Chapter 5

Hacktivism and the Future of Democratic Discourse

Introduction

Can the Internet serve as a new public sphere, a home to democratic discourse? This question frames much of the contemporary research on the prospects for electronic democracy.[55] It captures the widespread hope that online communications can help correct some of the recent injuries to democratic vitality, attributed variously to factors like television(Putnam 2000), excessive emphasis on scientific expertise (Fischer 2001), and the rise in “lifestyle politics” (Bennett 1998).

These aspirations are premised on our ability to create a virtual version of democratic deliberation. That deliberation is sometimes described in terms of a democratic agora, a town hall, a public sphere, or a commons. All of these models share a vision of deliberation in which diverse citizens congregate in order to exchange ideas, discuss issues and perhaps arrive at decisions.

Hacktivism raises a number of challenges for visions of online civic deliberation. In the broadest terms, it draws our attention to the fact that the Internet’s political impact may not be neatly contained by tidily structured participatory opportunities. But it also raises more particular challenges to a number of the specific issues surrounding deliberative democracy.

[55] See for example, (Dahlberg 2001), (Wilhelm 2000),(Malina 1999).

This chapter will examine two of these challenges: the challenges to deliberative concepts of free speech and accountability. Each of these concepts is to some degree contested, with different deliberative theorists arguing for different formulations. Yet hacktivism challenges the very terms of debate on each issue, encouraging us to reformulate each concept for the purposes of envisioning online deliberation.

Before approaching each of these challenges in turn, I begin with a brief discussion of the notion of online deliberation as others have formulated it. I then use my taxonomy of hacktivism to address each of these problems, demonstrating how the divisions among hacktivists translate into larger problems for conceptualizations of online deliberative discourse. I conclude by suggesting that the problems raised by hacktivism are symptomatic of larger phenomena in the online world, demanding a more fundamental review of our vision for online deliberative discourse.

Envisioning digital deliberation

Much of the debate over the Internet's potential as a home for democratic discourse has been framed by the theories of Jürgen Habermas. Habermas's account of the deterioration of democratic discourse is closely linked to the expansion and deterioration of the public sphere, due in part to the evolution of mass media (Chambers 2000). As a new type of media, the Internet thus presents fresh possibilities for the re-invigoration of that public sphere:

> The age of the public sphere as face-to-face talk is clearly over: the question of democracy must henceforth take into account new forms of electronically mediated discourse. What are the conditions of democratic speech in the mode of information? What kind of "subject" speaks or writes or communicates in these conditions? (Poster 1995)

The Internet's potential for realizing Habermas's vision of deliberative democracy lies in its sheer communicative capacity. As Froomkin frames it, "the Internet draws power back into the public sphere, away from other systems…Could it be that emerging technologies will enable new types of Internet-based discourses that generate the "communicative power" Habermas argues is needed to educate and mobilize citizens to demand that their governments make better and more legitimate decisions?" (Froomkin 2004) Similarly, Thornton argues that

> the Internet does allow people who are taking part to share a basis of understanding as common ground from which to mediate consensus. The Internet allows people to contribute to modifying systems (in the Habermasian sense), using communicative action (Thornton 2002, citing Lamber 1995.)

These authors draw attention to the parallels between the conditions for democratic discourse outlined by Habermas, and the potential conditions of online deliberation. Habermas's vision for deliberative democracy is fundamentally communicative, resting on a notion of deliberation as a perpetual conversation among citizens. The purpose of this conversation is "to generate a 'rationally motivated consensus' on controversial claims."(Benhabib 1986) Habermas specifies the conditions of the "ideal speech situation" necessary to enable this kind of conversation:

> 1. Participation in such deliberation is governed by the norms of equality and symmetry; all have the same chance to initiate speech acts, to question, interrogate, and to open debate;
> 2. All have the right to question the assigned topics of conversation;
> 3. All have the right to initiate reflexive arguments about the very rules of the discourse procedure and the way in which they are applied or carried out. There are no prima facie rules limiting the agenda or the conversation, nor the identity of the participants, as long as each excluded person or group can justifiably show that they are relevantly affected by the proposed norm under question (Mouffe 1999, citing Benhabib 1996.)

Dahlberg discerns the characteristics of the ideal situation in his study of Minnesota E-Democracy, a prominent example of online citizen-to-citizen political debate. Dahlberg describes Minnesota E-Democracy as a successful example of structuring online dialogue “to stimulate reflexivity, foster respectful listening and participant commitment to ongoing dialogue, achieve open and honest exchange, provide equal opportunity for all voices to be heard, and maximize autonomy from state and corporate interests.”(Dahlberg 2001)

Despite the theoretical congruity between Habermas’s ideal speech situation, and some of the apparent characteristics of online dialogue, there are concerns about whether theory can translate into practice. Dahlberg himself qualifies the longer-term prospects of Minnesota E-Democracy, which he believes “may largely be following the course of what Habermas described as the bourgeois public sphere, a narrowly defined rational-critical public increasingly marginalized by the commercialization of the medium and by more populist forms of political participation.”(Dahlberg 2001) Streck raises similar concerns about the WELL, a widely-praised online community that he describes as “a computer-based instance of Jürgen Habermas's bourgeois public sphere, in which the educated and affluent come together outside both home and state for critical discussion of art, literature and politics (Streck 1998).

While Habermas thus provides some useful frameworks for considering the challenge of online deliberation, his work is by no means the solution to questions about how the Internet could house democratic deliberation. Perhaps for that reason, some authors have attempted to go beyond Habermasian models, or to use Habermas’s work more loosely in their examinations of online discourse. Hale et al. are among those who draw on Barber's notion of "strong democracy" to consider possibilities for "more thoughtful, civic-minded and deliberative patterns of communication."(Hale, Musso, and Weare 1999) Coleman and Gøtze frame their examination of policy deliberation with Dewey's vision of "improvement of the methods and conditions of debate, discussion, and persuasion". (Coleman and Gøtze 2001) Witschge (Witschge 2004) synthesizes a range of deliberation theorists (including Dryzek, Bohman, and Cohen) in order to formulate the requirements for online deliberation as "equality in participation, discursive equality, and following from this, diversity of viewpoints and arguments."(Witschge 2004)

Both the Habermasian and non-Habermasian variants share some common preoccupations, however. Each assumes that some sort of free speech principle must be in operation – although the boundaries of legitimate speech may be conceived differently. Each also addresses the problem of anonymity, although there are significant differences as to whether it is seen as constructive or destructive to democratic discourse. The taxonomy of hacktivism introduced earlier (see Chapter 2) helps us understand the internal hacktivist divisions on key questions of free speech and accountability. Both issues are hotly debated in the hacktivist community – as well as among deliberative democrats.

The problem of free speech

Free speech is essential to any model of democratic discourse. Cohen (1998) usefully summarizes the arguments that have been made for the importance of freedom of political expression in a democracy:

1. Democracy is based on the principle of popular sovereignty, which demands "free and open discussion among citizens";
2. Restricting speech creates political inequality between those whose speech is allowed, and those whose speech is restricted;
3. Restricting speech impedes the free flow of information, "perhaps reducing the quality of democratic discussion and decision", and
4. Restricting speech limits the range of ideas or opinions in a political discussion. (Cohen 1998)

As Cohen himself points out, freedom of speech is even more crucial to deliberative democracy. For this reason protection must extend beyond specifically political speech to encompass the full range of "conscientious expression" (Cohen 1998) Some even argue that the very purpose of free speech is "to ensure that it is possible for people to engage in the discussion and deliberation necessary for the successful use of democratic institutions." (Nickel 2000)

But the Internet may make protecting free speech more difficult and more complicated, as the case of hacktivism suggests. Many forms of hacktivism – most notably web site defacements and virtual sit-ins – involve jamming or altering someone else's speech. Web site defacements replace one online message with another. Virtual sit-ins temporarily silence (or muffle) a message as a way of drawing attention to another. Are these actions forms of free speech, or a rebuke to it?

Political coders argue that freedom of speech is absolute, and that any form of hacktivism that interferes with the publishing rights of its target – such as defacements or virtual sit-ins – is thus illegitimate. They argue that freedom of speech is what hacktivism is all about:

> I think hacktivism should be about delivering a message, just like good old grass roots activism. It shouldn't be about doing damage to someone else network, or taking away their right to express their views. We just want to make a fuss so people will pay attention to what the message is we wish to deliver."(27-Aug-99)

Or as Hacktivismo leader Oxblood Ruffin puts it, "don't try to deny anyone the right of speech or the right of publishing" (Ruffin 2002).

This reflects the view, widespread among political coders as well as many other members of the hacker scene, that online freedoms – especially freedom of speech – are core values of Internet culture. Said one coder: "The internet is a free society. No content has ever been successfully banned from the internet." (Eisley 2003) His view is echoed by the comment of a coder who writes that "[f]reedom on the Internet, probably the only medium where censorship and monitoring can be circumvented, is very important." (Prasad 2002) Among the political coders I interviewed, only one took exception to the orthodox position on freedom of speech, saying that "I didn't want to take part in this debate [over code as speech] because the meaning of 'free speech' has a very different (and perverted, in my opinion) meaning in the U.S.A than in European countries." (Hocevar 2003)

The hacker culture's emphasis on freedom of speech leads political coders to put much of their energies into protecting freedom of speech online. The Hacktivismo/Peekabooty projects focus on extending online free speech protections to jurisdictions that have limited speech rights. The DeCSS projects, too, represent a commitment to free speech rights for code – consistent with coders' view of software as a form of speech. "I believe that code does have consciousness," says Oxblood Ruffin. "Cindy Cohn [a lawyer for the Electronic Frontier Foundation, and a Hacktivismo advisor] has established that code is speech." (Ruffin 2002)

The view that software code is protected speech has spurred much of the activity of DeCSS activists. Dave Touretzky, the founder of the Gallery of CSS Descramblers, wrote that "I was determined to show these movie industry types that it was a BAD IDEA to try to use trade secret law to interfere with free speech." (Touretzky 2003a) He is echoed by the coder who wrote that "It's also important to get every computer professional to understand that this [DeCSS] is a case of freedom of speech." ("Jon Johansen's Answers to Your DeCSS Questions" 2000) As another contributor to the gallery put it:

> I believe that programming code deserves protection under the First Amendment to the United States Constitution and, more generally, that censorship does not benefit society. Publishing a portion of DeCSS in my high school yearbook was a way to ensure that attempts to censor this speech would fail. (Michaels-Ober 2003)

The political coders' emphasis on freedom of speech fits comfortably with utopian visions of the Internet as a forum for unfettered, truly free speech. Their argument for a natural consonance between Internet culture and free speech, resting on the technical difficulty of online censorship, promotes the deliberative democrats' aspirations for democratic discourse online. In this view, the Internet is not only a welcoming forum for the free exchange of views, but it has its own class of warriors dedicated to protecting free speech online.

This sunny picture of the Internet as a natural home to free speech is countered by other members of the hacktivist scene. In sharp contrast to political coders, performative hacktivists and political crackers argue that freedom of speech is illusory, relative, and less important than political outcomes. Each of these arguments surfaces repeatedly in the writings and comments of performative hacktivists, political crackers and their supporters.

The argument that online freedom of speech is illusory takes several forms. “Arguably,” one hacktivist writes, “you cannot effectively implement your right to free speech without stepping on the toes of another....hence, politically motivated hacking.”(Me Uh K. 1999) A harder line view is expressed by the electrohippies, who write that

> any claim that you have 'rights' of expression online is clearly wrong. You have only what your service provider gives you. Beyond that, you'd have to challenge them under contract law through the courts - and you'll more than likely lose because in this arena it's contract law that has the primary weight, not civil rights law. (electrohippies 2003)

Other hacktivists seem to hold more respect for the notion of free speech, yet still defend actions that seem to infringe on the speaking rights of others. These are often justified on the grounds that speaking rights are relative, and that inequalities of communications access mean that some have more speech than others. Defacements and sit-ins thus level the playing field. In this view, hacking does not constitute a meaningful assault on speech rights, because

> People who have web sites up can spew whatever it is they want to say 24/7/365. If someone were to change the contents of a web site, and it remained changed for a few hours, how have they _REALLY_ infringed on their freedom of speech? (Buster 1999)

Or as another hacktivist put it, somewhat more dogmatically:

> This ‘free flow of information’ crap pisses me off. Fascists are fascists, you have to take the fight right up to their faces, to let them KNOW they are irresolutely opposed by members of society and they will not gain power without the cost of CIVIL WAR. fuck it, lets be realistic about who they ARE, what they stand FOR, and what METHODS fascists will use to achieve POWER....LIES and MISINFORMATION are not ‘free speech’ anyway. (scotartt 1999)

This argument has been used to justify a range of hacktivist projects, most often virtual sit-ins. Writing about the toywar project, one hacktivist observer asks:

> How is the little guy is supposed to fight an injustice against Goliath? A few artists taking on a multibillion dollar dot-com giant doesn't seem like much of a fight. As an example, in order to protect its name, etoy has had to fight eToys in a Los Angeles court. (Dugan 2000)

Similarly, another hacktivist writes:

> Which law are hacktivists to adhere to anyway, when they are trying to support an oppressed group of indigenous peoples in another country? Isn't the law one of the prime obstacles in any activists path? Isn't activism always a way of challenging institutionalised power without going through accepted channels? (xdaydreamx 1999)

Concerns about differences in substantive speaking rights lead to arguments suggesting that the ends justify the means – where the means is performative hacktivism or political cracking. As one member of the hacktivism.ca listserv writes, “[i]f governments are killing people, it seems that almost any action can be morally justified.”(Jones 1999a) The ends over means perspective is also reflected in the comment of one of the electrohippies that

> I don’t have a problem with this [information theft] where it’s done for the purposes of a public campaign. Information theft to support fraud, or some other activity like targeting people for abuse or violence, I don’t agree with. (Mobbs 2003)

And in the world of political cracking, the ends-over-means argument is also used as justification for web site defacements:

> We would call ourselves as people who’re trying to make a difference and showing the true faces of the countries like Israel, India or any other country doing unjustice. We don’t mind what people call us, our work speaks for itself.(m0r0n and nightman 2002)

> i dont have any intention to flame or hurt anyone..if anyone of you get hurt or feel insulted then i am sorry..I dont want to write too much but i will sure use the biggest medium to voice my opinion because its my right and ive been doing this for long. ... This defacing for a cause is to show the people what is going "behind the scenes"..and to make them know about the "real facts" of the respective casue.... I cant go and fight for

> all the nations suffering, but i can do something to make the world know about the injustice going around. Defacing a websites will cost nothing to the target.(Nuker 1999a)

Among performative hacktivists, the ends-over-means argument is explicitly juxtaposed with the hacker/coder preoccupation with protecting the flow of information online. For example, Ricardo Dominguez describes the reaction to one of his virtual sit-ins:

> as we were about to start the action, we were surrounded by a group of hackers called Hart. Dutch hackers. And they said, Ricardo, Stefan, what you're about to do will destroy infrastructure. And if you guys do it, we will take you down. It was our first encounter with what I call the "digitally correct" community. Those who believe that bandwidth is above human lives. (Dominguez 2002a)

Political coders greet this argument with great skepticism, treating the "level playing field" and "ends over means" claims as direct challenges to the hacker emphasis on freedom of speech. Critiquing a virtual sit-in campaign, one political coder wrote that

> I think Electrohippies should just come out and say, "We are not for free speech".Why else allude to it in these kinds of statements? Why admit you are doing Distributed Denial of Service attacks, admit that you are using these attacks to censor, and not just come out and admit you are pro-censorship? (thepull 2002)

The view that virtual sit-ins and other performative techniques are a direct assault on online freedom of speech is widespread among political coders, who worry that such techniques could damage the health of the Internet itself. Writes one hacktivist, "personally, I am against dos attacks even for activism purposes…its counter to the way the net was designed to be used."(sam) Another coder writes that

> I have never participated in any DOS activities, nor will I. DOS attacks almost always have innocent, unintended victims in addition to the intended. I once worked at a small ISP which hosted several customers who drew DOS attacks. The attacks took the entire ISP offline, affecting not only the intended victim but many others as well.

Some argue that performative hacktivist techniques like the virtual sit-in take the hack out of hacktivism:

> I’ve never found one of these [virtual sit-ins] to be beneficial. I always thought hackers were supposed to free information flow and spread data, not clog up the lines and shut people down.(Eisley 2003)

Not all hacktivists divide neatly on the issue of free speech versus creative action. Some hacktivists struggle with the question of whether certain hacktivist techniques represent intolerable assaults on the Internet and its free speech culture, or whether they are reasonable tactics for action on the part of disadvantaged groups. “I can’t take a hard line on the DoS issue,” metac0m said. “It’s turning tables for a brief period. I’ll give them publicity, but I won’t organize them.”(metac0m 2002) Similarly, another hacktivist said

> I have never taken part in such actions [redirects, defacements, DoS, information theft, or sit-ins]. I have been thinking of it a couple of times, and just could not decide whether it was right or not. For instance when I read about the Nike redirection I thought "haha, in their faces!", but I also thought "hey, that was illegal". Maybe most people do not care, but for me it's a very complex moral and philosophical issue. Will the effects be more important if more risks are taken? Does the righteousness of the political message make it "less" illegal? I just cannot decide yet, so I stick to more secure actions. (Hocevar 2003)

The hacktivist debate over free speech versus tactical effectiveness is an interesting one for deliberative democrats. Whereas much of the discussion over the bounds of legitimate speech focuses on freedom of expression,[56] the hacktivist problem does not derive from limitations on the ability to speak. After all, any hacktivist has the alternative of publishing his or her views on a web page. But that alternative has inherent limitations, as one cracker team notes:

> if we'd build up a site & post our messages on the site, hardly very few people would come & visit us, we've got to make people read the truth; if we post the things on a page already visited by many people for some reason or the other, that's effective. ("Interview with World's Fantabulous Defacers")

The motivation for hacktivism thus lies not in unequal access to speech, but rather, inequality in the ability to be heard.

[56] See, for example, (Cohen 1998), (Nickel 2000),(Charney 1998).

The “level playing field” and “ends over means” arguments both amount to claims about speaking rights that are substantive rather than procedural. It is not enough to have networked media that make it possible to speak, goes the level playing field argument: inequalities in access to publicity and mass media mean that the underdog’s message may be lost in the shuffle. Hacktivism is a way of ensuring that the underdog’s voice may be heard among the louder voices of the more privileged. Similarly, the ends over means argument holds that if your message is really important, it is not enough to simply float it out into the digital abyss; you need to ensure that the message is received. Again, hacktivism is seen as a way of commanding audience.

The problem of pursuing audience, rather than simply speech, stems from the very virtue that so many deliberative theorists see in the advent of the Internet: the universal availability of a platform for self-expression. By providing a very widely accessible tool of mass communication, the Internet has made the ability to communicate much less scarce. Instead, it is the availability of audience that is scarce.

The focus on audience, rather than speech, is clear from the comments of hacktivists themselves, who believe that their tactics translate into audience and awareness. “Sometimes a ‘pie in the face’ can draw more attention to your cause then putting up a thousand web sites countering their views.”(Buster 1999) A member of the Electronic Disturbance Theater said that her group was “forcing people to pay attention” in a climate in which the “attention span is a minute.” (Karasic 2002)

Political crackers have made similar claims; for example take the team of crackers who write that, “[u]s defacing sites may not bring peace, but it will certainly create global awareness about the suffering of the Muslims of Kashmir, and the righteousness of their cause." (m0r0n and nightman 2002) Another cracker claimed victory for his defacement campaign, using one web site defacement to reflect on the media attention he received for his previous defacements:

> At last, Kashmir issue got some attention..
> Thanks to CNN..
> What about a deal now??
> Took more than 40 defacements to get noticed..
> Exactly how many web sites you guys wanna see defaced to solve the problem??
> (Nuker 1999b)

Even those who criticize tactics that infringe on speech rights have sometimes acknowledged that these tactics can be effective attention-getters – if not effective agents of change. As one critic has written:

> The problem with you people (and that applies in equal measure to Paul Mobbs & the 'Electrohippies' EDT/Floodnet epigonism) is that you were for media attention from the very start. And you political ideas never went very much further than to create a cyberspace equivalent of the mass movements of old, with you of course as its avant-garde leaders. … You would do us all a great service if you folks would fold your buffooneries and join the ranks of serious activism. It's less spectacular, and your name will appear less often in the mainstream media. But it's more worthwhile and will get the cause (whatever we believe it to be, justice and peace may be?) more mileage. (Riemens 2001)

All of these comments underline the core problem: audience scarcity. As described by Goldhaber's work on "the attention economy", the problem stems from the fact that "attention…is an intrinsically scarce resource." (Goldhaber 1997) Yet where Goldhaber anticipates that "individual attention getters of all sorts will find it ever easier to get attention directly through the Web," the hacktivist case suggests that even skilled Internet users may find it hard to command an audience in an atmosphere with so many competing for audience. Hacktivism provides a way of addressing inequalities of audience access, even when avenues of expression are widely available.

The challenge for deliberative democrats is that acknowledging audience scarcity (and inequality of access) makes freedom of expression look like a relatively hollow basis for deliberation. If participants cannot be satisfied with the opportunity for speech, but instead demand the opportunity to be heard, how are we to constitute procedural principles for online deliberation?

The problem of anonymity

Perhaps no aspect of online communications poses as great a challenge to our aspirations for meaningful democratic discourse as the ready availability of anonymous speech. Anonymity has been only a rare feature of speech in the "real" world, but in cyberspace, it is routine.

The role of anonymity in public life has been subject to much debate. The debate can be distilled to two contradictory positions. One sees anonymity as a necessary and valuable part of political life. This position ties anonymity closely to free speech, holding that total privacy – anonymity – is sometimes necessary to free speech. Anonymity "encourages the free flow of ideas"(Amis 2001), allowing people to make unpopular statements that nonetheless enrich public debate. Anonymity allows speech in which the focus is on the speech, not the speaker. Anonymity allows people "to avoid persecution" (Marx 2001) even as they speak their conscience freely.

The opposite extreme sees anonymity as a danger to democracy and public life. This position focuses on accountability as the root of responsible behavior and responsible politics. Anonymity brings out the worst in people by allowing them to evade the consequences of their speech or actions. Anonymity precludes meaningful speech because it makes it impossible to judge the interests or motives of the speaker. Some also argue that "anonymity -- like the myth of Gyges's ring that makes the wearer invisible -- leads inexorably to immoral and even illegal behavior." (Saco 2002)

This debate is crucial to our assessment of the prospects for electronic democracy. If anonymity is congenial to democracy, online deliberation may be if anything more robust than its offline predecessors. If, on the other hand, anonymity is destructive to democracy, our hopes for electronic democracy must be constrained; or our laws and technologies of identity verification must be greatly strengthened.

Yet until now, the debate over anonymity has been largely a theoretical one. The two extreme positions in the anonymity debate represent normative beliefs about anonymous speech, not empirical claims about how anonymity actually works. As long as anonymity was constrained to "bathroom walls and prank calls"(Hilden 2001), this was by necessity a normative debate. But the rapid expansion in anonymous speech facilitated by the Internet allows us to examine these competing principles against a richer field of anonymity practices.

Hacktivism offers a particularly interesting array of anonymity practices. First, it offers three very distinct positions on anonymity, which to a large degree correspond with the three distinct cultures of political crackers, performative hackers, and political coders. Second, the very extremism of hacktivist practices make them appear very similar to the best and worst case scenarios envisaged by anonymity advocates and opponents.

If we fear that anonymity facilitates injurious or even criminal behavior, then hacktivism would seem to be a case in point. Political crackers deface web sites, slow, block, or damage web servers, distribute viruses, and wreak other kinds of havoc. Their actions seem to typify the kind of antisocial behavior feared by anonymity opponents.

On the other hand, hacktivism also embodies some of the hopes of anonymity proponents. As predicted by anonymity advocates, political crackers use their anonymity to express unpopular or challenging opinions. While they can be destructive, that destruction is usually limited, and is always in service to some form of political communication or action. Both political crackers and political coders detach their message from the identity, nationality or location of the messenger – realizing the vision of anonymous speech as speech in which the focus is on the message, rather than the speaker.

But the actual practices of hacktivists fit neatly with neither the hopes nor the fears expressed in the literature on anonymity. As Gary Marx has observed, anonymity is not a binary phenomenon. Rather, “identifiability at one extreme can be contrasted with anonymity at the other. Describing a variety of kinds of identity knowledge and approaching these as distinct continua brings us closer to the messiness of the empirical world” (Marx 2001).

Some hacktivists, almost always political crackers, usually use what Marx refers to as “pseudonyms that can not be linked to other forms of identity knowledge --the equivalent of "real" anonymity (except that the name chosen may hint at some aspects of "real" identity, as with undercover agents encouraged to take names close to their own)”(Marx 2001). This reflects the fact that crackers are engaged in activities that could entail significant legal consequences if they were caught.

In contrast, political coders most frequently use "pseudonyms that can be linked to legal name and/or locatability --literally a form of pseudo-anonymity." Coders vary somewhat in their use of pseudonymity; the participants in Peekabooty are identified by their legal names on the project's web site. Hacktivismo participants use their pseudonyms in their work with the project, but are mostly forthcoming with their real names in face-to-face interactions. DeCSS authors sometimes use traceable pseudonymns or real names, and sometimes use untraceable pseudonyms or remain anonymous.

Performative hackers – along with some political coders -- are generally known by their real names. The names of the electrohippies, the ®™ark team, and the members of the EDT are all publicly available. The EDT consciously rejected anonymity when it got the hacktivism ball rolling:

> we made a decision that was very very strange but that seemed on a gut level what we needed to do, but it went against all the usual elements. We decided not to be anonymous. Not to be secret – to be transparent. And this went against hacker culture, which is about anonymity, which is about secrecy. (Dominguez 2002a)

The decision to embrace accountability, and reject anonymity, is not always an easy one:

> I worry a lot about what I do online. There are ways to be completely anonymous on the Internet, and if you are very skilled and careful, no one can get back to you, not even the FBI or the NSA or whatever. But I believe that my actions would have less impact if performed anonymously. This is why I do not hide, and why I carefully choose my activities. (Hocevar 2003)

How are we to interpret this variation in nymity practices? Not in the terms afforded by democratic theory's debate over anonymity – with the possible exception of pseudo/anonymity practiced by political crackers. Their use of pseudo/anonymity as a shelter from legal consequences fits the argument that "anonymity supports the mischievous, the petty vandalisms against each other and authorities that give us room to mock perceived hegemonies and to release 'incorrect' but genuine feelings."(Smith 1997)

But the pseudonymity practiced by political coders is far cry from the kind of anonymity that some fear "facilitates wrong by eliminating accountability, which is ordinarily the very purpose of the anonymity"(Amis 2001). It is equally ill-described by those proponents of anonymity who see anonymity as a liberating tool in democratic discourse. It is true that deliberative theorists sometimes envision political debate in the public sphere as an "anonymous public conversation"(Benhabib 1996; cited in Charney 1998). But this is not the same type of anonymity as the anonymity practiced by hacktivists and other Internet users, as Bregman points out:

> An anonymous membership is ideal, but not necessarily in the sense of cyberspace anonymity. Anonymity as it is generally conceived of in cyberspace—where persons can communicate without regard for attributes such as race or gender—detracts from the humanity of the discourse. Members should have enough information about one another to gain a universal mutual respect for one another as human beings, but that's not enough. In addition, the discourse benefits from members who appreciate the importance of the recognition of "group-based" identities which can only be gained from knowing something about the specific identity/background of other discourse participants. (Bregman)

Hacktivist nymity practices, like many anonymity practices online, are ultimately ill-described by the scholarship on offline anonymity. They are better understood as decisions about the construction of a digital identity than as statements of offline compliance or subversion. As Diane Saco argues, "electronic pseudonymity -- anonymity through the adoption of an alias -- can have the parallel effect of constructing a kind of public voice even as it protects personal identity." (Saco 2002) This is a function of the exclusivity of usernames on e-mail systems: "Ideally, if someone chooses a pseudonym in one of these systems, no one else can send mail under that name. This allows for the possibility of a true digital persona -- an ‘identity’ permanently disembodied from one’s physical being.” (Saco 2002)

Political coders and political crackers create these digital alter egos through their consistent use of a pseudonym online. If crackers were only interested in escaping the legal consequences of their hacktions, they would be better off leaving their web defacements unsigned. But the use of digital pseudonyms allows the creation of a cumulative body of work – a digital manifesto – for which they are both identifiable and accountable within the virtual community.

Being able to take digital credit for one’s hacktivism is only part of the attraction of pseudonymity, however. As the Supreme Court of the U.S. has observed, “anonymity… provides a way for a writer who may be personally unpopular to ensure that readers will not prejudge her message simply because they do not like its proponent.”("McIntyre v. Ohio Campaign Commission 1995) This same benefit is provided by electronic pseudonymity, and is particularly in keeping with the tenet of the hacker ethic that holds that “[h]ackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.” (Levy 1984) This is explicit in political crackers’ rejection of questions about their age or nationality: “Dividing people according to country is not our style, as mentioned earlier ``DIVISION`` is not a word in our lexicon.”(m0r0n and nightman 2002) Pseudonymous and anonymous hacking is a statement about separating the virtual body from the physical body, and all the criteria (like nationality, race, or gender) that we use to judge physical personae.

Performative hackers’ use of real names is an explicit rejection of that separation. Performative hacktivists argue for a reunion of virtual and real politics, and criticize the hacker fantasy of “having the data body leave the real body, the electronic body uploading itself.” (Dominguez 2002a) Using real names in cyberspace is a way of rejecting the hacker separation between the virtual and real, and instead affirming real-world accountability for virtual acts.

These different nymity choices thus translate into different kinds of accountability claims. Political crackers use robust pseudonymity or anonymity to declare that they are accountable to no one (although either coder carelessness or government intelligence work may sometimes put the lie to that claim.) Political coders embrace (generally weak) pseudonymity as a hacker convention. While they thus construct a digital persona that is accountable to the digital community (and also subject to the laws of their physical homeland), it is accountable only in terms that divorce the judgement of the digital body from the characteristics of its fleshy analog. Performative hackers explicitly reject the pseudonymity and anonymity of the hacker world, and embrace accountability to the physical world instead.

These decisions about accountability are partly tied to perceptions of risk, and risk tolerance. Political crackers hack illegally and anonymously because they are confident that their anonymity can protect them from the legal consequences of their actions. As one team of crackers put it: “We don't leave our marks behind for ‘anyone’ to follow. We're not worried about it. We're outside the jurisdiction of any agency that is hostile to us.” (m0r0n and nightman 2002)

Performative hacktivists, on the other hand, tend to be more risk-averse. One performative hacktivist described her boundaries by saying that she “never did anything that I thought would have me arrested.”(Karasic 2002) Another said that he was “scared that taken out of context anything I or my friends are involved in could be considered illegal."(Karasic 2002) A third pointed out the strategic limitations of engaging in illegal activity: "I'm trying to be effective as an activist, and if you want to get the most people involved in movements you generally want to focus on legal activities so that people will participate." (Kreider 2003)

Political coders fall into a middle territory, in which an awareness of legal risks is leavened by confidence in their ability to manage those risks. Sometimes it is a question of picking one's battles: "I wouldn't do anything illegal in North America," says one member of Hacktivismo (metac0m 2002). He is echoed by a Hacktivismo collaborator who doesn't worry about legal issues "at all" because "none of the projects we have underway right now would fall under any [Canadian] laws." (Happy 2002) For others it is a matter of personal ethics happening to coincide with the law: I don't give a fuck about legal issues," said one political coder who had been arrested as a teen hacker. "I do whatever I want. I have my morality that forbids me to do things that are destructive so most times I live within our laws. If there are legal consequences, I was too under-skilled." (Jules 2002) And sometimes an acceptance of a certain degree of legal risk stems from trust in a broader network of support: " I believe I can defend myself, and that an advocacy group, like the EFF [Electronic Frontier Foundation], would help me in any legal battles I would have concerning my online activities." (Brown 2003)

While legal concerns thus factor into nymity decisions, hacktivists can be very explicit about seeing their nymity choices as conscious political statements. As one performative hacktivist put it:

> One main distinction between most Politicized Hacking and the type of Electronic Civil Disobedience just mentioned is that while ECD actors don't hide their names, operating

> freely and above board, most political hacks are done by people who wish to remain anonymous. It is also likely political hacks are done by individuals rather than by specific groups. …This distinction speaks to a different style of organization. Because of the more secret, private, low key, and anonymous nature of the politicized hacks, this type of activity expresses a different kind of politics. It is not the politics of mobilization, nor the politics that requires mass participation. (Wray 1999a)

Another performative hacktivist described the choice of anonymity versus transparency as a strategic choice about what kind of role to play within a broader political movement:

> Where a hardcore hactivist cant talk about what they do because they will go to jail, we court the media, blab about our actions to the press, and try to create the best stories possible. So, it is fundamentally different in that we are like the propaganda wing of a movement, whereas hactivists are the guerrilla fighters who cant show their faces at all. (Guerrero 2003)

All of these conscious nymity choices depart sharply from the theoretical expectations about anonymity in public speech. Hacktivists do not use anonymity as a blanket avoidance of legal consequences; nor do they treat it as a universally ennobling way of liberating message from messenger. Rather, they treat anonymity as a political tool, with different nymity choices conveying different kinds of claims about political strategy, risk, and above all, accountability.

The idea of nymity as a sort of accountability claim is a significant challenge to democratic theories that treat nymity as an issue of principle. Hacktivist practices suggest that rather than framing the question of anonymity as a principled debate over accountability in public speech, nymity should be seen as one of the kinds of claims that speakers make when participating in deliberative discourse.

Conclusion

The challenges that hacktivism has posed to the notions of freedom and accountability in democratic discourse are likely the first wave of a larger transformation. Hacktivist tools are being distributed to a widening audience that will find lower-and-lower barriers to entry. These include the Hacktivismo tools, as well as projects like the Disturbance Developers' Kit and the Yes Men's Reamweaver software. [57]

Meanwhile hacktivists are also publicizing and teaching hacktivist techniques. Several web sites maintain running news files on hacktivist activities and tools. The Ruckus Society, which trains protesters in non-violent resistance techniques, held its first hacktivist training camp in June 2002. These developments promise to expand the ranks of hacktivists, and extend hacktivist-style protest to activists whose primary allegiances lie outside of the hacktivist community.

The challenges to deliberative discourse posed by the digital world are not limited to hacktivists and their disciples. The developments that make hacktivism a challenge to deliberative speech are also visible in other corners of Internet culture. For example, the right to free expression is facing increasing claims of a right to be heard. Advertisers have made legal arguments against technologies that allow consumers to bypass advertising, claiming that what they have purchased is not airtime but eyeballs [58].

[57] The Disturbance Developers' Kit was a project of the Electronic Disturbance Theater, and made the EDT's FloodNet code available to any group interested in staging a virtual sit-in. Reamweaver is a program that automates the creation of web site parodies.

[58] Several entertainment companies launched a 2001 lawsuit against SonicBlue, makers of a digital video recorder known as ReplayTV. At the heart of the lawsuit was ReplayTV's ability to automatically skip commercials, which television and media companies (accurately) saw as a threat to their advertising revenue. For a summary of the case see(Isenberg 2001).

The strategic use of anonymity also seems to be a growing phenomenon. People routinely make choices about the degree of identifiability they wish to undertake in any given online context. They may use full names in professional discussion groups, traceable pseudonyms in online support groups or interest discussions, and untraceable anonymizers in discussions about illegal activities, sexuality, or other sensitive areas. These choices reflect decisions about how accountable people want to be, to whom, and under what circumstances.

Can deliberative democracy reformulate the debates over free speech and accountability in order to come to terms with these practices? The question may be moot. Along with the challenges to democratic discourse, hacktivism has significantly compromised the prospects for enforcing any rules of discourse – even if such rules could be agreed upon.

Hacktivists are making the difficult job of policing online speech even harder. And not by accident: many hacktivists are deeply committed to the idea that online speech should be freer than speech in the real world. They are heavily influenced by a kind of hacker romanticism that sees the Internet as the last frontier for truly free speech, and as a kind of generalized libertarian haven.

Both of the challenges previously outlined limit the state's capacity to monitor and regulate speech. Defacements and sit-ins grab opportunities for audience, whether or not they are institutionally or normatively sanctioned. Anonymity and pseudonymity can prevent monitoring and enforcement by the state.

But hacktivists are also consciously use technologies to limit the state's capacity to monitor and regulate speech. Policy circumvention projects like DeCSS and

Hacktivismo aim at crippling government's capacity to restrict online communications. Jam Echelon Day – a stunt that encouraged Internet users to overload government surveillance networks by e-mailing lists of keyword triggers – raised the prospect of stymieing automated monitoring.

The effort to resist regulation of online speech extends far beyond the hacktivist community, however. A variety of privacy tools and organizations are allowing Internet users to elude government regulation of speech. The widespread availability of encryption tools allows people to circulate information beyond the reach of government monitors or censors. Movies that fail government rating standards can be independently distributed online. Organizations like Privaterra[59] use privacy tools to ensure freedom of speech in monitored jurisdictions.

The purpose of these tools is to take the decision to monitor or regulate speech out of the hands of the state. Instead of collective decisions (or authoritarian decisions) about how speech should be regulated, individuals create their own speech regimes by choosing tools that provide them with a greater degree of privacy. By creating these tools, hacktivists and other Internet users preserve the Internet as a space for self-regulating speech.

That may be a challenge for proceduralist visions of deliberative democracy that seek to establish structures for discourse – including ground rules for free expression and accountability. But the impossibility of enforcing rules of discourse may be the ultimate victory for the Habermasian vision of the public sphere as deliberation without coercion,

[59] Privaterra works with international human rights workers to ensure that their activities can elude government monitoring and restriction.

its only goal “a consensus brought about by coercion-free communication.” (Habermas 1983)