INTERNET ACTIVISM OR CYBERTERRORISM?

THE ETHICS OF HACKTIVISM

As internet usage has expanded across the globe, it has made space for various new practices to thrive, including internet-based activism. From hashtag activism to online petitions, digital technology has allowed new and effective ways for activists to mobilize for change. More recently, another form of activism has also evolved online: hacktivism. Hacktivism has been described as a type of civil disobedience that "unites the talents of the computer hacker with the social consciousness of the political activist" (Manion & Goodrum, 2000). Converting traditional protest techniques like trespassing and blockades for use in the digital sphere, hacktivists "can attack the websites of any individual, corporation, or nation that is deemed responsible for oppressing the ethical, social, or political rights of others" (Manion & Goodrum, 2000). However, some have criticized hacktivism as a form of cyberterrorism. Indeed, as we shall see, the ethics of hacktivism have become a heated topic of debate.

While proponents of hacktivism agree that "the threat posed by cyberterrorism is very real," they nonetheless hold that "it is a mistake to identify cyberterrorism with hacktivism." Referencing U.S. law that defines terrorism as "an act of violence for the purpose of intimidating or coercing a government or civilian population," those who endorse hacktivism argue that it "clearly does not fall into this category, as it is fundamentally non-violent" (Manion & Goodrum, 2000). Furthermore, hacktivists operate under a completely different set of motives than cyberterrorists. Though "hacktivism is not always committed to democratic values," hacktivists typically try to achieve their goals "in a relatively peaceful manner" and do not aim to "cause significant damage, monetary loss, interruption of work of a governmental body or an organization, [or] to frighten authorities or civilians" (Gareeva, Krylova, & Khovrina, 2020). Indeed, some hacktivists have claimed that their actions are not random or reckless, but deliberate and "selective when choosing their targets in order to minimize the harmfulness of their actions and the impact of their protest" (Karagiannopoulos, 2018). In doing so, they identify damage control as "a crucial element in establishing the political usefulness and legitimacy of their actions" and even hope that they can prevent violent outbursts by allowing social tensions to be released through such actions (Karagiannopoulos, 2018).

Critics argue that even if *some* hacktivist actions do not fall under the definition of cyberterrorism, there are nonetheless *other* types of hacktivism that U.S. law recognizes as illegal. For example, sections of the Computer Fraud and Abuse Act (CFAA) prohibit actions such as "accessing and downloading documents from private servers or behind paywalls with the intent of making them publicly available" and distributed denial of service (DDoS) attacks, which "flood a web site's server with traffic from a network of sometimes

thousands of individual computers, making it incapable of serving legitimate traffic" (Thompson, 2013). However, the most concerning problem critics have with hacktivism by far is doxing: the publication of private, identifying information about an individual. In 2011, members of the infamous hacktivist group "Anonymous" (along with a group called "Lulzsec") "breached the Stratfor Global Intelligence Service database and published the passwords, addresses and credit card information of the firm's high-profile clients [claiming that] they planned to use the credit cards to donate $1 million to charity" (Thompson, 2013). Similarly, after members of the inflammatory Westboro Church tweeted their plans to picket outside the funerals of Sandy Hook victims in 2012, Anonymous hacked into the members' Twitter accounts and published their phone numbers, emails, and hotel reservation information (Thompson, 2013). Though some of these actions garnered public support, popularity does not always indicate virtue.

In response to arguments like these, proponents of hacktivism point out that legality is not synonymous with ethics. Of course, the United States' history is riddled with examples of legal, but immoral, practices – such as the enslavement of African Americans and subsequent segregation from public life. In this sense, if civil disobedience is defined as "the peaceful breaking of unjust laws," then hacktivist actions –while sometimes illegal— might count as legitimate activism nonetheless (Manion & Goodrum, 2000). Complicating this line of reasoning, however, critics point out that such a comparison does not align perfectly. When activists of the Civil Rights Movement staged actions like sit-ins, they may have broken Jim Crow laws, but the *law itself* was the target. Yet in the case of hacktivism, a certain person or entity is the target, as computer safety laws themselves are not necessarily unjust. Indeed, if someone hacked your personal accounts for non-political reasons, you would probably want some legal recourse and protections.

Ultimately, the debate about the ethics of hacktivism is far from resolved, and will likely continue to become more complex as the internet continues to evolve further. While hacktivism can be viewed as an effective and popular form of online political activism, it can also be viewed as a dangerous "slippery slope" headed towards cyberterrorism. In debating the ethics of hacktivism, we must pay attention to the new abilities that anonymity and the ability to create motivated groups that the online environment affords individuals, and reason through what principles and values we prioritize in present causes—and what they mean for resolving future conflicts our communities must address.

Discussion Questions:

1. What ethical tensions exist in the practice and evaluation of hacktivism?
2. Do you think hacktivism crosses the line dividing civil disobedience from cyberterrorism? Why or why not?
3. Which actions (if any) of hacktivism do you support? Which go "too far"?
4. What principles should guide hacktivism? Are these principles helpful in preventing well-intentioned but destructive courses of online activism?

Further Information:

Gareeva, A., Krylova, K., & Khovrina, O. (2020) "Hacktivism: A New Form of Political Activism." *Journal of Society and the State* No. 2 (7). Available at: https://sgpjournal.mgimo.ru/2020/2020-7/hacktivism

Karagiannopoulos, V. (2018). "Looking into the Positive and Negative Aspects of Hacktivism." In *Living with Hacktivism. Palgrave Studies in Cybercrime and Cybersecurity*. Palgrave Macmillan, Cham.
Manion, M., & Goodrum, A. (2000). "Terrorism or Civil Disobedience." *ACM SIGCAS Computers and Society*, *30* (2), 14–19. https://doi.org/10.1145/572230.572232

Martin, M., Coleman, G., & Cohen, R. (2013, June 13). "Hacktivists: Heroes or, well, Hacks?" *NPR*. Available at: https://www.npr.org/templates/story/story.php?storyId=191316143

Thompson, C. (2013, January 18). "Hacktivism: Civil Disobedience or Cyber Crime?" *ProPublica*. Available at: https://www.propublica.org/article/hacktivism-civil-disobedience-or-cyber-crime

Authors:

Claire Coburn, Kat Williams, & Scott R. Stroud, Ph.D.
Media Ethics Initiative
Center for Media Engagement
University of Texas at Austin
August 18, 2022

Image: Clint Patterson on Unsplash

This case was supported by funding from the John S. and James L. Knight Foundation. These cases can be used in unmodified PDF form in classroom or educational settings. For use in publications such as textbooks, readers, and other works, please contact the Center for Media Engagement.