

Hacking as Politically Motivated Digital Civil Disobedience: Is Hacktivism Morally Justified?

Kenneth Einar Himma, Ph.D., J.D.
Seattle Pacific University

Forthcoming in Kenneth Einar Himma (ed.), *Readings on Internet Security: Hacking, Counterhacking, and Other Moral Issues*, Jones & Bartlett

Hackers believe that non-malicious intrusions are morally permissible and have offered a number of arguments purporting to justify such intrusions. Some hackers believe, for example, these intrusions are justified because they increase humanity's stock of knowledge about the relevant technologies and thereby promote research that will ultimately make the Internet more secure. Some believe that any barriers to information are morally illegitimate and hence deserve no respect – including barriers that prevent a person from accessing the information on another person's computer.

These arguments have not persuaded many theorists or laypersons.¹ To begin, it is not clear that unauthorized digital intrusions are necessary to increase the stock of knowledge; community-minded hackers could always produce the same good by hacking each other or by going to work for some software company. Further, the idea that all barriers to information are morally illegitimate is incompatible with the right to information privacy; if all information should be free, then our efforts to protect sensitive information about ourselves (like social security numbers) are morally wrong. But regardless of whether the premises of these arguments are correct, the conclusion doesn't follow because unauthorized digital intrusions involve a trespass upon computers and networks belonging to other people and thereby violate the victims' rights to their physical (as opposed to intellectual) property.

Recently, a more plausible line of justification has emerged. A number of writers, such as Manion and Goodrum (2000), have argued that certain attacks on government and corporate sites can be justified as a form of political activism. The argument is roughly as follows. Since civil disobedience is morally justifiable as a protest against injustice, it is sometimes permissible to commit digital intrusions as a means of protesting injustice. Insofar as it is permissible to stage a sit-in in a commercial or governmental building to protest, say, laws that violate human rights, it is permissible to intrude upon commercial or government networks to protest such laws. Thus, digital intrusions that might otherwise be morally objectionable are morally permissible if they are politically-motivated acts of electronic civil disobedience – or “hacktivism,” as such intrusions have come to be called.

A shorter version of this paper was presented at ETHICOMP 2005 in Linkoping, Sweden.

¹ For a critical evaluation of these lines of argument, see Spafford (1992) and Himma and Dittrich (forthcoming 2006).

In this essay, I consider the issue of whether and when hacktivism is morally impermissible. First, I argue that the above line of reasoning wrongly presupposes that committing civil disobedience is morally permissible as a general matter of moral principle; in an otherwise legitimate state, civil disobedience is morally justified or excusable only in narrowly defined circumstances. Second, I attempt to identify a reliable framework for evaluating civil disobedience that weighs the social and moral values against the social and moral disvalues. Third, I apply this framework to acts of hacktivism. I argue that hacktivism is impermissible insofar as such acts result in significant harms to innocent third-parties or insofar as the persons responsible for such acts conceal their identities to avoid the potential legal consequences.

I. Civil Disobedience and Morality

A. What is Civil Disobedience?

It has come to be an article of faith among many activist-minded persons that acts of civil disobedience are, as a general moral matter, not only permissible but positively good. On this view, it is true not only that people who commit acts of civil disobedience violate no moral obligations, but also that such persons are actually producing something that counts as a moral good. Accordingly, these behaviors deserve praise rather than punishment.

This common view cannot be evaluated without saying something about the concept of civil disobedience. While a fully comprehensive analysis of the concept of civil disobedience is beyond the scope of this paper, I think it is fair to say that, as a conceptual matter, acts of civil disobedience involve the following elements: (1) the open, (2) knowing (3) commission of some non-violent act (4) that violates the law (5) for the expressive purpose of protesting the law (or the legal system) or calling attention to its injustice. Since acts of civil disobedience are deliberately open so as to call attention to the putative injustice of the law, they are fairly characterized as “political expression.”

Several comments about these elements are in order. First, as I have defined it, it is a necessary condition for an act to count as civil disobedience that it openly disobeys the law. Clandestine acts of disobeying law do not count as civil disobedience, even if they are motivated by a desire to protest the law. The openness of an act of civil disobedience signals to the public that the act is intended to call attention to the injustice of some element of the law or legal system; indeed, as we will see, this feature of civil disobedience helps to make it reasonable to think such acts are morally permissible.

Second, it is a necessary condition for an act to count as civil disobedience that it be non-violent; violent acts, regardless of motivation, do not count as “civil” disobedience. As the notion is traditionally understood, a violent act is one that involves *physical* force and results in damage to *physical* property or harm to one’s *physical* person. It is worth noting, at the outset, that the traditional understanding of violence seems to preclude the possibility of digital violence; unauthorized digital trespass is neither fairly characterized

as “physical force” nor as resulting in “physical harm or damage.”² A digital act might not be fairly characterized as “civil disobedience,” but it will be for some other reason than that the act fails to satisfy the non-violence element of civil disobedience.

Third, to count as civil disobedience, an act need not target a law or system that is unjust as an objective moral matter. It is enough that the actor is motivated by a belief that the law or system is unjust and that the act is contrived to protest it and call attention to its injustice. The conceptual elements of civil disobedience, then, imply a purely subjective element that makes reference to the beliefs and motivations of the relevant class of actors – rather than to the objective moral quality of the law or system.

It should be noted, however, that the subjective element is a necessary condition for civil disobedience. Someone who breaks the law for some other purpose than to protest or call attention to the injustice of a law is not committing an act of civil disobedience. Indeed, someone who believes the law unjust and disobeys it does not commit an act of civil disobedience if her violation of the law is motivated by some other desire than a desire to protest or call attention to its injustice. Acts of civil disobedience are, by their very nature, expressive in the sense that the point is to communicate something to someone.

B. Are Acts of Civil Disobedience Morally Permissible?

It is tempting to infer from the above analysis of the concept of civil disobedience, together with the claim that people have a moral right to free speech, that acts of civil disobedience, as political expression, are morally justified as an exercise of the moral right to free speech. On this line of analysis, the right to free speech entails a right to express one’s political views about the legitimacy of the law. Since the very point of civil disobedience is to call attention to the illegitimacy of the law, it is a morally justified exercise of the right to free expression.

This line of reasoning is problematic. Civil disobedience might be expressive, but it is considerably more than that. Civil disobedience, by its nature, involves disobeying something that has the status of law. It is one thing to *assert* that a law is unjust; it is another thing to deliberately and openly behave in a manner that violates the law; the former is a pure speech act, while the latter is behavior. Civil disobedience, then, might be expressive conduct, but it is primarily *conduct* and secondarily expression.

Ordinary views about the moral right to free speech commonly distinguish between speech acts and expressive behavior. On these views, expressive behavior is subject to more stringent moral limits than those to which pure speech is subject. One might seek, for example, to make a point about sexual morality by having sex in public, but the moral right to free speech does not entail a right to have sex in public for the purpose of promoting some view about sexual morality. One has a moral right to express oneself, but the protection afforded by that right extends further with respect to pure speech acts than with respect to acts that are primarily conduct and secondarily expression.

The reason for this, of course, has something to do with the effects on other people of these different kinds of act. As a general matter, pure speech acts are reasonably

² I do not find the idea that violence is necessarily physical particularly plausible, but there is no reason to challenge it in this essay. Nothing turns on this idea.

calculated to affect only the mental states of the audience; a joke, for example, is intended to induce a sense of amusement in the listener. The effects of pure speech acts intended to express a political or moral position, however, are somewhat narrower: such acts, other things being equal, are calculated to affect only *doxastic* states in any morally significant way. The point of this class of speech acts is to alter or reinforce the belief structure in the audience.

It is true, of course, that a speech act intended to express a position can have other effects; an obscene speech act can cause offense, shame, and perhaps something resembling emotional trauma to someone who witnesses it. But pure speech acts intended to express a position, as a general matter, are tend to affect only the doxastic states of the audience; the point is to communicate something in order to persuade or induce belief in the audience.

In contrast, while conduct might frequently be *intended* to only affect doxastic states, conduct tends to have effects on other states in which a person has a strong interest. Someone who seeks to express anger with you by hitting you not only affects your doxastic states, but also runs the risk of causing you physical and emotional injury. Injury is just not a reasonably likely outcome from pure speech acts of just about any kind.

As is evident from the examples above, these additional effects of conduct can implicate morally significant interests. Someone who injures another person because she expressed her anger violently has affected morally significant interests of the other person. Someone who causes great offense to another person by masturbating in front of her has affected interests that are morally significant. Conduct is far more likely than pure speech to implicate such interests precisely because it is reasonably calculated to have other effects than on doxastic states, which receive comparatively little moral protection. Conduct, unlike pure speech, is not the kind of thing with primary effects limited to doxastic states.

None of this, of course, should be construed to deny that violating the law might sometimes be morally permissible, and even obligatory, in certain circumstances. Legal and political philosophers are nearly unanimous in believing not only that there is no universal moral obligation to obey the law, but also that there is no general moral obligation to obey the law of even reasonably just states; even reasonably just states, like morally wicked states, might sometimes enact legal content so morally problematic that it does not generate a moral obligation to obey.

At an intuitive level, this is quite plausible. It seems clear, to begin, that citizens in Nazi Germany were morally obligated to violate many laws. But it seems also clear that citizens of the U.S., a reasonably just state, were, at the very least, morally permitted to disobey Jim Crow laws because of their egregious injustice. In such circumstances, one need not justify such behavior by reference to the right to free speech.

The circumstances in which one is permitted or obligated to disobey the law, however, will be comparatively rare in a morally legitimate democratic system with a body of law that is largely, though not perfectly, just for a number of reasons. First, citizens have alternative channels through which to express their political views in morally legitimate democratic systems. Since such systems recognize a legal right of free speech against the

state, citizens can express their views through pure speech acts and have a growing array of media available to them that can be used to express their views – including democratizing digital media, like websites and blogs. The easy availability of such avenues of speech operate to circumscribe the circumstances in which someone is permitted to take the law into her own hands, so to speak, by deliberately flouting it.

Second, one of the justifying features of democracy is that, properly administered, it affords each person an equal voice in determining what content becomes law. Someone who violates democratically enacted law is arrogating to herself a larger role than that to which she is entitled in a democracy. It is presumptively (as opposed to conclusively) problematic to circumvent democratic procedures in this way – again, assuming that such procedures are legitimate and legitimately administered.

Third, while legitimacy theorists once focused on trying to show that morally legitimate systems give rise to a general content-independent moral obligation to obey law and hence an *absolute* permission to enforce the law, this idea has fallen out of favor; the consensus is now that a morally legitimate state may, as a general (though not absolute) matter, permissibly enforce laws that are reasonably thought just. As is evident from the discussion above, even a morally legitimate state might produce legal content so patently unjust that the state may not permissibly enforce the law.

Even so, it is important to realize that the law of a morally legitimate system will more often than not give rise to a moral obligation to obey the law. It is hard to make sense of the idea that the state is morally justified in coercively enforcing a law against a citizen (with, e.g., threat of incarceration) if it is not morally wrong to disobey *that* law. It is reasonable to assume that a citizen may be punished for disobeying a law (either directly in the case of criminal law or indirectly in the case of civil law through use of the contempt sanction) only insofar as he or she is morally culpable for disobeying it. Since a person can be morally culpable for disobeying a law only insofar as he or she has a moral obligation to obey it, any law that is justifiably enforced by the state will give rise to a moral obligation on the part of citizens to obey it.

The idea that there are limits on the scope of even a legitimate state's permission to coercively enforce the law suggests, rightly, that civil disobedience is sometimes morally justified. In cases where an otherwise legitimate state has enacted a sufficiently unjust law that falls outside the scope of its coercive authority, citizens have a qualified moral permission to disobey it. That is, in cases in which the state is not justified in coercively enforcing a law, citizens may permissibly disobey that law because it does not give rise to any moral obligation to obey.

But this permission is qualified by a number of factors. To begin, it is reasonable to think that acts significantly impinging on the interests of innocent third-parties are not justified. There are moral limits on the extent of the costs one may permissibly impose on innocent third-parties. Conduct that, for example, is reasonably calculated or likely to result in loss of innocent life is generally not permissible – regardless of whether the conduct is expressive. It is morally impermissible to yell “Fire” in a crowded theater precisely because the resulting reaction is likely to result in a stampede that may result in significant harm to another person.

Moreover, it is reasonable to think that disobedience must be properly motivated in order to be justified. Even acts that are generally permissible might be morally problematic when motivated by malicious intentions. If I give you something fairly characterized as a “gift” with the intention of making you feel you have to do something for me down the line, I have done something morally wrong.

Finally, it makes a difference as to whether or not someone is willing to accept responsibility under the law for her acts. Open disobedience seems, other things being equal, morally preferable to clandestine disobedience – a point that is especially relevant to *civil* disobedience. Someone who, say, openly performs an act of civil disobedience knowing he or she will be arrested seems more deserving of moral respect than someone who disobeys the law and attempts to conceal his or her identity. Intuitively, there is a world of difference, for example, between someone who openly defaces a billboard in front of fifteen police officers to protest its content and someone who does so in a clandestine manner hoping to avoid detection. One seems fairly characterized as vandalism while the other, even if ultimately unjustified, does not.

This is especially true of electronic civil disobedience. One worry that many theorists share about hacktivism is that it can be difficult to distinguish an act of electronic civil disobedience from an act of cyberterrorism. Huschle (2002) argues that hacktivists should make it a point to accept responsibility for their actions precisely to ensure that their acts are not mistaken for acts of cyberterrorism, which could cause significant disruption in the population beyond what was intended to result from their acts. Similarly, Manion and Goodrum (2000) contend:

[T]he justification of hacktivism entails demonstrating that its practitioners are neither “crackers” – those who break into systems for profit or vandalism – nor are they cyberterrorists – those who use computer technology with the intention of causing grave harm such as loss of life, sever economic losses, or destruction of critical infrastructure. Hacktivism must be shown to be ethically motivated (15-16).

The acceptance of responsibility sends a strong signal that the act is motivated by a principled stand. The most obvious explanation for the behavior of someone who breaks a law *knowing* that she will suffer some unpleasant legal consequences – at least in circumstances in which she does not stand to gain some more significant material benefit – is that the act of disobedience is motivated by considerations we would intuitively regard as morally commendable. Such acts of disobedience might not succeed in expressing the particular principles motivating the act, but they generally succeed in expressing that the act is motivated by moral considerations, a feature that operates to legitimize these acts.

There is another reason that acceptance of responsibility is a necessary element in justifying an act of civil disobedience. Someone who breaks the law breaches the public peace and contributes to a public sense of vulnerability and insecurity; if someone is hacking into machines all around me, I respond with feelings of vulnerability and insecurity – feelings that are fairly characterized as constituting an injury. The willingness of the perpetrator to accept responsibility usually (though not necessarily)

signals that the breach of the public peace is exceptional rather than part of a general pattern of misconduct and need not give rise to feelings of vulnerability and insecurity.

C. Should Unjustified Civil Disobedience be Punished?

A second important moral issue regarding civil disobedience is whether the state *should*, as a moral matter, punish unjustified acts of civil disobedience. A couple of observations would be helpful by way of clarification. First, the claim that it is permissible for a legitimate state to punish unjustified acts of civil disobedience does not imply that it is obligated to do so – or even that it should do so. The claim that act *A* is morally permissible, as a logical matter, is consistent with the claim that not-*A* is morally permissible.

Second, the claim that *A* is permissible does not imply that *A* is the best thing to do from the standpoint of morality. In circumstances in which *A* and not-*A* are both permissible (which frequently occurs), only one of the two options can be *the* best from the standpoint of morality. If, for example, giving to charity is not obligatory, then not-giving is morally permissible. However, it seems clear that, absent exceptional circumstances, not-giving is not ideal from a moral point of view. Other things being equal, it is better to give than not to give.

Accordingly, the issue of whether the state should punish civil disobedience is different from the issue of whether it is permissible for the state to punish civil disobedience – though it is crucial to note that there is some relationship between them. If it is not permissible for the state to punish civil disobedience, then it follows that the state should not punish civil disobedience; one should not do what one is not permissible. But, as was seen above, the two issues are logically distinct because the claim that it is permissible for the state to punish civil disobedience does not imply that it should; if not doing so is ideal, then the state should not punish such acts.

Though the issue of whether *the state* should punish civil disobedience is frequently conflated with the issue of whether it is morally permissible *for individuals* to engage in civil disobedience, the two are distinct issues. There might be any number of reasons why the state should tolerate an act that is morally impermissible. For example, lying is presumptively impermissible, but the social costs of enforcing perfect honesty (including those to privacy) seem to militate decisively against attempting to prohibit all instances of dishonesty. Advocating racist views is morally impermissible, but one might have a moral right to assert patently immoral views.

This raises the question of whether, and under what circumstances, a morally legitimate state should punish *unjustified* (as opposed to justified) acts of civil disobedience. Proponents of civil disobedience have offered a number of reasons for thinking that the law should not, as a general matter, punish even unjustified acts of civil disobedience. First, acts of civil disobedience, even unjustified ones, call attention to laws that ought to be changed because they are unjust or because they lack sufficient support among citizens. Like any other form of speech, acts of civil disobedience can promote moral dialogue and debate, which conduces to the benefit of all.

Second, proponents maintain that acts of civil disobedience do not typically result in morally significant harm to other persons. A sit-in at a local restaurant might

inconvenience other patrons, but minor inconvenience does not justify punishing participants. Indeed, according to the proponent, the benefits of civil disobedience greatly outweigh the costs; and for this reason should not be punished.

Neither of these arguments is successful in justifying the general claim that civil disobedience ought not to be punished. For starters, it is true that civil disobedience can stimulate debate and presumably open minds, but it is also true that civil disobedience can close them as well because civil disobedience is not merely speech. Someone who commits an act of civil disobedience runs the risk of alienating people and thereby closing channels that would otherwise be available for debate. I doubt, for example, that anyone who burned U.S. flags to protest laws prohibiting flag-burning did much to change the minds of those who supported those laws. Indeed, I suspect that such behavior led supporters of laws prohibiting flag-burning to believe that stiffer penalties should be authorized for violating those of laws. Unlike the act of giving a reasoned argument, acts of civil disobedience are likely to alienate many members of the community.

Moreover, it is not necessarily true that acts of civil disobedience do not result in morally significant harm to a person. After citizens in the state of Washington passed an initiative banning affirmative action in public institutions (an initiative I think is unjust and unfair), opponents marched onto a highway bridge and blocked traffic for hours. As far as I know, no one was significantly harmed by this protest, but it is not difficult to see that this could have resulted in significant harm: someone could have lost a job or, worse, been denied essential medical service because of the traffic jam caused by this act of civil disobedience. Injury to morally significant injury is always a possible result of civil disobedience.

D. An Epistemic Issue in Justifying Civil Disobedience

Supporters of civil disobedience also argue that the state should not punish civil disobedience because the motivation is a laudable one. Since acts of civil disobedience are, by definition, motivated by conscience, it is not entirely clear what the legitimating point of punishment would be. One might think, for example, that someone who commits an act of civil disobedience does not need to be either rehabilitated or segregated for the protection of other people (which are two legitimating points of punishment). Further, one might think that persons apt to commit *open* acts of civil disobedience are willing to accept a proportional punishment and even court such punishment and hence cannot be deterred by the threat of punishment (another legitimating point of punishment).

As it turns out, the mental state of someone who commits an act of civil disobedience is not entirely unproblematic from a moral point of view. While such a person's *motivations* might be laudable, she will likely have another mental state that is not unproblematic from a moral point of view. Someone who commits an act of civil disobedience is usually acting on the strength of a conviction that is deeply contested in the society – and, indeed, one that is frequently a *minority* position.

This, by itself, can obviously be laudable in many circumstances. The courage to act on one's convictions and the willingness to sacrifice for one's convictions are both virtues. We encourage a child, for example, not to follow the crowd when doing so is wrong or

foolish, knowing that such behavior will frequently result in unpleasant social consequences to the child, such as being ridiculed or ostracized. One who is willing to risk ridicule and ostracism in order to honor her moral convictions is courageous and deserves praise.

But there are clear moral limits on how far one can go in acting on a contestable moral conviction. To take an extreme case, Paul Hill argued that he was morally justified in murdering John Bayard Britton, an abortion provider, by the moral principle that allows deadly force in defense of the lives of innocent moral person against culpable attack.³ Since, according to Hill, fetuses are moral persons from the moment of conception and since murdering Britton was necessary to save the lives of fetuses he would culpably abort, he was justified in killing Britton in defense of others – just as he would be justified under that principle in killing someone who was trying to murder a newborn infant.⁴

Hill's violent act, however, cannot be justified under the moral principle allowing defense of others for an interesting reason. The fact that the issue of whether fetuses are moral persons from the moment of conception is so deeply contested in this society by intelligent persons of conscience shows that much more evidence and argument is needed to provide adequate reason to believe that fetuses have this special moral status from the moment of conception. Since Hill lacked morally adequate reason to believe that the principle allowing deadly force in defense of innocent persons applied to *fetuses*, he could not be justified under this principle in killing Britton and was rightly convicted of murder. As a general matter, a person who takes aggressive action against a person under a moral principle without adequate epistemic grounds for believing its application-conditions are satisfied commits a moral wrong against that person.

The same principle applies to cases far less extreme than the Hill case. For example, those persons who effectively shut down traffic on the Washington state bridge *deliberately* caused significant inconvenience to other persons after having their position rejected at the polls. Although their position might have been the correct one, their willingness to cause such inconvenience to others on the strength of a view that might, or might not, have been particularly well reasoned (protesters, after all, need not be philosophers) is problematic from a moral point of view for exactly the same reason that Hill's violent act is problematic. One must have adequate reason for believing that one's moral conviction is correct to be justified in imposing significant detriment on innocent third parties.⁵

The mental state of someone who deliberately imposes detriment on innocent third parties position on the strength of a moral conviction that lacks adequate epistemic

³ For Hill's tragically misguided views on the morality of killing abortion providers, see <http://www.armyofgod.com/PHillonepage.html>.

⁴ Indeed, this is a very consequence of the claim that a fetus is a moral person. If a fetus has a full and equal set of moral rights, then murdering a fetus violates the same right to life that murdering a newborn infant violates and is just as grave a moral offense. This is why the issue of fetal personhood is so crucial to the abortion debate.

⁵ Some of the motorists delayed by the protest surely voted against the initiative and shared the view of the protesters.

support is morally problematic in at least two possibly related ways. First, it evinces disregard for the interests of innocent third parties, a failure to appreciate the importance of other people. Second, it evinces an arrogant judgment about the importance and reliability of one's own judgments. It seems, at the very least, arrogant for one person to deliberately subject another to a risk of harm on the strength of an idea that lacks adequate support.⁶

One sign that a moral conviction lacks adequate epistemic support is that it is deeply contested among open-minded, reasonable persons of conscience in the culture. The idea that there are many open-minded reasonable persons of conscience on both sides of an issue suggests that both positions are reasonable in the sense that they are backed by good reasons that lack an adequate rebuttal. Insofar as a disagreement is reasonable in this sense, neither side can claim to have fully adequate support.

This helps to explain why Hill's act was morally wrong. Even on the assumption that Hill's view about fetal personhood is correct, the fact that so many reasonable persons of conscience – who otherwise agree on so much – disagree upon fetal personhood should have told Hill that there were limits on how far he could go in acting on his conviction. While he could legitimately protest abortion rights in a variety of ways, he could not legitimately act in ways that deliberately impose significant detriment on other persons.

This should not be construed as overlooking the possibility of a disagreement that continues because one side is unreasonable or not open to reasoned argument. It seems clear, for example, that persons who disagreed in the 1960s and 70s with the idea that race-based segregation is wrong lacked even minimal support for a position that had been all but conclusively refuted by that juncture. Sometimes there are a lot of unreasonable, narrow-minded persons who simply refuse to see the light.

In many instances, however, disagreement will be reasonable, calling into question whether persons on one side of an issue may legitimately impose morally significant costs on other persons for expressive purposes. In cases where a position is held by only a small minority of the people and dissenting views are reasonably held, the worry is greater. In such cases, it seems clear that, other things being equal, persons should refrain from deliberately imposing morally significant costs on innocent third parties as a means of protesting the majority view or calling attention to its injustice.

But even when a position is in play among reasonable persons, a person should be in cognitive possession of a reasonably thoughtful justification for the position before deliberately imposing detriment on third parties as a means of expressing support for that position (or opposition to the contrary position). Someone who deliberately impacts the morally significant interests of others to their detriment without anything that would count as a thoughtful justification might as well be acting on the basis of a coin-flip. It seems clear that we have an obligation not to deliberately harm morally significant

⁶ This primarily applies to individuals; the state is in a somewhat different position because, in many cases, it cannot avoid taking a position on a contested issue by refraining from acting. If it refrains from prohibiting abortion, for example, the absence of a prohibition presupposes (at least to the extent that we presume the state is trying to do what is morally legitimate) that abortion does not result in murder. If it prohibits abortion, the prohibition presupposes either that a woman does not have a privacy right in her body or that abortion results in murder. Citizens are rarely in such a position.

interests of innocent third parties unless we have some good reason for believing it is morally justified.

E. A Framework for Evaluating Acts of Civil Disobedience

The foregoing discussion suggests a useful framework for evaluating acts of civil disobedience. From the standpoint of morality, acts of civil disobedience have both pluses and minuses that have to be weighed. The moral value, for example, of a conscientious desire to call attention to injustice must be weighed against the moral disvalue of imposing costs on third parties.

Accordingly, the following considerations weigh in favor of finding that an act of civil disobedience against an otherwise legitimate state is justified (or excused) and should not be punished by the state. First, the act is committed openly by properly motivated persons willing to accept responsibility for the act. Second, the position is a plausible one that is, at the very least, in play among open-minded, reasonable persons in the relevant community. Third, persons committing an act of civil disobedience are in possession of a thoughtful justification for both the position and the act. Fourth, the act does not result in significant damage to the interests of innocent third parties. Fifth, the act is reasonably calculated to stimulate and advance debate on the issue.

In contrast, the following considerations weigh in favor of finding that an act of civil disobedience against an otherwise legitimate state is not excused and ought to be punished. First, the act is not properly motivated or committed openly by persons willing to accept responsibility. Second, the position is implausible and not in play among most thoughtful open-minded persons in the relevant community. Third, the people who have committed an act of civil disobedience lack a thoughtful justification for the position or the act. Fourth, the act results in significant harm to innocent third parties. Fifth, the act is not reasonably calculated to stimulate or advance debate on the issue.

Again, it is important to emphasize here that the context here is a legitimate democratic state with laws that are generally just. It is reasonable to think that the moral calculus in an illegitimate state is radically different insofar as citizens of such a state have a right to openly rebel. How exactly one distinguishes legitimate from illegitimate states is a matter of dispute among political philosophers and theorists; but I will assume that the readers of this paper live in states that are not illegitimate.

The civil-rights sit-ins of the 1960s are paradigmatic examples of justified acts of civil disobedience under the framework described above. Someone who refuses to leave segregated lunch counters until police arrive to remove her is clearly committing an open act of civil disobedience and is willing to accept the consequences of her behavior. The view that such segregation is wrong was not only in play among open-minded, reasonable persons of conscience, but had pretty much won the day by the time the mid-60s arrived. The people who committed these acts justified them by reference to a principle of equality that open-minded, reasonable persons of conscience in the culture had nearly universally accepted. Lunch-counter sit-ins had significant effects only on the owners who wrongly implemented policies of segregating blacks and whites. These sit-ins helped to call attention to the ongoing racial injustices in the southern U.S.

In contrast, acts of vandalism by anarchists during the 1999 WTO protests in Seattle were not justified acts of civil disobedience (assuming, of course, that these were acts of civil disobedience and hence motivated by the right sort of considerations) under this framework. Anarchists who broke windows and set fires typically fled the scene as soon as the police arrived. Anarchism – especially the confused version to which this class of protesters subscribe – is not in play among reasonable, open-minded persons in the community. If televised interviews with some of the anarchists were any indication, they generally lacked a thoughtful justification for their views; most of them I saw were strikingly inarticulate. The cost of replacing a large plate-glass storefront window is in excess of \$10,000 – a morally significant cost to innocent store owners. These acts of vandalism tend to alienate people and entrench them further in their opposition to anarchism, rather than provoke reasoned discussion.

These are, of course, fairly easy cases under the framework described above (or, for that matter, any plausible framework for evaluating acts of civil disobedience) because all of the relevant factors point in the same direction. All of the factors in the civil rights case weigh in favor of justification, while all of the factors in the anarchism case weigh against justification.

One should not think this will always be the case. One would expect that there will many instances of civil disobedience, electronic or otherwise, in which there are elements that weigh in favor of justification, as well as elements that weigh against justification. These cases will be quite difficult to evaluate under the framework above because there is no easy methodology for weighing the various factors against one another.

Sill, it is reasonable to think that a couple of these factors define necessary conditions for an act of civil disobedience to be justified. It seems clearly impermissible to deliberately impose morally significant costs on other people for purely expressive purposes – at least in democratic societies in which one’s point can openly be expressed in other ways without fear of reprisal; thus, it is a necessary condition for an act of civil disobedience to be justified in such societies that it not impose morally significant detriment on innocent third parties. In addition, willingness to accept responsibility seems to be a necessary condition for an act of civil disobedience to be justified. Anonymously claiming responsibility is not enough to assure the public that the breach of the peace is exceptional, a crucial factor in justifying civil disobedience; as noted above, even terrorists do this much.

II. What is Hacktivism?

To determine whether or not hacktivism might be excused or justified as civil disobedience, we need a sense for what is involved in hacktivism. Insofar as hacktivism is a form of hacking, the word “hacktivism” is related to the word “hacking.” The latter term, however, is a highly contentious term that means different things to different people. Consider, for example, the entry for “hacker” in the original Hacker’s Dictionary⁷:

⁷ <http://www.dourish.com/goodies/jargon.html>.

HACKER n. 1. A person who enjoys learning the details of programming systems and how to stretch their capabilities, as opposed to most users who prefer to learn only the minimum necessary. 2. One who programs enthusiastically, or who enjoys programming rather than just theorizing about programming. 3. A person capable of appreciating hack value (q.v.). 4. A person who is good at programming quickly. Not everything a hacker produces is a hack. 5. An expert at a particular program, or one who frequently does work using it or on it; example: "A SAIL hacker". (Definitions 1 to 5 are correlated, and people who fit them congregate.) 6. A malicious or inquisitive meddler who tries to discover information by poking around. Hence "password hacker", "network hacker".

While the first five clauses define “hacker” in terms of approbation, these usages are currently idiosyncratic at best. Definition 6 comes closest to expressing the current use of the term “hacker” now irrevocably associated with computer crime. A “hacker,” on this usage, is a (1) malicious or inquisitive (2) meddler who (3) pokes around to (4) discover information. Although many persons in the computer industry continue to use the term “hacker” to pick out programmers of distinction, the term “hacker” is now used by most persons only to pick out persons who intrude upon systems and machines belonging to other people without any meaningful authorization (whether through the consent of the owners or through the legal process). Anyone who trespasses upon someone else’s system or network qualifies under this definition as a “hacker” according to this common usage. This is the definition that will be presupposed in this paper.

At the most general level, “hacktivism” is reasonably defined as “politically-motivated hacking” (Manion and Goodrum, 2000) or as “hacking that is performed as political activism.” Since hacking, as a conceptual matter, involves the commission of an unauthorized digital intrusion, “hacktivism” is more precisely defined as “the commission of an unauthorized digital intrusion for the purpose of expressing a political position or for the purpose of achieving a political agenda.” As a species of digital act, hacktivism does not involve the use of physical force (at least, as traditionally understood) and hence is non-violent in nature. As a species of activism, hacktivism does not seek to achieve its political purposes, unlike terrorism, by inspiring general fear or terror among the population; it attempts to achieve these purposes by stimulating reasoned discussion and debate. Hacktivism is thus conceptually distinct from cyberterrorism – though the boundaries, as we will see, sometimes seem to overlap in practice.

What distinguishes hacktivism from ordinary hacking (as opposed to “cracking”) is the motivation. While the motivation of hackers (as opposed to crackers) is benign, a benign motivation does not necessarily involve one that is expressive of a political or moral view. Simple curiosity, for example, is benign, but not expressive of a political or moral view. Nor is a benign motivation necessarily a praiseworthy one. Simple curiosity is always benign but not necessarily morally laudable; indeed, there are many things about which it is probably not good, from a moral point of view, to be curious (e.g., what it feels like to kill someone). In contrast, the motivation of the hacktivist is both expressive and praiseworthy: the motivation is to bring about some greater moral good by calling attention to injustice for the purpose of eliminating it. Accordingly, for purposes of this

paper, the term “hacktivism” will be understood as involving unauthorized digital intrusions for the purpose of protesting some injustice or advancing some political agenda.

There will be forms of digital activism that do not, strictly speaking, count as hacktivism. Posting a website in the U.S. with a petition protesting the Iraqi war would be a form of digital activism, on this definition, but would not count as an act of hacktivism because it does not involve an unauthorized digital intrusion. Nor, for that matter, would such an act count as act of electronic civil disobedience because the posting of such content online breaks no laws; electronic civil disobedience, as a conceptual matter, is a form of civil disobedience and hence requires the violation of a valid law.

In contrast, the following acts would all count, on this analysis, as acts of hacktivism: (1) a DoS attack launched against the WTO website to protest economic globalization and WTO policies⁸; (2) the altering of the content of a government website to express outrage over some policy of that government⁹; and (3) the unauthorized redirection of traffic intended for a KKK website to Hatewatch.¹⁰ Each of these acts would involve some unauthorized digital intrusion and hence would, since presumably intended as a piece of political activism, count as hacktivism.

III. Is Hacktivism Justified as Civil Disobedience?

The issue of whether hacktivism is justified civil disobedience must be addressed on a case-by-case basis because acts of hacktivism vary with respect to morally relevant characteristics. Some hacktivists, for example, make no attempt to conceal their identity and evince a willingness to accept responsibility for their acts, while others conceal their identities in order to evade detection. Some acts involve no significant damage to innocent third parties (e.g., defacing a governmental website to protest its policies), while others do (e.g., shutting down commercial websites with DDoS attacks). Open acts of hacktivism that do not impact innocent third parties have a different moral quality than clandestine acts that harm innocent third parties.

In addition, there are a variety of positions that motivate hacktivism. Many acts of hacktivism are motivated to advance the cause of universal human rights and intrude against governmental entities believed to be violating those rights. Others are motivated by a desire to protest the increasing commercialization of the Internet and commodification of information. Some of these positions are more plausible and better supported than others; acts of hacktivism motivated by well-supported plausible positions are, other things being equal, morally preferable to acts not motivated by well-supported plausible positions.

⁸ In 1999, the Electrohippies attacked a WTO website for such reasons. For a summary of notable hacker attacks, see “Timeline of hacker history,” *Wikipedia*; available at http://en.wikipedia.org/wiki/Infamous_Hacks,

⁹ In 1996, hackers changed the content of the Department of Justice website, replacing “Justice” with “Injustice.”

¹⁰ Anonymous hackers did exactly this in 1999. Intriguingly, a Hatewatch press release characterized the act as “vandalism.” See HateWatch Press Release: Activism vs. Hacktivism, September 4, 1999; available at <http://archives.openflows.org/hacktivism/hacktivism01048.html>.

A comprehensive survey of hacktivist acts is not possible here. In what follows, I consider some of the factors relevant to the evaluation of hacktivism under the framework described above and illustrate them with a couple of examples. For this reason, the discussion below makes no claim to being complete or even comprehensive in scope.

A. How Much Harm is Caused?

One of the key issues in evaluating whether an act of hacktivism is morally justified is the extent to which the act harms the interests of innocent third parties. In thinking about this issue, it is important to reiterate that the context being assumed here is a morally legitimate democratic system that protects the right of free speech and thus affords persons a variety of avenues for expressing their views that do not impact the interests of innocent third parties.

As the amount of harm varies from case to case and thus must be determined by empirical means, I will briefly discuss some general issues that will commonly arise in connection with evaluating the amount of harm.

1. Public, Private, Commercial, Non-Commercial Entities

How much harm is caused will frequently depend on whether the target of the hack is a public, private, commercial, or non-commercial entity. Attacks on public non-commercial, purely informative websites, for example, tend to cause less damage than attacks on private, commercial websites. The reason for this is that attacks on commercial websites can result in significant business losses ultimately passed on to consumers in the form of higher prices (reflecting a higher cost of doing business) or to employees in the form of layoffs. If the information on a public website is non-essential information (i.e., unrelated to vital interests), an attack on that website is not likely to result in anything more serious than inconvenience to citizens who are not able to access that information.¹¹

This should not be taken to suggest that hacktivist intrusions upon public entities *cannot* result in significant harm to third parties. One can conceive of a depressingly large variety of acts that might very well cause significant damage to innocent third parties. A digital attack on a public hospital server might very well result in deaths. Of course, these more serious acts are probably not motivated by expressive purposes (and, I would argue, should be characterized as “violent acts”¹²) and, if so, would not count either as civil disobedience or as hacktivism as these notions are defined here.

Acts of hacktivism directed at private individuals can also have morally significant effects. A DoS attack, for example, that effectively denies access to a citizen’s website can impact her moral rights. A DoS attack on a citizen site impacts her ability to express

¹¹ The Electrohippies justify attacks on various public websites precisely on such grounds: “Neither the Whitehouse nor 10 Downing Street web site are [sic] essential services. For the most part they merely distribute the fallacious justifications in Iraq, as well as trying to promote the image of the two prime movers behind war in Iraq: Messrs. Bush and Blair (Electrohippies, 2003).” The idea here is that the harm caused by attacks that ultimately deny access to public websites not providing essential services result in no significant harm to innocent third-parties.

¹² See footnote 2, *supra*.

her views and hence infringes her moral right to free speech (as opposed to her legal right to speech, which is typically against only governmental entities). An attempt to gain access to files on a citizen's computer impacts her rights to privacy, as well as her property rights in her computer.

2. *The Character of the Hack*

How much harm is done also depends not only on the character of the victim, but also on the nature of the attack.¹³ In the area of physical attacks, this is, of course, obvious. Throwing a Molotov cocktail into an open window is, other things being equal, likely to cause significantly more harm than tagging the building with some sort of graffiti. The more forceful the attack, the more harm is likely to result.

It should be emphasized that this is not necessarily true. Someone might throw a Molotov cocktail into a building that is slated for destruction and save the owner the costs of tearing it down, while the owner of a property being tagged might have a heart attack as a result of the distress caused by someone vandalizing her property. Accordingly, an accurate determination of how much damage any particular attack, physical or digital, requires an empirical analysis that looks to the specific circumstances of the attack.

Still, as a general matter, some digital attacks are less likely to cause harm than others. Defacement of a website – or “E-graffiti” as sympathetic theorists sometimes call it – seems far less likely to cause significant harm than attacks that have the effect of denying access to the contents of a website. Changing “Department of Justice” on a government website, for example, to “Department of Injustice” is not likely to result in significant harm to third-party interests. At most, it will cause embarrassment to the government agency running the site and perhaps some minor loss of confidence among citizens in the accuracy of the site's contents.

This should not, however, be taken to suggest that defacement of a website can never result in significant damage to innocent third-parties. Publishing sensitive information about individuals, like social security numbers, as “E-graffiti” on a government website could obviously result in significant damage to those individuals. As is true of physical graffiti, one must look to the specific circumstances to evaluate the damage caused by digital graffiti to ensure an accurate assessment.

Nevertheless, it is reasonable to think that, as a general matter, denial of service (DoS) and distributed denial of service (DDoS) attacks are calculated to cause more damage, other things being equal, than defacement of websites. These attacks are calculated to deny access of third-parties to the content of a website, effectively shutting it down by overwhelming the server with sham requests for information. While there are undoubtedly exceptions to any generalizations about the comparative harm caused by defacement of websites and denial of service attacks, it seems reasonable to think that shutting down a website is a more harmful act than merely defacing it. For this reason, denial of service attacks will be harder to justify, as a general matter, as permissible electronic civil disobedience than defacement.

¹³ For a helpful discussion of various tactics, see Auty (2004). My discussion in this and the last section owes an obvious debt to Auty's discussion.

But, again, the amount of harm caused to innocent parties will depend on a host of circumstances, including the character of the website being shut down. Other things being equal, DoS and DDoS attacks on commercial websites are likely to result in greater harm than such attacks on non-commercial public websites providing non-essential services or information. Still, as a general matter, these attacks should be regarded as one of the more aggressive tools currently employed by hacktivists and hence as more problematic, from the standpoint of morality, than other tools.

It is true, of course, that most civil disobedience has effects on third-parties, but digital civil disobedience can potentially do much more damage to the interests of far more people than ordinary non-digital civil disobedience. Though it could have been worse, the effect of the protest in Washington was that many persons might have been late to work – losses that are easily made up. An attack that shuts down a busy commercial website for a few hours can easily affect hundreds of thousands of people. If the website's activity is vital to its profit-margin, this can translate into morally significant losses of revenue, which will usually be shifted to employees and consumers.

Indeed, a coordinated and sustained attack on the largest commercial websites, which can be carried out by a fairly small group of highly-skilled hackers, could result in the sort of economic downturn that affects millions of people. According to experts on terrorism, al Qaeda is exploring the possibility of large-scale cyberattacks on public and commercial networks precisely because a large enough attack might suffice to weaken confidence in E-commerce to such an extent as to precipitate a recession – or worse. Here it is worth noting that an increase of the unemployment rate in the U.S. from 5 to 6% means the loss of approximately one and a half million jobs (according to the U.S. Government, there were 147 million people in the labor force in 2004).

As is readily evident, electronic civil disobedience can have a greater impact on the interests of the targeted entity and third parties than ordinary civil disobedience. This, of course, is part of what makes digital trespass appealing to politically-minded hackers and explains why electronic civil disobedience raises more serious moral concerns than ordinary civil disobedience.

B. Are Hacktivists Prepared to Accept Responsibility?

One important factor contributing to justify an act of civil disobedience is that the persons committing the act are willing to accept responsibility for those acts. Manion and Goodrum (2000), for example, assert that “[w]illingness [of participants] to accept personal responsibility for outcome of actions” is a necessary, though not sufficient, condition for the justification of an act of civil disobedience: “In order for hacking to qualify as an act of civil disobedience, hackers must be clearly motivated by ethical concerns, be non-violent, and be ready to accept the repercussions of their actions” (15).

Nevertheless, there is a distinction between claiming responsibility for an act and being willing to accept the legal consequences of that act. One can claim responsibility without coming forward to accept the legal consequences of one's act. One could do this, I suppose, by giving one's real name and then attempting to conceal one's location to avoid facing those consequences. Or, more likely, one can do this by giving some sort of pseudonym instead of one's real name or by attributing the act to a particular group to which one belongs that protects the names of its members. While such a claim of

responsibility helps to signal an ethical motivation, this is not tantamount to be willing to accept responsibility.

The heroic civil-rights activists of the 60s who staged sit-ins went beyond merely claiming responsibility; they accepted, even invited, prosecution. It was part of their strategy to call attention to the injustice of Jim Crow laws in the South by voluntarily subjecting themselves to prosecution under those very laws. These courageous activists did not anonymously claim responsibility for the sit-ins from a safe distance: they would continue the protests until the police arrived to arrest them.

Some noteworthy hacktivists evince a similar willingness to accept responsibility for their actions. As Manion and Goodrum (2000) observe:

Examined in this light, the hack by Eugene Kashpureff clearly constitutes an act of civil disobedience. Kashpureff usurped traffic from InterNIC to protest domain name policy. He did this non-anonymously and went to jail as a result (15).

But this seems to be the exception and not the rule. There are a variety of hacktivist groups, including Electrohippies, MilwOrm, and Electronic Disturbance Theatre, but these groups typically claim responsibility for acts *as a group* without disclosing the identities of any members to avoid prosecution. For example, MilwOrm and another group claimed responsibility for the defacement of approximately 300 websites (they replaced the existing content with a statement against nuclear weapons and a photograph of a mushroom cloud), but did not disclose the identities of members who belong to the group. As far as I can tell, persons committing acts of hacktivism typically attempt to conceal their identities to avoid detection and exposure to prosecution – even when claiming responsibility.

Anonymous hacktivist attacks impose significant costs on social well-being. First, such attacks, regardless of motivation, contribute to an increasing sense of anxiety among the population about the security of the Internet, which has become increasingly vital to economic and other important interests. Second, these attacks require an expenditure of valuable resources, which could be allocated in more productive ways, to protecting computers against intrusions – costs that are passed on to consumers.

In any event, it is worth noting that terrorists typically claim responsibility as a group but attempt to evade the consequences of their actions by concealing their identities and locations. It is important, of course, not to make too much of this similarity: terrorists commit deliberately attempt to cause grievous harm to innocent people while hacktivists do not. The point, however, is merely to illustrate that there is morally significant difference between claiming responsibility and accepting responsibility. Accepting responsibility is, other things being equal, needed to justify an act of hacktivism.

C. Is the Political Agenda Plausible and Supported by Adequate Reasons?

The motivating agenda behind electronic civil disobedience, other things being equal, is not as transparently evident as the motivating agenda behind ordinary civil disobedience. Whereas the protesters who shut down the Washington state highway carried signs and alerted the press they were protesting a specific measure, the point of many putative acts of hacktivism is not clear. A distributed denial of service (DDoS) attack, for example,

directed against Amazon.com could mean any number of things – some of which have nothing to do with expressing a political view (e.g., a recently discharged employee might be taking revenge for her dismissal). The absence of any clear message is surely problematic from a moral standpoint.

In any event, I will consider in this section what I take to be the two most common motivating agendas behind hacktivist acts to illustrate the above framework for evaluating acts of civil disobedience.

1. Hacktivism in Support of Human Rights

Acts of hacktivism are frequently motivated by a desire to protest the suppression and violation of human rights by oppressive non-democratic regimes and are directed at servers maintained and owned by governmental entities in those regimes. Chinese governmental websites, for example, have been hacked to protest the oppression of both Chinese and Indonesian citizens.

There are a number of things worth noting about digital intrusions directed at oppressive governments that are motivated by a desire to protest violations of human rights, like torture of political dissidents. The first is that the primary impact of such acts is on the parties culpable for committing violations of human rights. Defacing a governmental website that does not provide essential services or information, for example, is not likely to have any significant effects on innocent citizens.

The second is the regimes that are being targeted do not recognize or respect a right of free speech. These regimes forcefully repress political dissent, usually with the threat of incarceration or worse. It is reasonable to think that the moral calculus of civil disobedience is considerably different in states that systematically deny citizens the opportunity to express dissent without fear of reprisal.

The third is that such acts of civil disobedience are frequently successful in calling attention to the injustice and stimulating debate. While a digital defacement of a governmental website is easily addressed by the affected governmental entities, it is likely to receive worldwide attention from the press. Given the peaceful character of the act, it is more likely to inform citizens of the world and provoke thought and discussion than to alienate them.

The fourth is that the position is probably a majority position among people in this culture and worldwide. It is fairly clear that, in Western cultures, support for universal human rights is, far and away, a majority position. But it is also reasonable to think that such support is also a majority position in non-Western cultures. In nations where citizens are denied human rights, those citizens frequently demand them. When liberated from oppressive regimes, moreover, citizens tend to behave in ways that were suppressed under those regimes. Women, for example, in Afghanistan adopted a Western style of dress and rejected the oppressive burqa after the Taliban was removed from power. People almost universally want speech rights, equality, and a right to be free from torture or political persecution,

While theorists may disagree on some particulars, the philosophical literature in support of universal human rights is much more prevalent than the literature against it. One of the few objections to the idea that there are universal human rights is grounded in the

normative ethical relativist position that there are no objective moral truths. There are two problems with this line of objection. First, it ignores the fact that people almost universally demand human rights. If we assume, quite reasonably, that reasonably conscientious people would not *demand* something unless they believed themselves morally entitled to it, then we have reason to believe that people are universally entitled to human rights on the assumption that normative ethical relativism is true. Second, normative ethical relativism is vulnerable to a host of external and internal criticisms (e.g., that the supposition that there are no objective moral truths is self-contradictory because such a supposition must be construed as an objective moral truth to be normatively relevant) and remains a minority position.¹⁴

2. *Hactivism in Support of the “Hacker Ethic”*

Unlike the human-rights agenda, other positions that commonly motivate hacktivism are fairly characterized as fringe positions not generally in play among thoughtful, open-minded members of the community. Consider, for example, the main tenets of the “hacker ethic” as summarized by Levy (1984):

1. Access to computers should be unlimited and total.
2. All information should be free.
3. Mistrust authority – promote decentralization.
4. Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.
5. You create art and beauty on a computer.
6. Computers can change your life for the better.

While tenets 4 through 6 are largely uncontroversial (and so obvious they do not need to be stated), these are not the tenets that motivate acts of hacktivism. The tenets that are most likely to motivate acts of hacktivism are the first three tenets.

It is hard to know what to say about tenet 3, as it is not entirely clear what it means, beyond pointing out that it is overly general (Should all doctors be mistrusted? Always?); however, tenets 1 and 2 are clearly fringe positions that are not really in play among open-minded, thoughtful people. Tenet 1 implies that people have no property rights in their own computers and hence may not permissibly exclude others from their machines – an implausible position that, consistently applied to other forms of property, would vitiate ownership in homes and automobiles. Tenet 2 implies that people have no privacy rights in highly intimate information about themselves. While many people are rightly rethinking their positions about information ethics in response to the new technologies, tenets 1 and 2 are simply too strong to be plausible because inconsistent with bedrock

¹⁴ It is worth noting that relativists rarely argue for their moral positions the way one would expect of relativists. I have seen a fair number of relativists argue for a moral position without any reference to what people believe or accept in the relevant culture; this is not surprising in many of these cases because they argue for positions that would be rejected by the vast majority of people in the relevant culture. I have seen a number of them state something like “we must, of course, avoid the mistake of assuming that there are objective moral truths” and then go on to commit that very mistake by arguing for a minority position without any attempt to evaluate existing social practices or conventions.

views about privacy and property rights. For this reason, neither is in play among open-minded, reasonable persons in the community.

One might reasonably think that these extreme positions are not exactly what hacktivists have in mind, but these are the positions that emerge most clearly from what is being said by and on behalf of politically-minded hackers who commit acts of civil disobedience. Universal quantifiers, for example, are most naturally interpreted as, well, performing the function of universal quantifiers. “All information should be free” is naturally interpreted as meaning that all information should be free.

In any event, if these positions are not what hacktivists have in mind, then they need to make themselves clearer – and this is something that they are obligated to do before they undertake to commit acts of digital civil disobedience. It seems clear that, as a moral matter, one should know exactly what position one is attempting to further before one deliberately attempts to compromise networks and systems that belong to other people so as to cause inconvenience and damage to those persons.

D. Are Hacktivists in Cognitive Possession of a Plausible Justification for the Positions Motivating Their Acts?

It is not enough, according to the framework described above, that an act of hacktivism is motivated by a plausible position in play among thoughtful, reasonably conscientious persons; it is a necessary condition for an act of hacktivism to be justified that the actor be in cognitive possession of a reasonably plausible justification for that position.

As a general matter, there is little reason to think that the hacktivists themselves are in possession of a reasoned justification that would support the positions they take. It is reasonable to hypothesize that hacktivists are much better at solving the technological problems associated with committing digital intrusions than they are at articulating and defending the positions that motivate them. Occasionally, they will articulate their position with some sort of slogan, but rarely provide the position with the critical support it needs. Consider, for example, Manion’s and Goodrum’s (2000) discussion of one such motivation:

In order to determine the motivations of hacktivists, one place to look is what hacktivists *themselves* say is their motivation.... In June of 1998 the hacktivists group “MilwOrm” hacked India’s Bhabha Atomic Research Centre to protest against recent nuclear tests. Later, in July of that year, “MilwOrm” and the group “Astray Lumberjacks,” orchestrated an unprecedented mass hack of more than 300 sites around the world, replacing web pages with an anti-nuclear statements[sic] and images of mushroom clouds. Not surprisingly, the published slogan of MilwOrm is: “Putting the power back in the hands of people” (Manion and Goodrum, 2000, 16).

Again, one should say much more by way of justification for hacking 300 sites than just a vague slogan like “Putting the power back in the hands of people.” The victims of such an attack, as well as the public whose peace has been breached, have a right to know exactly what position is motivating the attack and why anyone should think it is a plausible position.

The willingness to impose morally significant costs on other people to advance fringe positions that are neither clearly articulated nor backed with some sort of plausible justification is clearly problematic from a moral point of view. It seems clear that such behavior involves, at least in most cases, a fairly serious form of arrogance – a mental state that is problematic according to ordinary intuitions about morality. Indeed, it is exactly the sort of arrogance hacktivists would attribute to their intended victims.

The foregoing argument should not, of course, be construed to condemn all acts of hacktivism. Nothing in the foregoing argument would justify a condemnation of narrowly targeted acts of electronic civil disobedience properly motivated and justified by a well-articulated plausible position that do not result in significant harm to innocent third-parties. Acts of hacktivism that have these properties might very well be justified by the right to free speech – though, again, it bears emphasizing here that such acts will be much harder to justify in societies with morally legitimate legal systems.

The problem, however, is that the most common (or at least the most widely reported) acts of digital civil disobedience are justifiably condemned by the foregoing arguments. Hacktivists simply have not done the kinds of things they ought to have done to make sure their acts are unproblematic from a moral standpoint. In their zealousness to advance their moral causes, they have committed acts that are far more obviously problematic from a moral point of view than the positions they seek to attack. If, as Manion and Goodrum (2000) suggest, hacktivists have been misunderstood by mainstream media and theorists, they have only themselves to blame.

IV. Should Unjustified Hacktivism be Punished?

As noted above, the issue of whether civil disobedience should be punished by the state is different from the issue of whether civil disobedience is morally justified. While it would presumably be wrong for the state to punish a morally justified act of civil disobedience, it is not as clear whether the state should punish *un*justified acts of civil disobedience. Not every morally unjustified act should be punished by the state; ordinary lying, for example, should not be criminalized.

The issue of whether unjustified hacktivist acts should be punished by the state must be determined on a case-by-case basis. Whatever values might be served by punishing such acts must be weighed against the costs associated with punishment. Punishing an offender can be expensive and not really worth the costs if the act is comparatively innocuous and the offender's mental states are sufficiently blameless.

Even so, it is reasonable to think that the costs will sometimes be worth incurring. In cases where an unjustified act of hacktivism results in significant financial losses to individuals, offenders should be punished – at least where those losses are reasonably foreseeable. To begin, punishment in such cases seems pretty clearly deserved. It is simply wrong for an individual to take it upon herself to deliberately perform an act that is calculated to cause significant harm to others for expressive purposes. Further, culpable offenders stand in need of some rehabilitation (though our penal system is admittedly not particularly well-equipped to perform this legitimating feature of punishment). Finally, society has an interest in preventing and deterring morally unjustified behavior, but has an especially strong interest in preventing and deterring unjustified behavior reasonably calculated to cause significant harm to others.

Moreover, acts of electronic civil disobedience committed anonymously should be punished to the full extent under the law. Again, it is not enough to claim responsibility as a group; even terrorist organizations like al Qaeda do this much. The willingness of responsible individuals to come forward and accept the legal consequences of their behaviors helps to distinguish their acts from the acts of cyberterrorists; as such, their acts should be treated differently from the acts of cyberterrorists. For this reason, willingness to accept responsibility should be treated as a mitigating factor. In cases where no significant harm results from the act, willingness to accept responsibility might even be enough to warrant a dismissal of criminal charges.

In this connection, it is important to note that the boundaries between activism and terrorism are becoming increasingly blurred. Organizations such as the Earth Liberation Front and the Animal Liberation Front have adopted a particularly aggressive form of what they characterize as “activism.” Targeting property, rather than people, these organizations have bombed animal research facilities in an attempt to induce the victims’ to adopt more environmentally- and animal-friendly policies and practices. The tactics of such organizations resemble the tactics of terrorists in that they frequently involve physical force, but are distinct in that they have attempted up to now to avoid human casualties.¹⁵ These organizations, like terrorist organizations, will claim responsibility but never step forward to accept the legal consequences of their acts.

The effect of these and like-minded organizations have been to blur the distinction between activism and terrorism in the minds of the public who increasingly view such anonymous acts as posing a serious threat to the public peace. For this reason, it is especially important that a legitimate legal system provide (1) an incentive for hacktivists to do more than just anonymously claim responsibility for their actions and (2) a significant deterrent to anonymous cyberattacks of any kind, no matter how well motivated they might be. Punishment of anonymous attacks to the full extent of the law is at least a step towards providing appropriate incentives and disincentives.

References

- Auty, Caroline, (2004). Political hacktivism: tool of the underdog or scourge of cyberspace? *ASLIB Proceedings: New Information Perspectives*,. 56, 212-221.
- Himma, Kenneth Einar and Dittrich, David (forthcoming 2006). Hackers, crackers, and computer criminals. *The Handbook of Information Security*. Wiley.
- Jordan, Tim and Taylor, Paul A. (2004). *Hacktivism and cyberwars: rebels without a cause?* London: Routledge.
- Levy, Stephen (1984). *Hackers: computer heroes of the computer revolution*. New York: Delta Trade Paperbacks.

¹⁵ They typically deny that such acts constitute violence on the ground that “violence” involves force directed at people, not property. As is evident, the terms “force” and “violence” are becoming increasingly contentious.

Manion, Mark, and Goodrum, Abby (2000). Terrorism or civil disobedience: toward a hacktivist ethic. *Computers and Society*, June. 14-19.

Spafford, Eugene (1992). Are computer hacker break-ins ethical? *Journal of Systems Software* 17