5

Programs or People? Participation and the Ethics of Hacktivism

Brett Lunceford

The widespread diffusion of internet access and new media technologies have opened new opportunities for social movements and protest actions. Protestors are no longer limited to acting in the physical spaces in which they reside, as protest can take place online. Moreover, as police have become increasingly militarized, potential protestors must consider whether they wish to place their physical bodies on the line and/or if they can afford to be arrested for their cause. Protesting through a virtual presence can be a powerful tool toward mitigating perceived dangers of physical protest because, as Thomas (2002) notes, "the virtual presence of the hacker is not enough to constitute a crime—what is always needed is a body, a real body, a live body" (182). In this chapter I will consider one form of digital activism: hacktivism, or politically motivated computer hacking.

Hacktivism is often referred to as "electronic civil disobedience" (ECD), but although *hacktivism* is *activism*, it does not enjoy the same protection under the First Amendment as traditional protest methods. Indeed, this chapter makes no argument concerning the legal aspects of hacktivism—hacktivism is clearly a criminal act—but rather, my focus is on its ethical dimensions. Elsewhere I have argued that scholars must consider hacktivism not merely as a criminal act, but as a rhetorical act (Lunceford 2012). Actions that are legal are not always ethical, ethical acts are not always legal, and protestors may find themselves in disagreement concerning specific tactics, even if they agree with the goals of the protest itself.

This chapter examines the arguments between two hacker groups concerning the ethical dimensions of actions that took place during the 1999 protests of the World Trade Organization (WTO) meetings in Seattle, Washington. One group,

the electrohippies collective, engaged in a distributed denial-of-service attack in order to take down the WTO's website. In a distributed denial-of-service attack, a large group of computers overloads the server of the targeted website and shuts down access to the website. Distinguishing this tactic from other forms of denial-of-service attacks, which do not require a large group of participants, is an important strategy for the electrohippies, who argued that because the denial-of-service attack required the participation of many individuals to work it was inherently democratic and, thus, ethical. Another group, the Cult of the Dead Cow (cDc), argued that the protest was unethical because it violated the principle of freedom of speech. This argument illustrates how the changing media landscape challenges the ethical principles readily accepted in traditional protest and how different groups can come to very different conclusions when employing traditional ethics.

What is hacktivism?

Wray (1999) explicitly connects the tactics of hacktivism with those of traditional protest: "The same principles of traditional civil disobedience, such as trespass and blockage, will be applied, but more and more these acts will take place in electronic or digital form: The primary site for ECD will be in cyberspace" (108). Hacktivism has become an important component in many protest activities as the internet becomes increasingly integrated into our lives. For example, the antiglobalization and the environmental movements have been particularly web-savvy in their protests (DeLuca and Peeples 2002; Juris 2005; Kahn and Kellner 2004; Van Aelst and Walgrave 2002). In some ways, social movements have had to enter the digital realm to remain relevant; McKenzie (1999) argues that "long-entrenched practices of political activism—street protests, strikes, sit-ins, boycotts—are becoming less and less effective and in their place have arisen practices of 'electronic civil disobedience' and 'hacktivism'" (¶32).

Like traditional protest actions, there are many forms in which hacktivism can take place. The two most common incarnations of hacktivism are website defacements and denial-of-service attacks. Website defacement is pretty much what it sounds like. The hacker takes control of a website and replaces the original content with a message from the hacker. In order to do this, hackers run scripts to find potential security holes, allowing the hackers to automate this aspect of hacking. As such, hackers can deface many sites in a short period of

time (Lunceford 2012). In these cases, the website itself may be inconsequential, serving only as a means of reaching potential viewers. However, these hacks can also be targeted to specific entities against whom the hackers have some grievance; for example, an antifur activist hacks the website of a furrier. In each case, the goal is to disseminate one's message.

Denial-of-service attacks, alternatively, attempt to silence the message of the target rather than replace it: "At its most basic, a denial-of-service attack is overloading a server through the use of a zombie network or a script" (Lunceford 2009b, 243). Some have compared this attack to a virtual sit-in because the principles are similar (Lane 2003; Wray 1999). Bandwidth is not infinite and a server can only handle a certain amount of traffic. When the requests for the website exceed the allotted bandwidth, others cannot access the site. The bandwidth is consumed entirely by the protestors. There are two forms of denial-of-service attacks: denial-of-service (DoS), which involves a single attacker or group, and distributed denial-of-service attacks (DDoS), which involves multiple sources of attack (Chowriwar et al. 2014; Ghazali and Hassan 2011).

It may be tempting to directly map digital strategies onto traditional protest actions. As Schwartau (2000) put it, "Graffiti on billboards, graffiti on web sites, same difference, different medium" (25). But hacktivism is more than the same tactic in a digital sphere; one cannot change the medium without changing the nature of the act in some way (see McLuhan 1994). As Postman (1993) explains, "A new technology does not add or subtract something. It changes everything" (18). One must come to new tactics like hacktivism with a fresh outlook, considering them on their own terms.

Jordan (2002) argues that "hacktivists are not so much bending, twisting and reshaping information flows as creating alternative infrastructures to enable new types of flow" (135). Hacktivism has the potential to give voice to those who would otherwise be drowned out in a flood of mass-mediated messages. McChesney (1997, 1999) and others (Aufderheide et al. 1997; Sussman 1997) have pointed out that as the mass media have consolidated, the available messages have likewise become consolidated, leaving less room for alternative voices. In this environment, it is difficult to voice dissenting opinions and present alternate viewpoints. Moreover, as the costs of participating in the public sphere become higher, fewer citizens will have a chance to participate in the deliberations that will have an impact upon their lives. Hacktivism has changed the nature of protest and some groups have created tools that allow non-hackers to participate in acts of electronic civil disobedience. For example, Electronic Disturbance Theater

created a program called Zapatista FloodNet that automated denial-of-service attacks (Lane 2003). One needed only to type the URL of the website he or she wished to attack and the program would do the rest. As Martin (2000) explains, "Electronic protesting these days is a simple matter of downloading easy-to-use software from the Web, or of visiting a protest site where you can set your browser to bombard a target site with requests for information. Anyone can be a hacktivist" (6). By allowing for the automation of political action, hacktivism allows those who may have the desire, but not the time, to participate.

The digital battle of Seattle: A tale of two ethics

Contrary to media accounts of hacking, hackers have long been political actors (Jordan and Taylor 2004; Lunceford 2009a). One hacker group in particular that has fully embraced hacktivism (even claiming that one of their members coined the term) is Cult of the Dead Cow (cDc) (see Ruffin 2004). In 1999, they formed "Hacktivismo" to emphasize this focus. The Hacktivismo Declaration (2001) draws on the United Nations Universal Declaration of Human Rights and states:

> We are convinced that the international hacking community has a moral imperative to act, and we declare:
>
> That full respect for human rights and fundamental freedoms includes the liberty of fair and reasonable access to information, whether by shortwave radio, air mail, simple telephony, the global internet or other media.
>
> That we recognize the right of governments to forbid the publication of properly categorized state secrets, child pornography, and matters related to personal privacy and privilege, among other accepted restrictions. But we oppose the use of state power to control access to the works of critics, intellectuals, artists, or religious figures.
>
> That state sponsored censorship of the Internet erodes peaceful and civilized coexistence, affects the exercise of democracy, and endangers the socioeconomic development of nations.
>
> That state-sponsored censorship of the Internet is a serious form of organized and systematic violence against citizens, is intended to generate confusion and xenophobia, and is a reprehensible violation of trust.
>
> That we will study ways and means of circumventing state-sponsored censorship of the Internet and will implement technologies to challenge information rights violations.

These words portray an extreme depiction of the hacker motto, "information wants to be free." For cDc, censorship of the internet is equivalent to "systematic violence." There are some paradoxes within this declaration, many of them dependent upon definition. For example, they recognize the right to "forbid the publication of properly categorized state secrets, child pornography, and matters related to personal privacy and privilege," but what constitutes a "properly categorized state secret?" From this perspective, all that must be done to enable wholesale censorship and remain within the bounds of this declaration is to simply declare the censored material a "state secret," a tactic that has been used to great effect in squelching the release of information even in the United States (see "Government Secrecy" 2005).

Perhaps the most problematic aspect of the Hacktivismo Declaration is the conclusion: "We will study ways and means of circumventing state-sponsored censorship of the Internet and will implement technologies to challenge information rights violations." What, exactly, is an information rights violation? Hacktivismo's argument seems to be based mainly on the consumption of information, but the production of information is likewise essential. In the Hacktivismo FAQ, they state: "We are also interested in keeping the Internet free of state-sponsored censorship and corporate chicanery so all opinions can be heard" (Ruffin, Warren, and Marie 2000–01). This underlying focus on information access and consumption at times paints them into an ideological corner. Even as they proclaim the importance of information access and decry the use of censorship, they still grant governments the ability to decide what should be censored. "Accepted restrictions" may, even in the United States, apply to critics who wish to see the government overthrown, so the kinds of critics and the types of criticism matter.

The writers of the declaration refuse to become bogged down in the details of what information should be available and what kinds of actions should be censored (besides obvious ones like child pornography), leaving this open to interpretation by the state. Hacktivismo likewise recognizes the difficulty of prescribing specific guidelines in light of varying levels of legality in different jurisdictions:

> The term "lawfully published" is full of landmines. Lawful to whom? What is lawful in the United States can get you a bullet in the head in China. At the end of the day we recognize that some information needs to be controlled. But that control falls far short of censoring material that is critical of governments, intellectual and artistic opinion, information relating to women's issues or

> sexual preference, and religious opinions. That's another way of saying that most information wants to be free; the rest needs a little privacy, even non-existence in the case of things like kiddie porn. Everyone will have to sort the parameters of this one out for themselves. (Ruffin, Warren, and Marie 2000–01)

As one could expect, other hacker groups have come to different conclusions as to how these parameters should be sorted out. One such group that came to different conclusions is the electrohippies collective, a hacktivist group in the United Kingdom.

Within hacktivist collectives, an age-old question arises: do the ends justify the means? And, more precisely, which means justify desired ends? This is an argument that plays out in the white paper published by the electrohippies, titled "Client-side Distributed Denial-of-Service: Valid Campaign Tactic or Terrorist Act?" and the response to this action by cDc. In their white paper, the electrohippies defend the use of client-side denial-of-service attacks and reveal their anticapitalist leanings from the very beginning:

> As Jesus ransacked the temple in Jerusalem because it had become a house of merchandise, so the recent attacks on ecommerce web sites are a protest against the manner of its recent development. But, do we label Jesus as a terrorist? Those involved probably have a reverential view of the 'Net. The public space that the 'Net represents is being promoted as a marketplace for large corporate interests, and many of those who use the 'Net for other purposes are dissatisfied with this. (DJNZ and Collective 2001, 1)

The electrohippies clearly place the internet within the realm of the public sphere and decry the commercial nature of the internet and the associated concentration of power by corporate interests, comparing the internet to the den of thieves that Jesus Christ cast out of the temple (Mk 11:17). Like cDc/Hacktivismo, the electrohippies have a penchant for placing their causes in epic terms and share a commitment to hacking as a form of social change, but there are many differences between the two groups; these points of disagreement illuminate ideological schisms within the hacker community concerning appropriate means for enacting hacktivism.

The first difference between the groups concerns how each views the legitimacy of denial-of-service attacks. The electrohippies argue that client-side denial-of-service attacks have greater legitimacy as a protest action because of their distributed nature. "Client-side distributed actions require the efforts of real people, taking part in their thousands simultaneously, to make the action

effective. If there are not enough people supporting [the] action it doesn't work. The fact that service on the WTO's servers was interrupted on the 30th November [and] 1st of December, and significantly slowed on the 2nd and 3rd of December, demonstrated that there was significant support for the electrohippies action" (DJNZ and Collective 2001, 3). They contrast this form of denial-of-service attack with server-side denial-of-service attacks that can be done with only a few individuals and a legion of zombie computers. The fact that the electrohippies use client-side attacks gives them what they call a "democratic guarantee."

cDc rejects this premise, arguing that

> Denial of Service, is Denial of Service, is Denial of Service, period. The only difference between a program like Stacheldraht [a DDoS application written by The Mixter] and the client side javascript program written by the Electrohippies is the difference between blowing something up and being pecked to death by a duck. And if numbers lend legitimacy—as the Electrohippies propose—then the lone bomber who tried to assassinate Hitler in his bunker was wrong and the millions who supported the dictator were right. (Ruffin 2000)

Ignoring for a moment the resort to Hitler in this statement, this illustrates a fundamental disagreement on the nature of online democratic practice. In essence, the electrohippies seem to subscribe to the great hope of democracy—that the majority of the people will support that which is just and good the majority of the time.

If cDc does not believe that numbers grant legitimacy, then what does? In their appeal to the First Amendment, it is difficult to ascertain whether cDc appeals to a transcendent ideal of freedom of speech or an appeal to the First Amendment as rule of law. Either of these possibilities are ethically problematic. If they are appealing to a transcendent ideal of freedom of speech, they do so unilaterally and with little authority. If they base their appeals on the First Amendment, they gloss over the fact that the internet is a global entity and that the United States Constitution is not the standard by which all other nations should be judged (Lunceford 2013). Each group is committed to the idea of free exchange of information, although they differ in what information should be available to whom and by whom. The main concern of cDc is government censorship of information. The right to access information belongs to the individual, so cutting off any information is undesirable, even if it comes from a controversial entity. In other words, the information flows toward the individual. The electrohippies, on

the other hand, see the flow of information going in the other direction—toward the organization from the individual. Silencing the WTO's website is less an act of censorship and more an act of compelling the organization to listen to the protestors. Each seeks to perpetuate the "I-Thou" relationship prescribed by Buber (1958), but differ in who deserves to be "I."

This raises an ethical question however, as Buber (1958) would likely wonder at the wisdom of ascribing either I or Thou to such institutions as the WTO, remarking that "the separated *It* of institutions is an animated clod without a soul" (53). In short, who deserves to speak, and are individuals ethically obligated to listen to an organization, especially a nongovernmental organization like the WTO? For cDc, this seems an irrelevant question, as they seem driven by a sense of duty toward the principle of freedom of speech for everyone. In this regard, they seem to follow Kant's ([1785]1959) categorical imperative: "Act only according to that maxim by which you can at the same time will that it should become a universal law" (39). In other words, if it is unacceptable to squelch speech for one person, one must accept free speech for all. As such, they are placed in the position of defending the WTO's right to expression, regardless of what they say. The electrohippies recognize that by engaging in denial-of-service attacks they prevent free speech, but they justify their actions under two conditions: the target must be reprehensible to a majority of the people, and the attack should be limited to a specific, politically salient occasion. They point out that their actions against the WTO only took place during the conference in Seattle, which not only provided the opportunity to raise consciousness concerning the actions of the WTO, but also allowed those who opposed the WTO to voice their arguments (DJNZ and Collective 2001, 7–8). Although this may work in theory, it may not be very effective in practice. In the case of the WTO protests, where the actions of the electrohippies were likely to generate news coverage in addition to that already generated by the disruptions taking place in the physical space of Seattle, this would likely be an effective use of denial-of-service attacks. Still, the question remains whether it did anything to actually raise consciousness concerning the WTO. One can only speculate on how effective this act of hacktivism would be with little action taking place in physical space; indeed it seems unlikely that the electrohippies would engage in such actions because they would be less likely to bear a stamp of legitimacy (the organization must be reprehensible to a majority of the people and the widespread protests seemed to serve as evidence of this fact).

In contrast to the cDc's Kantian leanings, the electrohippies seem more aligned with the utilitarian school of ethics, which considers the outcomes of one's actions. Their defense of the action against the WTO call to mind Bentham's (1823) argument that "it is the greatest happiness of the greatest number that is the measure of right and wrong" (vi). If one group (the WTO) must be silenced to provide a space in which the many (the protestors) can be heard, the net result in happiness is positive. As such, the two groups are fundamentally at odds concerning what constitutes the greatest good. The electrohippes are willing to accept some collateral damage in free speech if it makes more people happy, while cDc is unwilling to budge on squelching freedom of speech out of a sense of duty.

Another fundamental difference between the two groups concerns the ontological nature of cyberspace compared to physical space. The electrohippies argue that "as another part of society's public space the Internet will be used by groups and individuals as a means of protests. There is no practical difference between cyberspace and the street in terms of how people use the 'Net" (DJNZ and Collective 2001, 2). The electrohippies suggest that tactics that work in the offline world will work in the online world, which is demonstrated in their comparison between online and offline protest actions. "Distributed clientside DoS action is only effective if it has mass support, and hence a democratic mandate from a large number of people on the Net to permit the action to take place. These type[s] of actions are directly analogous to the type of demonstrations that take place across the world. One or two people do not make a valid demonstration—100,000 people do" (DJNZ and Collective 2001, 5). The electrohippies view the internet as a public space rather than a private space, so they reject arguments of virtual trespassing. Once again, we see the principle of greatest happiness at work in the electrohippies' reasoning. The website may belong to the WTO, but the internet belongs to everyone and no one person or entity has any special right to be heard over the masses. If the website is publicly accessible and a mass of people want to enter the website repeatedly in order to hinder access to the site, this should be their right. The electrohippies argue that the strategies of the digital world and the strategies of the physical world are equally valid, and this is demonstrated by means of electronic protest. They are borrowing strategies that have worked in the past (sit-ins, demonstrations) and adapting them to the digital world. Only the location has changed.

cDc acknowledges that for street protests, larger numbers suggest greater legitimacy—cDc member Oxblood Ruffin (2000) notes that he has participated

in such protests—but they dismiss the core assumption that there is little difference between cyberspace and physical space: "Where a large physical mass is the currency of protest on the street, or at the ballot box, it is an irrelevancy on the Internet. Or more correctly, it is not always necessary. . . . But to think that it takes a lot of people to execute an act of civil disobedience on the Internet is naive. Programs make a difference, not people." The desired end of shutting down a website can be done with an efficient program much more effectively than hoping that enough individuals take part in the action. But although cDc is correct that the nature of the internet allows for different modes of protest that are impossible in traditional protest (e.g., using only a few hackers to create a digital sit-in that would otherwise take thousands), to say that a mass of people is an irrelevancy is an overstatement. As Jordan (2002) observes, a large mass of people makes it a "popular protest"; "A mass event needs the masses. Hacktivists producing denial-of-service actions choose a technically inefficient means to serve politically efficient ends" (125). Even as cDc recognizes that the online environment changes the nature of legitimacy, they overlook how this may affect their own standards of legitimacy. cDc seem to draw their legitimacy from transcendent values (e.g., freedom of speech), but there is no reason why those values must function the same way in both online and offline environments. Both the electrohippies and cDc seem to place greater importance on the values of the offline world.

cDc argues that programs are what matter in cyberspace, the electrohippies argue that people are what matter, and both have written programs for use in protest activities. But the question of whether people or programs matter more in cyberspace depends more on one's ethical stance than on what is technologically possible. Both the electrohippies and cDc are technologically savvy enough to create programs that would take full advantage of the medium of cyberspace, so this must be a conscious choice. For the electrohippies, the means are precisely what justify the ends. They are ethically justified in silencing the WTO because a large number support this action. For the cDc, the desired ends are morally suspect and thus would be indefensible by any means.

This argument between the electrohippies and the cDc illuminates some of the basic issues surrounding the ethics of hacktivism and illustrates how two groups with similar aims (social justice) can disagree on the means to that end. With the electrohippies invested in the "greatest happiness" principle (Mill 1907, 9–10) and cDc duty-bound to the principle of freedom of speech, they cannot help but arrive not only at different conclusions, but at different means to those

ends. If the goal is to fight censorship and ensure free speech for all, without exception, then a technological solution may be the most effective means of doing so. On the other hand, if one's ethics require both qualitative judgments and quantitative validation, then creating a structure that facilitates a large number of participants in the protest action would be desirable. But because each considers their respective stances to be axiomatic truths—cDc argues that denial-of-service attacks violate First Amendment rights and the electrohippies believe that the more people involved, the more democratic—the electrohippies and the cDc talk past each other.

Despite these differences, both parties have valid concerns and flaws in their arguments. Do we take for granted that the First Amendment is always good? Is this an appeal to the law or an appeal to the idea that free speech is an inalienable human right? If so, to whom does that right belong—to citizens, corporations, political parties? Although the courts have ruled that commercial speech is not protected by the First Amendment, a recent Supreme Court decision equates financial political contributions with protected speech, opening the door for corporate entities to enjoy even more protections (for more on the problematic legal nature of corporate entities, see Aljalian 1999; Edwards and Valencia 2002; Manning 1984; Rafalko 1989; Wilson 1994). But corporate entities do not enjoy all of the same rights as citizens, so the argument that cDc makes about suppressing a company's First Amendment right is problematic, especially when upholding the website owner's freedom of speech by squelching that of the hacktivists denies the hacktivists' equally valid (in terms of the First Amendment) right to peaceably assemble. The electrohippies seem to believe that to have thousands of people on your side is to have justice on your side. Although numbers do grant at least a veneer of legitimacy—despite cDc's claims—the amount of people it takes to shut down a website is a very small percentage of the population. Even if one takes at face value the electrohippies' assertion that around 450,000 people around the world took part in the action against the WTO (believing for the moment that these were separate individuals, which would be difficult to verify), then considering a world population of six billion people, roughly 0.0075 percent of the world's population participated. Their argument that "tens of thousands (if not hundreds of thousands) of people" provide a "democratic guarantee," then, is not really accurate (DJNZ and Collective 2001, 7).

The disagreement between the electrohippies and the cDc is a continuation of familiar arguments concerning protest rhetoric: Do the ends justify the means? What is the difference between terrorism and activism? Where does one draw the

moral and ethical lines for protest behavior; are extralegal means of protest still ethical? These questions are not inconsequential, and the answers to each one by different groups are bound to differ depending on the fundamental assumptions held by each group. If an organization has a fundamental assumption, for example, that the legal system is irreparably corrupt and broken, then such an ideology would invite extralegal means of protest.

One fundamental assumption of the electrohippies is that they are not simply silencing the WTO—they are opening a space in which the voices of others, which are drowned out when the WTO is granted the opportunity to continually speak, can be heard. In considering the restriction of protest activities in white residential neighborhoods during the civil rights movement, Haiman (1967) asks:

> The question, I think, is what price a society is willing to pay to insure that the messages of minority groups are not screened out of the consciences of those to whom they are addressed. For once the principle is invoked that listeners may be granted some immunity from messages they think they would rather not hear, or which cause them annoyance, a Pandora's box of circumstances is opened in which the right of free speech could be effectively nullified. (106)

Similar arguments can be made concerning the WTO protests. Hacktivists can easily post web pages arguing against WTO policies, just as Black marchers could have easily marched in their own neighborhoods during the civil rights era. The point of the marches was to take the message to those whom the protestors believed needed to hear it. The electrohippies' stated goal was to "substitute the deficit of speech by one group by encouraging debate with others" (DJNZ and Collective 2001, 7). The cDc would argue that this is still wrong, but the electrohippies may see no other way to place their message on a relatively level-playing field with the WTO, which has the backing of the establishment. As Barnlund and Haiman (1960) explain:

> When one person or a few people in a group or society possess all the guns, muscles, or money, and the others are relatively weak and helpless, optimum conditions do not exist for discussion, mutual influence, and democracy. Discussion in such circumstances occurs only at the sufferance of the powerful; and generous as these persons may sometimes be, they are not likely voluntarily to abdicate their power when vital interests are at stake. (12)

Ethical considerations of hacktivism must also consider its lack of permanence. Unlike the physical world, the medium of the internet is a constantly shifting,

evolving space. One cannot simply re-upload a building that has been burned down, but one can replace a defaced website with a backup. In other words, "hackers are not defacing property so much as they are defacing a presentation of self that can quickly be reclaimed" (Lunceford 2012, 44). Of course this creates problems when attempting to quantify the damages to the organization that has been defaced. It is difficult to know how to compensate an organization for a brief loss of image. After all, most hackers do not attempt to represent the organization—although this has happened in protest actions (Yes Men 2004)—because they want the defacement to be obvious. Therefore it is unlikely that visitors to the defaced site will mistake the defaced site for an authentic version of the website. Denial-of-service attacks are likewise transitory; the electrohippies limited their actions to the dates in which the WTO meetings were taking place. Even if they wished to continue the attack, the WTO would be able to counter by addressing the technical flaw in the server or by increasing available bandwidth. In short, any attack that takes place in the digital domain will be temporary at best. When considering the ethics of hacktivism, this fact must be taken into account—the destruction of a virtual presence is not equal to the destruction of a physical presence.

Conclusion

The debate between the cDc and the electrohippies illustrates the perils of mapping the ethics of the industrial age onto the internet. The cDc's assertion that programs, not people, matter in the digital realm is a profound refutation of most social movement strategies in which the goal is to mobilize resources—most importantly people. Perhaps the electrohippies cling to the notion that a large enough mass of bodies will somehow grant legitimacy to one's cause because this is how causes have often been evaluated in the past. But hacktivism need not adhere to old notions of legitimacy any more than it need slavishly ape old protest tactics. Hacktivism allows for new forms of protest much as the internet allows for new ways of constructing citizenship, governments, and society (see Jordan 1999, 2002). Indeed, Bodó (2014) explains that hacktivism itself is undergoing a kind of evolution, moving away from the model championed by the electrohippies in which the nonspecialist can be a hacktivist and toward "a much more potent form of hacktivism, which relies on insiders to expose the ways power operates and create a more transparent society" (8).

As the world becomes more globalized, protest activities likewise become more globalized because the effects of organizations and legislation may be experienced beyond national borders. Moreover, because there is no longer a need to physically assemble, the risks inherent in assembly are dissipated as well. One no longer need risk bodily harm by engaging in protest activity. Law enforcement officials are highly skilled in crowd control, but in the virtual domain, the playing field is slanted toward the activists. But more importantly, one no longer need even be somewhere at all. As the cDc notes, one can simply automate protest. This leads to another ethical consideration; one should exercise caution when one press of a button can reproduce the actions of millions.

Still, hacktivism has a long way to go before it can yield the same effects of traditional protest, and traditional means of protest seem to be alive and well. Marches in Washington, D.C. are still rather common. Letter-writing campaigns are also in heavy use. Lobbyists still wield significant power. It seems that there are many for whom protest occurs outside of the digital realm. One limitation of hacktivism is its relative invisibility. The first order of business for any protest action is to gain the attention of the media (Oliver and Myers 1999). Physical demonstrations of protest are often covered in the media, but the electrohippies' actions have been largely forgotten. Hackers stand little chance against impressive displays of black bloc anarchists and smashed windows in the battle for gaining mindshare (see DeLuca and Peeples 2002).

Hacktivism seems to be a double-edged sword. There are ethical dilemmas concerning the silencing of other voices, but there is also the increased possibility for more individuals to engage in activism in previously impossible ways. Hacktivism takes advantage of the networked society in ways that traditional means of protest cannot. However, these hacktions are unlikely to stand alone successfully—they are best understood within the context of movements and actions that take place in the physical world. We are far from the science fiction fantasy of leaving the body behind as our minds traverse the vast expanse of cyberspace. As such, we cannot completely abandon the physical world and the material considerations with which most social movements are concerned.