Righteous Devils:
Unpacking the ethics of hacktivism

Ethan Hanner
Department of Computer Science
University of Colorado Boulder
ethan.hanner@colorado.edu

Jed R. Brubaker
Department of Information Science
University of Colorado Boulder
jed.brubaker@colorado.edu

Hackers and Hacktivists: Modern Folk Devils

The term "hacktivism" was first used in 1994 by a member of the technology collective Cult of the Dead Cow (cDc) to refer to the use of technology for direct action intended to bring about social change. Since then, however, this term has been seized by popular media coverage to associate hacktivist campaigns with behavior that is malicious, destructive, or undermines the security of the Internet. This characterization is partly supported by popular portrayals of hackers in general as "modern folk devil[s]" [8]. According to Sauter, "…popular media stokes common fears that armies of basement-dwelling adolescent males are eager to dish out vindictive mayhem to a society so tied to technology (and yet so clueless as to its inner workings) that it would be unable to adequately defend itself" [8].

The reality is far different. Individuals who leverage technology (and specifically the Internet) for purposes of advocacy and activism span all demographics and geography [9]. Although there is some truth to the idea that hacktivists are members of a disenfranchised population seeking only to create mayhem, there are just as many out there who have far greater goals than just "doing it for the lulz" [3,7].

Unfortunately, the framing of much of the coverage around hacktivist activities contributes to the perception of these individuals and groups as "bad actors." In particular, early activities of the hacktivist/trolling collective known as Anonymous centered around disruptive actions such as the Habbo Hotel raids [10], swatting (a type of harassment that involves deceiving emergency response dispatchers into sending police and other emergency personnel to a target's address), and doxxing (publishing personal information about an individual or group on public forums, often with malicious intent). Rather than renouncing this characterization, members of Anonymous at the time reveled in their newfound fame and embraced labels like the "Internet Hate Machine," a moniker coined during a news segment aired by a FOX affiliate in July 2007 [6 as cited in 3].

When we look beyond media coverage, however, many of the issues around which hacktivists engage also motivate activism more broadly [8]. How, then, are we to understand hacktivists' style of techno-civil disobedience? To answer this question, we are researching the ways that members of the public view the individuals and activities associated with hacktivism and online activism. We seek to understand how people understand and differentiate these two terms, how they make judgments on the appropriateness and effectiveness of the tactics used, and their feelings on the use of technology for protest generally. We are motivated by an ever-growing need to reconcile the affordances and limitations of online platforms and social media with the rights of free speech, dissent, and political organizing and how they align with community values and norms.

Ethical Perceptions of Hacktivism

Our research on hacktivism has focused on understanding how the public perceives these types of activities and what their views are on the legality, morality, and possible repercussions for those involved. Starting in Fall 2016, we conducted an online survey to explore attitudes and beliefs in this area. Based on a survey of the literature on past hacktivist campaigns [1,3,4,8], our survey investigated attitudes about four specific methods of hacktivism:

1. client-side distributed denial of service (DDoS) action involving voluntary participation,
2. server-side DDoS action involving botnets or "zombie" computers,
3. website defacement, and
4. information theft and leaking.

Our results revealed points of tension when people evaluate the appropriateness of hacktivism, including: conflicts between the free speech rights of protestors and of the targets (e.g., with DDoS actions and website defacements); concerns over privacy and anonymity both of activists and targets; potential harms and how to define damage in a digital space; and concerns about power imbalances and Internet vigilantism.

The results from our survey were used to inform the design of an interview study. We conducted a total of 12 interviews and are currently performing a thematic analysis of the data to understand the factors that influence the public's perception of the groups and activities associated with hacktivism, especially with regards to how judgments are made about the justification, effectiveness, and appropriateness of hacktivist tactics and goals. In addition to hacktivism,

these interviews explored related topics such as the use of social media for online activism and advocacy, attitudes about offline protests, and how they compare to digital protest.

We are already seeing distinctions between how people discuss hacktivism versus online activism. For example, participants associate hacktivism with decidedly negative connotations, such as "devious", "malicious", "stolen data", and "unsanctioned use of data." In contrast, online activism has more positive associations, with participants mentioning the value of social media for advocacy and activism. While hacktivism is often seen as disruptive, online activism is seen as a powerful way of spreading information and awareness that historically was not possible.

Even though evaluations of hacktivism and online activism differ, when they are appropriate and what counts as each is far more nuanced. For example, one participant mentioned how a nominally Anonymous-affiliated Twitter account spoke out against ISIS after the Pulse nightclub shooting in Orlando by spamming their accounts with gay pornography. This type of activity echoes the type of trolling, trickster behavior that characterized 4chan and Anonymous in the early 2000's – behavior that valued "the lulz" over any political motivation or goals. This form of "protest", however, walks a very fine line — in terms of how it is evaluated by both people and platforms.

Our participant recognized the disruptive nature of Twitter spam, but like many of our participants, ideological agreement with the activist's intent left them supportive of what might otherwise be questionable behavior. Meanwhile, Twitter's content guidelines largely forbid gratuitous imagery including sexually explicit and violent content, discourages abusive behavior like harassment, and explicitly disallows spamming (defined in part as "bulk or aggressive activity that attempts to manipulate or disrupt Twitter or the experience of users on Twitter"). One could easily make an argument, from the point of view of ISIS and/or their sympathizers on Twitter, that this protest response to the Orlando shooting violates one or more of those guidelines. However, in doing so, one might suggest that Twitter's policies should not be aligned with the values of the community.

The tension between a platform and those who populate it may be indicative of the tensions surrounding activism more broadly. For many participants, the collective action represented by hacktivism was seen as society's last resort for keeping large entities like governments and multi-national corporations accountable to the public.

Addressing Hacktivism and Online Activism Through Design and Policy

Although laws such as the Computer Fraud and Abuse Act have been used in the past to charge individuals involved in DDoS actions or unauthorized access to protected systems, these laws do not explicitly address how those activities might overlap with acts of protest and civil disobedience. The ability to organize and protest is generally seen as a fundamental right in a civilized society, and historical acts of civil disobedience are often held up as necessary and heroic sacrifices, even when the actor receives harsh punishment. However, there is no clear consensus on what constitutes civil disobedience in the electronic realm and what should be the benchmarks or criteria for

weighting the rights of activists with the need for security and privacy of the Internet and its denizens (c.f., [2,5,8,9] for discussions on electronic civil disobedience).

Thus, before we can make suggestions regarding the design, policy, and guidelines for online platforms to address the complicated issues surrounding the transfer of offline activism, protest, and dissent to digital spaces, we must understand the values and motivation of both the activists and the rest of the community. Ultimately, it is our argument that understanding the nuances behind these values is critical, especially when the ways that major Internet companies choose to accommodate or discourage expressions of dissent on their platforms will have far-reaching implications for political and social activism both online and off.

References

1. Caroline Auty. 2004. Political hacktivism: tool of the underdog or scourge of cyberspace? In *Aslib Proceedings*, 212–221. https://doi.org/10.1108/00012530410549240
2. Andrew Calabrese. 2004. Virtual nonviolence? Civil disobedience and political violence in the information age. *Info* 6, 5: 326–338. https://doi.org/10.1108/14636690410564834
3. Gabriella Coleman. 2014. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. Verso, New York and London.
4. The Electrohippies Collective. 2000. Client-side Distributed Denial-of-Service: Valid campaign tactic or terrorist act? Retrieved from http://www.iwar.org.uk/hackers/resources/electro-hippies-collective/op1.pdf
5. Brian J. Huschle. 2002. Cyber Disobedience: When is Hacktivism Civil Disobedience? *International Journal of Applied Philosophy* 16, 1: 69–83. https://doi.org/10.5840/ijap20021613
6. NegativeNigra. 2007. Anonymous on FOX11. Retrieved February 4, 2018 from https://youtu.be/DNO6G4ApJQY
7. Parmy Olson. 2013. *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency*. Back Bay Books, New York, NY.
8. Molly Sauter. 2014. *The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet*. Bloomsbury Academic, New York, NY, NY.
9. Zeynep Tufekci. 2017. *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. Yale University Press, New Haven & London.
10. Pool's Closed. *Literally Media Ltd.* Retrieved February 4, 2018 from http://knowyourmeme.com/memes/pools-closed