behavior? Or is there a positive role for the troll to play on the Internet as site/place of constant play and performance? Is the troll playing the role of the trollster, or is the troll playing, you know, just for the lulz?

NOTES

I would like to thank Patrick Davison, Micah Anderson, Ashley Dawson, Finn Brunton, and especially Michael Mandiberg, who all provided such generous feedback and comments. This work is licensed under the Creative Commons Attribution-ShareAlike license.

6. It is far more common for hackers who do not engage in transgression to accuse transgressive hackers like the UNIX Terrorist of not being authentic hackers, instead being “crackers.” See the entry for “cracker” in the tome of hacker lore, the Jargon File: http://catb.org/jargon/html/C/cracker.html.
9. Ibid., 398.
11. Phil Lapsely is currently writing a comprehensive history of phone phreaking and has given various lectures on the topic. See http://www.historyofphonephreaking.org/.


16. Rosenbaum, "Secrets of the Little Blue Box."


19. Ibid.

20. Rosenbaum, "Secrets of the Little Blue Box."


24. Thomas, Hacker Culture.

25. Ibid., 92.

26. Ibid., 132.

27. Thomas, Hacker Culture; Sterling, The Hacker Crackdown. Among underground hackers, media representation and commodification were and still are largely ineffective tools to placate them. However, lucrative information-technology jobs, especially within the security industry, as Andrew Ross has noted, has led "two generations of hackers" to agonize "over accepting lucrative offers of employment within corporate or government IP security." Andrew Ross, Nice Work If You Can Get It (New York: NYU Press, 2009), 124.


29. Kevin Mitnick's case and others are covered in Thomas, Hacker Culture.


38. This is difficult to empirically verify, yet it is not unreasonable to surmise that the well-publicized hacker arrests of the 1990s, combined with even stiffer penalties for computer intrusion mandated in the Patriot Act, would work to curb the most flagrant or potentially illegal behaviors or, alternatively, possibly make the underground burrow back into the recesses of its crevasses, away from the watchful eye of law enforcement.

34. Contemporary trolls encompass a wide range of subgroups, each with particular histories and techniques and some also harboring great distaste for other trolling groups.


37. See http://www.whyweprotest.net/.


43. Sterling, The Hacker Crackdown.


50. "Phrack Prophile on the UNIX Terrorist."


Although I am not answering this question here, I am certainly not posing it rhetorically. It is crucial to interrogate trolling in all its dimensions, roots, and consequences, which I am unable to do here, as the main purpose of this essay is to establish aesthetic linkages between phreakers, hackers, and trolls. Lisa Nakamura has written about online racism extensively. See Lisa Nakamura, *Digitizing Race: Visual Cultures of the Internet* (Minneapolis: University of Minnesota Press, 2008) and *Cybertypes: Race, Ethnicity, and Identity on the Internet* (New York: Routledge, 2002). Recently, she has explored the intersection between racism and griefing in a talk: “Don’t Hate the Player, Hate the Game,” June 16, 2010, available online at http://blogs.law.harvard.edu/mediaberkman/2010/06/16/lisa-nakamura-dont-hate-the-player-hate-the-game. Legal scholar Danielle Citron has examined cyberharassment of women in terms of discrimination, building on her previous work on legal barriers and opportunities for addressing online abuse. See Danielle Citron, “Law’s Expressive Value in Combating Cyber Gender Harassment,” *Michigan Law Review* 108 (2009): 373–416; and Danielle Citron, “Cyber Civil Rights,” *Boston University Law Review* 89 (2009): 61–125. Not all cases of trolling are relevant to the issues raised by these scholars, but some of them certainly are pertinent.
The Language of Internet Memes

PATRICK DAVISON

In *The Future of the Internet—and How to Stop It*, Jonathan Zittrain describes the features of a generative network. A generative network encourages and enables creative production and, as a system, possesses leverage, adaptability, ease of mastery, accessibility, and transferability. Notably absent from this list of characteristics, however, is security. Many of the characteristics that make a system generative are precisely the same ones that leave it vulnerable to exploitation. This zero-sum game between creativity and security implies a divided Internet. Those platforms and communities which value security over creativity can be thought of as the “restricted web,” while those that remain generative in the face of other concerns are the “unrestricted web.”

The restricted web has its poster children. Facebook and other social networking sites are growing at incredible speeds. Google and its ever-expanding corral of applications are slowly assimilating solutions to all our computing needs. Amazon and similar search-based commerce sites are creating previously unimagined economies. Metaphorically, these sites, and countless others, make up the cities and public works of the restricted web. However, the unrestricted web remains the wilderness all around them, and it is this wilderness that is the native habitat of Internet memes.

The purpose of this essay is twofold. The first is to contribute to a framework for discussing so-called Internet memes. Internet memes are popular and recognizable but lack a rigorous descriptive vocabulary. I provide a few terms to aid in their discussion. The second purpose is to consider Foucault’s “author function” relative to Internet memes, many of which are created and spread anonymously.

*What Is an Internet Meme?*

In 1979 Richard Dawkins published *The Selfish Gene*, in which he discredits the idea that living beings are genetically compelled to behave in ways that are “good for the species.” Dawkins accomplishes this by making one point
clear: the basic units of genetics are not species, families, or even individuals but rather single genes—unique strands of DNA.³

At the end of the book, Dawkins discusses two areas where evolutionary theory might be heading next. It is here that he coins the term “meme.” He acknowledges that much of human behavior comes not from genes but from culture. He proposes that any nongenetic behavior be labeled as a meme and then poses a question: can the application of genetic logic to memes be productive? To make the differences between genes and memes clear, I offer a short example of each.

Genes determine an organism’s physical characteristics. A certain gene causes an organism to have short legs, or long, for instance. Imagine two zebra. The first has the short-leg gene, and the second the long. A lion attacks them. The short-legged zebra runs more slowly and is eaten. The long-legged zebra runs more quickly (because of its legs) and lives. At this point, there are more long-leg genes in the imaginary ecosystem than short-leg genes. If the long-legged zebra breeds and has offspring, those offspring with long legs will continue to survive at a higher rate, and more offspring of those offspring will contain the long-leg gene. The genes themselves are not thinking beings—the long-leg gene does not know it causes long-leggedness, nor does it care, but given that it bestows a property that interacts with the environment to allow more of itself to be produced, it is successful.⁴

Memes determine the behavior of an organism. They are either taught to an organism (you go to school and learn math) or learned through experience (you stick a finger in an outlet, get shocked, understand that outlets should be avoided). Imagine two soccer players. There are genetic factors which might make them better or worse at playing (long or short legs, for instance); however, their ability is also dependent on their understanding of the game. For this example, let us imagine that the two players are physically identical. However, one of them goes to practice, and the other does not. At practice, the coach teaches the attendant player about passing; you pass the ball to other players and increase the chance that your team will score. During a game, the attendant player is likely to pass and to experience success because of it. The truant player, having not learned the passing meme, will not pass, and that player’s team will suffer because of it.

While genes rely on the physical process of reproduction to replicate, memes rely on the mental processes of observation and learning. In our example, the truant player comes to the game without the passing meme and suffers. That player is, however, able to observe the attendant player passing, and succeeding, and can decide to imitate the attendant player by passing as
well. The passing meme successfully replicates itself in a new organism without the all-or-nothing cycle of life and death. This highlights one of the critical differences between genes and memes: speed of transmission. Compared to genetic changes (which span generations upon generations), memetic changes happen in the blink of an eye. Offline memes, cultural cornerstones like language or religion, are hyperfast when compared to their genetic counterparts. Internet memes are even faster.

The other notable difference between genes and memes is their relative fidelity of form. In our zebra example, a zebra is granted physical characteristics based on a discrete combination of DNA. All the genes that Dawkins discusses are at their most basic made up of sequences of only four chemicals. The memes that I examine in this essay, however, are not made up of chemicals but of ideas and concepts. Our truant player may observe and learn the passing meme, but that process does not transfer an identical chemical "code" for passing. The meme is subject to interpretation and therefore to variation.

In Dawkins's original framing, memes described any cultural idea or behavior. Fashion, language, religion, sports—all of these are memes. Today, though, the term "meme"—or specifically "Internet meme"—has a new, colloquial meaning. While memes themselves have been the subject of entire books, modern Internet memes lack even an accurate definition. There are numerous online sources (Wikipedia, Urban Dictionary, Know Your Meme, Encyclopedia Dramatica) that describe Internet memes as the public perceives them, but none does so in an academically rigorous way. Given this, I have found the following new definition to be useful in the consideration of Internet memes specifically:

*An Internet meme is a piece of culture, typically a joke, which gains influence through online transmission.*

While not all Internet memes are jokes, comparing them to offline jokes makes it clear what makes Internet memes unique: the speed of their transmission and the fidelity of their form. A spoken joke, for instance, can only be transmitted as quickly as those individuals who know it can move from place to place, and its form must be preserved by memory. A printed joke, in contrast, can be transmitted by moving paper and can be preserved by a physical arrangement of ink. The speed of transmission is no longer limited by the movement of individuals, and the form of the joke is preserved by a medium, not memory.
Now, consider a joke that exists on the Internet. The speed of transmission is increased yet again, in an incredible way. Space is overcome: computers connect to one another through far-reaching networks. Time is overcome: the digitally represented information is available as long as the server hosting it remains online. A joke stored on a website can be viewed by as many people as want to view it, as many times as they want to, as quickly as they can request it.

An online joke's fidelity of form, however, is subject to a unique contradiction. Being digital, the joke is perfectly replicable. Copy and paste functions (or their equivalents) are ubiquitous, expected parts of software platforms. However, a piece of digital media in the modern landscape of robust and varied manipulation software renders it also perfectly malleable. Individual sections of a piece of digital media can be lifted, manipulated, and reapplied with little effort.

Once I say that a piece of media, or a meme, is replicable and malleable, I must specify what exactly is being copied or changed. A meme can be separated into components. I propose three: the manifestation, the behavior, and the ideal.

The manifestation of a meme is its observable, external phenomena. It is the set of objects created by the meme, the records of its existence. It indicates any arrangement of physical particles in time and space that are the direct result of the reality of the meme.

The behavior of a meme is the action taken by an individual in service of the meme. The behavior of the meme creates the manifestation. For instance, if the behavior is photographing a cat and manipulating that photograph with software, the manifestation this creates is the ordered progression of pixels subsequently uploaded to the Internet.

The ideal of a meme is the concept or idea conveyed. The ideal dictates the behavior, which in turn creates the manifestation. If the manifestation is a funny image of a cat and the behavior is using software to make it, then the ideal is something like “cats are funny.”

When tracking the spread of a particular meme, it is useful to identify which of these three aspects is being replicated and which adapted. Dawkins prefigures this in his original chapter by theorizing that the principal tool for meme identification would be the perception of replication. This is important, because identifying the replication of memes is subjective. Sometimes this identification is easy: one person acts, and another person copies that person exactly. Other times the process of replication is less exact. This is why separating the manifestation, behavior, and ideal is useful. As long as one of the three components is passed on, the meme is replicating, even if mutating and adapting.

The Language of Internet Memes
Early Internet Memes

In 1982 Scott E. Fahlman proposed a solution to a problem he and other users were experiencing when communicating via the Internet. Members who participated on the bulletin-board system at Carnegie Mellon would on occasion descend into “flame wars”—long threads of communication that are hostile or openly aggressive to other users. Fahlman believed that many of these disagreements arose out of misinterpreted humor. His solution to this problem was to add a specific marker to the end of any message that was a joke.8 That marker was :-) I am going to assume that anyone reading this has seen this “emoticon” and understands that if rotated ninety degrees clockwise, the colon, hyphen, and close-parenthesis resemble a smiling face, a symbol lifted from pre-Internet time. This practice of contextualizing one’s written messages with an emoticon to indicate emotional intent has become widespread. Today there are countless other pseudopictograms of expressions and objects which are regularly added to typed communication. Emoticons are a meme.

To leverage my framework, the manifestation of an emoticon is whatever combination of typed characters is employed as pseudopictogram. These can be in any medium—handwritten or printed on paper, displayed on a screen, any form capable of representing glyphs. The behavior is the act of constructing such an emoticon to contribute emotional meaning to a text. The ideal is that small combinations of recognizable glyphs represent the intent or emotional state of the person transmitting them.

If we analyze the emoticon meme from a genetic point of view which values survival and defines success through continued replication, it proves itself remarkably well situated. Emoticons can be very quickly used. Emoticons are easy to experiment with. The tools for making emoticons are included on every device we use to type. The primary glyphs used for many of the emoticons are glyphs used less often than the upper- and lower-case alphabets. Emoticons reference a previously existing source of meaning (human facial expressions) and therefore can be easily interpreted upon first encounter. More than just re-creating face-to-face meaning in textual communication, emoticons also add the possibility of a new level of meaning—a level impossible without them.

If all these factors were not true, perhaps emoticons would see less use. If keyboards full of punctuation were not already spread across the landscape, or if human facial expressions were not a cultural constant, maybe emoticons would disappear or be relegated to obscurity. As it stands, though, emoti-
Emoticons come from the Internet's childhood, when bulletin boards and e-mails accounted for a bulk of the activity online. Another early meme came from its adolescence—1998, after the widespread adoption of the World Wide Web and during the heyday of GeoCities. Deidre LaCarte, who was a Canadian art student at the time, made a GeoCities-hosted website as part of a contest with a friend to see who could generate the most online traffic. The website she created, popularly known as “Hamster Dance,” consisted of row upon row of animated gifs, each one depicting a hamster dancing, all set to a distorted nine-second audio loop. As of January 1999 the site had amassed eight hundred views, total. Once 1999 began, however, without warning or clear cause, the site began to log as many as fifteen thousand views a day. The comparison of these two early memes, Hamster Dance and emoticons, provides an opportunity to expand and clarify some of the vocabulary I use to discuss memes and to make two important distinctions.

Emoticons are a meme that serve a number of functions in the transmission of information. They can be used to frame content as positive or negative, serious or joking, or any number of other things. Hamster Dance essentially serves a single function: to entertain. This difference in function influences the primary modes of access for each of these memes. For the emoticon meme the behavior is to construct any number of emotional glyphs in any number of settings, while for the Hamster Dance meme the behavior is only a single thing: have people (themselves or others) view the Hamster Dance web page. The Hamster Dance page is a singular thing, a spectacle. It gains influence through its surprising centralization. It is a piece of content that seems unsuited given more traditional models of assessment of organizing people around a central location, but yet, that is precisely the function it serves.

Emoticons gain influence in exactly the opposite way. There was an original, single emoticon typed in 1982, but other emoticons do not drive people toward that single iteration. The emoticon has gained influence not by being surprisingly centralized but by being surprisingly distributed. Hamster Dance is big like Mt. Rushmore. Emoticons are big like McDonald’s. This first distinction, then, is that the influence gained by memes can be both centralized and distributed.

The second distinction is closely related to the first. Just as Hamster Dance is characterized by many-in-one-location, and emoticons are characterized by individuals-in-many-locations, the two also differ in the nature of
the behavior they replicate. Many more people have used an emoticon, or concocted their own, than have seen the very first emoticon from 1982. In contrast, many more people have seen the original Hamster Dance site than have created their own Hamster Dance site. It is tempting, then, to say that this difference implies two categories of memetic behavior: use and view. It is more useful, though, to treat both of these behaviors as characteristics present in varying degrees for any given meme. These two behaviors connect directly to the previously mentioned states of replicable and malleable. A piece of media’s being replicable makes it easier for that media to gain influence through views. A piece of media’s being malleable makes it easier for that media to gain influence through use. Engagement with a meme, then, takes the form of either use or viewing or, more in keeping with the terms of malleable and replicable, of transformation or transmission.

These distinctions help to account for the variety of phenomena popularly identified as Internet memes. Working from Dawkins’s initial conception, the term “meme” can mean almost anything. By limiting the scope of what is meant by “Internet meme,” the goal is not to create a basis for invalidating
the widespread use of the term but, rather, to provide an inclusive method for accounting for and relating the various phenomena labeled as such.

Current Internet Memes

All memes (offline and on) are capable of existing in layers. For instance, consider language. The meme of language is communication through speech. There are, however, multiple languages. Each individual language is a meme nested within the larger language meme. Additionally, within each individual language there are even more submemes: dialects, slang, jargon.

Internet memes follow the same structure. One very common, rather large meme is the image macro. An image macro is a set of stylistic rules for adding text to images. Some image macros involve adding the same text to various images, and others involve adding different text to a common image. Just like emoticons, which exist in an environment well suited to supporting their survival, image macros are able to thrive online because the software necessary for their creation and distribution is readily available.

There are countless submemes within the image macro meme, such as LOLcats, FAIL, demotivators. I am going to focus on just one: Advice Dog. The trope of this meme is that Advice Dog, a friendly looking dog at the center of a rainbow-colored background, is offering the viewer whatever advice is contained in the text above and below his head. The formula is simple:

1. Image of dog in center of rainbow
2. First line of advice
3. Second line of advice (usually a punch line)

Iterations of the Advice Dog meme vary not only in the specific text they use to communicate humor but also in the type of humor communicated. When Advice Dog gives someone advice, genuine good advice, it can be humorous simply by virtue of being attached to a bright background and smiling dog. Once it is established that the explicit function of Advice Dog is to give advice, though, having him give bad or unexpected advice is ironic. The text can also be transgressive, giving advice that is intentionally offensive or absurd, accompanied by text that is not advice at all.

In addition to having Advice Dog offer various kinds of advice, one can also have other figures deliver other kinds of messages. These are Advice Dog–like variants. Whether a “genuine” Advice Dog iteration or a simply an Advice Dog–like variant, all of these are contained within the larger Advice

The Language of Internet Memes
Fig. 9.2. Advice Dog meme

GET A JOB ALREADY

YOU'RE 28 GODDAMN

GET DRUNK

DRIVE CAREFULLY
Figs. 9.3–9.5. More Advice Dog memes
Dog meme. The manifestations are the individual images, among which numerous replicated elements are obvious. The style of the background, the square format of the image, the central placement of a cropped figure—all of these remain constant (with consistent variation) from image to image. The behavior of the meme is a varied set of practices. Viewing and linking to various Advice Dog manifestations is part of the meme, as is saving and reposting the same. Creating original iterations with new text is part of the meme, as is creating or contributing to any of the Advice Dog–like variants in the same manner.

The ideal of the Advice Dog meme is harder to describe. The meaning conveyed by any single Advice Dog macro can vary wildly. Some have ironic meanings, while others have aggressive or offensive meanings. The subject can be a dog that gives advice or a child that celebrates success. So we can say that for Advice Dog, the ideal of the meme is not always replicated from instance to instance. With no qualities recognizable from iteration to iteration, it would seem there is no justification for linking them together as part of the same meme. However, what is replicated from instance to instance is the set of formal characteristics. We are able to identify each instance as part of the larger Advice Dog meme because of the similarities in form and regardless of the differences in meaning.

Attribution

The identification of memes relies on the identification of replications. One of the most common replicated elements that sets memes of the unrestricted web apart from memes of the restricted web is attribution. Attribution is the identification of an author for a piece of media. Attribution is central to much of the restricted web: YouTube is host to numerous copyright battles, fueled by rights holders’ desire to derive worth from media attributed to them. Wikipedia encourages submissions from anyone but meticulously tracks participation and only allows images to be uploaded by their license holder. Creative Commons offers numerous alternative licenses for content creators, but attribution is common to every one. 13

It is clear that many of the popular platforms of the Internet preserve and extend a historical prioritizing of attribution and authorship. Foucault, in his essay “What Is an Author?” writes that the author’s name “performs a certain role with regard to narrative discourse, assuring a classificatory function. Such a name permits one to group together a certain number of texts, define them, differentiate them from and contrast them to others. In addi-
Figs. 9.6–9.11. Advice Dog variants: Courage Wolf, Politically-Neutral Dog, Depression Dog, Bachelor Frog, Rich Raven, Success Kid
tion, it establishes a relationship between the texts."¹⁴ Foucault’s concept of the “author function” is therefore similar in function to modern metadata. The author’s name serves to classify and group together separate works, much in the same way tags and keywords allow distributed digital media to be searched and sorted. The Internet is a system filled with an incalculable amount of data. The question of where to find a piece of media has become just as relevant as the question of how to produce a piece of media. Attribution supports this model and fits within the modern practice of prioritizing metadata. Metadata is a meme. It is a meme that existed well before the Internet but that has, like other memes introduced to the Internet, achieved an accelerated rate of growth and change.

Then why do certain memes eschew attribution? The memes of the unrestricted web (Advice Dog is only one example) not only often disregard attribution and metadata; they are also frequently incorporated into systems and among practices that actively prevent and dismantle attribution.¹⁵ Some people might argue that many Internet memes lack attribution because their creators have no stake in claiming ownership over worthless material. However, if the practice of attribution is a meme, then the practice of omitting attribution is also a meme, and insofar as it exists and replicates within certain populations, we must say that it is successful. The nonattribution meme possesses characteristics that make it likely to be replicated in others.

What, then, does the practice of anonymity offer to the individuals who enact it? In many ways, anonymity enables a type of freedom. This freedom can have obvious personal benefits if the material one is generating, sharing, or collecting is transgressive. For those Internet users who revel in the existence of racist, sexist, or otherwise offensive memes, a practice and system of anonymity protects them from the regulation or punishment that peers or authorities might attempt to enact in response to such material. However, there is an additional layer of freedom afforded by a lack of attribution. With no documented authors, there exists no intellectual property. Memes can be born, replicated, transmitted, transformed, and forwarded with no concern for rights management, monetization, citation, or licensing. This takes us full circle back to Zittrain’s generative network and to the unrestricted web it implies. The prioritization of creative freedom over security is epitomized by the nonattribution meme.

The question I am left with, that I am as of yet unequipped to answer, is whether this thought process casts the nonattribution meme in the role of a metameme. If the presence of the nonattribution meme in a network makes that network more likely to be generative, and if being generative makes a
network a more fertile environment for the production and evolution of memes, then is nonattribution a meme that makes the creation of other memes more likely? Lastly, how important is the effect of this metameme when we consider a network (the Internet) whose platforms can require either attribution or anonymity?

NOTES

This work is licensed under the Creative Commons Attribution-ShareAlike license.


4. The use of the word “successful” here is nontrivial. Dawkins explains that replication is a fundamental process for genetics. The earliest forms of life achieve their status as such by virtue of their ability to create copies of themselves. The process of evolution relies entirely on the particulars of the process of reproduction. The theoretical method of meme identification that Dawkins proposes is one that relies on identifying replications. Given all of this, success is always measured by volume of replication. Insofar as an entity (gene, meme, or otherwise) makes more of itself, it is successful.

5. These are the same two characteristics that differ so greatly between genes and memes. If memes transmit faster and are more adaptable than genes, then Internet memes are the most extreme example of that tendency: they are transmitted the fastest and are the most adaptable.


7. I use “ideal” here specifically to reference a platonic ideal. The historical understanding of a platonic ideal is ultimately centralized. A single, theoretical ideal dictates characteristics down to individual manifestations. The ideals of memes operate in reverse. The ideal of a meme is the aggregate of all manifestations of that meme. This is a bottom-up rather than top-down organization.


9. The “Gchat” functionality inside of Google’s Gmail, for instance, not only automatically animates any of a number of popular emoticons; it also allows users to select from various styles of animation and provides buttons for inserting emoticons without typing.

10. Geocities was an early website-hosting service from 1994 which allowed people with no programming knowledge to create their own websites for free. It was later acquired by Yahoo! in 1999 and then closed in 2009 (http://geocities.yahoo.com).


12. When considering the form of any given meme, one must consider how easily the form is copied and how easily the form is changed. As I have said, Internet memes are cultural units that are the most replicable and malleable.

*The Language of Internet Memes*
13. Since the initial writing of this essay, Creative Commons has introduced a CC0 license, which does not require attribution.


15. 4chan.org is a website which has become the most popular example of a site that eschews attribution. It allows contributions from users with no registration process, which has led to a user base operating largely in anonymity.