Online Vigilantism in the Age of OSINT
Josh Lefkow

Thirty years ago, joining your local white nationalist chapter presented something of a logistical challenge. The reticence of many white nationalists to publicly out themselves meant that such groups were not necessarily easy to find, and their membership was restricted to those who actually WERE white—or at least white-passing enough to blend into a clique hyper-obsessed with racial purity. As the internet has removed traditional entry barriers to hate groups, however, they have frequently been investigated and targeted by a host of private citizens who would never have been able to do so in the pre-digital age. The very technologies that have enabled pasty malcontents and would-be jihadists to easily find their ideological ilk online have created a parallel cohort of anti-racist activists who have used their newfound access to these spaces to expose and disrupt them. This internet vigilantism, well-intentioned as it may be, raises a host of ethical questions about the propriety of such actions.

Today, finding white supremacist groups and joining them is a possibility for anyone with access to the internet, no proof of Aryan background necessary (at least in the initial stages of membership). A simple Google search will bring up rudimentary information about dozens of such groups, and anyone brave enough to delve into the murky depths of 8Chan can be quickly exposed to a seemingly infinite variety of toxic ideologies. A growing number of activists have taken advantage of their newfound cyber-anonymity to gain access to and then identify hate group members utilizing open-source intelligence (OSINT), often resulting in real world consequences.

OSINT, essentially “information from published or otherwise publicly available sources,” presents intrepid researchers with a veritable goldmine of resources. An errant comment about where one works, a picture featuring an identifiable tattoo—the more information that people put online, the easier it becomes for the internet-savvy to track and identify them (a process known as “doxxing”). In the words of one such investigative journalist, “if you’ve ever stayed up all night scouring Instagram for pictures of your ex’s wedding, you can do this. It’s the same skills.”

This sort of penetration has increasingly become the domain of anti-fascist activists and investigative groups working in tandem to expose neo-Nazis. The leftist journalism organization Unicorn Riot (UR) have successfully conducted a number of such infiltration projects, primarily targeting Discord servers utilized by hate groups. At the time of this writing, UR have released the internal chats of over 180 such servers, and successfully identified dozens of members of such groups. The Huffington Post, utilizing those leaks, was able to identify at least seven active-duty military members who were members of white nationalist groups, which resulted in several of them being discharged from active service.

The individual perhaps best known for doxxing white supremacists goes by the Twitter handle @AntiFashGordon. In addition to outing numerous white nationalists himself, Gordon (a pseudonym) has even
led workshops for aspiring OSINT users. The sophistication of Gordon’s operation illustrates how seriously many of these activists take their work. Rather than simply scrolling through the internet, Gordon utilizes three phones at all times, as well as a variety of encrypted messaging apps and security measures to preserve his own anonymity.

One noteworthy element of the current environment of entrepreneurial internet vigilantism is that it seems to primarily target white nationalist groups, rather than other sorts of extremist networks (such as those run by jihadists). This can perhaps be explained by the fact that white nationalist groups, while extreme in their rhetoric, nevertheless communicate in a language (English) and utilize terminology that is relatively easy for their opponents to imitate. It seems fair to assume that an activist located within the United States would have a far easier time mimicking slurs about racial minorities than engaging in a conversation about the complexities of Wahhabist ideology. Another likely contributing factor is the prominence of white supremacy within the United States. While the threat posed by other violent ideologies such as jihadism is real, ISIS simply doesn't command anywhere near the same sort of support within the United States as do white supremacists. A recent Homeland Threat Assessment from the Department of Homeland Security noted that such groups pose “the most persistent and lethal threat in the Homeland”, and the number of fatal extremist attacks attributed to white supremacists rose from 20% to 60% between the years of 2016 and 2017 alone.

There also seems to be a somewhat justified perception among activists that law enforcement is doing far too little to address white nationalism online (as opposed to its’ rigorous over policing of Muslim communities), compelling private citizens to step in. Law enforcement has, at times, undertaken efforts to combat white nationalist movements. In the 1960’s, the FBI utilized a network of some 2000 informants to disrupt Ku Klux Klan activities across the South, at one point anonymously mailing postcards to Klansmen with the ominous message: “we know who you are.” In 1979, one particularly daring operation (immortalized in Spike Lee’s 2018 film BlackKklansman) saw a black officer from the Colorado Springs Police Department gain access to the local chapter of the KKK, posing as an avowed racist when speaking with unsuspecting Klansmen over the phone. Recent reports, however, paint a troubling picture of a policing culture in which cops not only fail to act on reports of hate speech, but frequently even participate in it themselves.

There are serious risks inherent in anti-racist vigilantism. While many of these chatrooms are populated by what one could derisively term “keyboard warriors,” others, such as the white nationalist American Identity Movement (formerly known as the cartoonishly-styled Identity Evropa), have participated in violence at events such as Charlottesville’s deadly “Unite the Right” rally in 2017. Members speak openly of committing violence against minorities, and the same sort of tracking of social-media profiles which has allowed for these white supremacists to be exposed could very well be used by white nationalists themselves in order to locate and even physically harm those doing this kind of work. While there have yet to be any actual attacks on investigators, some activists who choose to publicly identify themselves have had their homes visited by members of the groups whose rhetoric they combat online. Some left-wing activists, however, take comfort in what they
consider to be an inherent advantage over their ideological opponents. As one prominent researcher put it, “They try, but they’re fucking terrible at it because they don’t understand leftist politics. It’s easier to understand the right: They’re bigots and they hate people. All you have to do is sprinkle in a couple slurs, and you’re good.”

Although Twitter is often abuzz with triumphant stories of neo-Nazis “doxxed” by private citizens, lost in the conversation is any sort of examination of the ethics behind what amounts to a highly dangerous form of catfishing. Talia Lavin, author of last year’s *Culture Warlords: My Journey into the Dark Web of White Supremacy*, used the anonymity granted her by the internet to infiltrate a number of white supremacist chatrooms and online forums, roleplaying as a variety of different white nationalists and incels (short for involuntary celibate, a man who wishes to have sex with women but is unable to). After publicly identifying a member of a white nationalist group and leaving the rest of the group in the dark as to the traitor’s identity, Lavin managed to sow discord within the white nationalist ranks, all while hiding behind a series of online personalities radically different from her own. While Lavin’s work has been widely lauded online, there seems to have been little pushback over the fact that her identity was forged in part via the unauthorized use of strangers’ pictures.

Lavin was eventually forced to resign as a fact-checker for the New Yorker after she misidentified a combat-disabled ICE agent as a neo-Nazi, a fitting encapsulation of another problem presented by such activism: there is no oversight process for those doing the “doxing.” As reprehensible as white supremacists may be, being publicly misidentified as one by some overzealous internet crusader accountable to no one creates its own kind of hell for those on the receiving end.

For all of its reticence to engage with the issue, law enforcement at the very least adheres to strict guidelines for creating fake personas in the name of intelligence gathering, to include keeping records of any and all online aliases and requiring that aliases be screened and approved by commanding officers. Whereas the NYPD go through a review process when selecting pictures for aliases online, no framework exists to prevent activists from utilizing any pictures they wish to when constructing their false identities. Using someone else’s pictures in furtherance of a false neo-Nazi identity without their consent is not only troubling, but illegal in states like Texas.

Perhaps the most dangerous issue presented by the new wave of ideological catfishing is the fact that it stands to be readily employed by hate groups themselves. It’s understandably hard to muster any sort of sympathy for KKK Kevin being outed as such and losing his job, but those on the far right could just as easily utilize these tactics to bring about great harm to their own ideological opponents. This could take the form of targeting support groups for transgender individuals with the intention of exposing them to transphobic family members, or of Black Lives Matter activists being outed to less-than-sympathetic employers. Allowing the Twittersphere to determine which kind of vigilantism is worthy of approval or even support isn’t a successful recipe for combating hate—it’s a ticking time bomb. Without safeguards in place to hold actors accountable and
prevent malicious activity, online vigilantism will continue to exist in an ethical and legal gray area, rife with
danger and subject to malevolent use.