Is Doxxing the Right Way to Fight the "Alt-Right?"

daily.jstor.org/is-doxxing-the-right-way-to-fight-the-alt-right/

"I'm not the angry racist they see in that photo," 20-year-old Peter Cvjetanovic told media after the now-infamous picture of him yelling in the wake of the Charlottesville "Unite The Right" March. The march, which escalated into violence, was heavily photographed, and images of participants spread across the web like wildfire. Although photos of the attendees weren't captioned, their identities were swiftly revealed by internet vigilantes.

Doxxing—uncovering and publishing private information, including an individual's identity and contact details, without the target agreeing—is a form of hacktivism. Hacktivism is an umbrella word for digital activism. It "aims to capture attention; it is calculated for maximum media effect, trying to raise the awareness of citizens regarding certain rights and liberties," explains Peter Krapp.

Learning Cvjetanovic's name satisfied a primal urge in many who were angered by the events in Charlottesville. The consequences of the marchers' unmasking—one losing a job, one being disowned by his family—brought a sense of justice.

People with similar names to white supremacists involved in the march were caught in the crossfire.

Yet while groups like Anonymous have made cult heroes out of hacktivism, in the earlier days of the internet, scholars were concerned about its power and its scope. "Hacktivists see cyberspace as a means for nonstate actors to enter arenas of conflict, and to do so across international borders. They believe that nation-states are not the only actors with the authority to engage in war and aggression," Dorothy Denning wrote in the *Harvard International Review* back in 2001.

Denning cautioned against the power this grants individuals. "Unlike nation-states, hacker warriors are not constrained by the 'law of war' or the Charter of the United Nations. They often initiate the use of aggression and needlessly attack civilian systems."

One chilling example of this was the Nuremberg Files. In the 1990s, extreme pro-life activist Neal Horsley created a hit list of abortion providers online, with their addresses and personal information, with the specific purpose of encouraging violence against them. The website went so far as to cross off names of providers who had been killed.

While Denning was focused on larger forms of hacktivism—web sit-ins, site defacement and denial-of-service attacks—her underlying concern still applies. What happens when you give significant power to anyone and everyone? Hacktivists can use their power to draw attention to injustice, yes; or they can create chaos.

"It seems likely that every major conflict in the physical world will have a parallel operation in cyberspace," Denning prophesied. In recent times, major events have led to personal attacks online. Even seemingly trivial disagreements can have massive repercussions.

Since Charlottesville, public blunders have raised questions as to whether the ends justify the means. For example, people with similar names to white supremacists involved in the march were caught in the crossfire.

As with most things in technology, the ethics of hacktivism aren't a new problem, but a new embodiment of an ageless dilemma, one that we should pay close attention to. In 1886 Nietzsche warned, "beware that, when fighting monsters, you do not yourself become a monster."

JSTOR Citations

Activists and Terrorists Turn to Cyberspace

By: Dorothy Denning

Harvard International Review, Vol. 23, No. 2 (SUMMER 2001), pp. 70-75

Harvard International Review

Terror and Play, or What Was Hacktivism?

By: Peter Krapp

Grey Room, No. 21 (Fall, 2005), pp. 70-93

The MIT Press