The Ethics of Hacktivism

Abby Goodrum *and* Mark Manion

Introduction

In a civil society, it is the responsibility of all ethical individuals to take a stand against oppression, inequality, and injustice. Civil disobedience is a technique of resistance and protest whose purpose is to achieve social or political change by drawing attention to problems and influencing public opinion. Civil disobedience requires that individuals be willing to peacefully break laws that are unjust and be willing to suffer the legal consequences of their actions. It does not condone violent or destructive acts against its enemies, focusing instead on nonviolent means to expose wrongs, raise awareness, and prohibit the execution of unethical acts by individuals, organizations, companies, or governments. Breaking specific laws that are unjust constitutes direct acts of civil disobedience. Symbolic acts of civil disobedience are accomplished by drawing attention to a problem indirectly. Sit-ins and other forms of blockade and trespass are symbolic acts of civil disobedience. While the underlying principles of civil disobedience have not changed much over the course of the past 150 years, the tactics of civil disobedience have been continually influenced by available technologies.

Abby Goodrum, College of Information Science & Technology, Drexel Univrsity, 3141 Chestnut Street, Philadelphia, PA 19104-2875.

Mark Manion, Department of Humanities and Communications, Drexel University, 3141 Chestnut Street, Philadelphia, PA 19104-2875.

Electronic Activism & Civil Disobedience

The Internet has created a brave, new world of digital activism by providing forums for organizing, communicating, publishing, and taking action. The use of the computer as a tool of civil disobedience has been termed Electronic Civil Disobedience (ECD). Electronic civil disobedience comes in many forms, and ranges from conservative acts such as sending email and publishing web sites, to breaking into computer systems. A distinction must be made between the use of computers to *support* ECD, and the use of computers as an *act* of ECD. If a US citizen wishes to speak out against the government's actions in Kosovo, it is legal to publish a web site or host mailing lists or chat rooms for this purpose. This activity does not constitute an act of civil disobedience; electronic or otherwise. Running a program such as FloodNet that posts the reload command to a web site hundreds of times a minute is also not against the law but it may constitute an act of ECD since the intended aim of such programs is to create an electronic disturbance akin to a sit-in or blockade. The effect of hundreds of persons reloading a targeted page on the web thousands of times effectively blocks entrance by outsiders and may even shut down the server. In 1998, pro–Zapatista activists took this action against Mexican Government web sites (Cleaver, 1998). This is easily seen as a symbolic act of ECD. The purpose of most ECD is to disrupt the flow of information into and out of institutional computer systems. The point is not to destroy information or systems, but to block access temporarily. This results in virtual sit-ins and virtual blockades. Since institutions today are no longer localized in physical structures but exist in the decentralized zones of cyberspace, electronic blockades can cause financial stress that physical blockades cannot. These activities in large part are not undertaken anonymously and seldom result in reprimands let alone arrests. Taken to an extreme, ECD has been interpreted to mean breaking into a computer system for the purpose of altering information and /or leaving political messages. In contrast to other forms of ECD, these acts of hacktivism are almost exclusively anonymous and have been prosecuted as felonies.

Hacktivist groups such as the Electronic Disturbance Theater, the Cult of the Dead Cow, and the Hong Kong Blondes, have used electronic civil disobedience to help advance the Zapatista rebellion in Mexico, protest nuclear testing at India's Bhabba Atomic Research Centre, attack Indonesian Government websites over the occupation of East Timor, as well as protest anti-democratic crackdowns in China. In addition, hacktivism has been used to inveigh against the corporate domination of telecommunications and mass media, the rapid expansion of dataveillance, and the hegemonic intrusion of the "consumer culture" into the private lives of average citizens.

Hacktivism has the potential to play an active and constructive role in the

overcoming of political injustice, to educate, inform and be a genuine agent of positive political and social change. However, there is the fear that cyber-activism could transform into more radical and violent forms of cyber-terrorism (Arquilla and Ronfeldt, 1993). How governments and societies react to this new form of social activism has not been sufficiently addressed in the computer ethics literature. Researchers concerned with ethical issues in computing, policy makers, and computer professionals must come to terms with the complex set of issues surrounding the potential power of hacktivism.

The Relationship Between Hacktivism and Civil Disobedience

Nothing has fired debate about ECD so completely as the issue of hacktivism. In order to justify hacktivism's direct action praxis and to legitimate its theoretical foundations, two things must be demonstrated. First, it must be shown that hacktivism is *not* the work of teenagers with advanced technical expertise and a thirst and curiosity for infiltrating large computer networks for mere intellectual challenge or sophomoric bravado. In addition, the justification of hacktivism entails demonstrating that its practitioners are not cyber terrorists— breaking into systems for profit or vandalism. Hacktivism must be shown to be politically, i.e., ethically motivated. Second, politicized hacking must be shown to be a form of civil disobedience. The central question of whether hacking can reasonably be defined as an act of civil disobedience revolves around five basic tenets that have generally defined civil disobedience:

- No intentional damage done to persons or property
- Non-violent
- Not for personal profit
- Ethical motivation
- Willingness to accept personal responsibility for outcome of actions

May the same points be taken as evidence of hacking as an act of ECD? 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. Examined in this light, the hack by Eugene Kashpureff clearly constitutes an act of ECD. Kashpureff usurped traffic from InterNIC to protest domain name policy. He did this non-anonymously and went to jail as a result. Similarly, members of the Electronic Disturbance Theater use their own names and emphasize disrupting Internet traffic rather than altering sites or crashing servers. Further evidence of an ethical motivation underlying hacktivism can be found in an examination of the style and messages left behind at hacked sites.

On October 12, 1998, the website of Mexican president Ernesto Zedillo was attacked. From all accounts, the Zedillo attack was not the work of bored teens. It was a political act, according to the Electronic Disturbance Theater, to "demonstrate continued resistance to centuries of colonization, genocide, and racism in the western hemisphere and throughout the world" (Wray, 1998). In August of the same year, the hacktivist group X-Ploit hacked the website of Mexico's finance ministry, defacing it by replacing the contents with the revolutionary hero Emiliano Zapata, in sympathy with the Zapatista rebellion in the Chiapas region of southern Mexico (Cleaver, 1998). These acts are protests that are drawing attention to what is perceived to be grave social injustices. One thing is clear: they are motivated by a socio-economic system that perpetuates discrimination, racism, and economic inequality — not the mere thrill and challenge of breaking into networks for fun.

In June of 1998, the hacktivist group MilwOrm hacked India's Bhabba Atomic Research Centre to protest against recent nuclear tests. 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 anti-nuclear statements and images of mushroom clouds. Not surprisingly, the published slogan of MilwOrm is "Putting the power back in the hands of the people" (Glave, 1998a). This appears to be more motivated by belief in the force of participatory democracy than mere vandalism or cyber-terrorism.

Several Indonesian government web sites were hacked to protest the targeting of Chinese and Indonesian citizens for torture, rape, and looting during the anti-Suharto riot in May of 1998. On August 1, the Portuguese hacktivist group Kaotik Team hacked 45 Indonesian government websites, altering pages to include calling for full autonomy for East Timor and the cessation of the harsh military crackdown on dissidents (Hesseldahl, 1998). Again, fighting for social justice and human rights is motivated by ethics, not anarchy. Many, many other hacktivist activities can be cited to demonstrate the ethical motivation behind this new form of political activism. These messages demonstrate a striking change from hacker attacks of the past. Prior hacks have had little, if any, socio-political content, and bear a closer resemblance to "tagging" and other forms of boasting graffiti. There has been a certain juvenile style to messages left by hackers in the past, but the hacks discussed above represent a new breed of hacker — one motivated by the advancement of ethical concerns. Hence, one can conclude that our thesis — that hacktivism is ethically motivated and constitutes an act of civil disobedience — can be clearly established.

The Law and Civil Disobedience

Historically, our legal system evolved in order to protect narrow economic interests, rather than administer to broader social concerns. Civil disobedience,

therefore, is treated as a philosophical or political action, not a legal right, and is subject to penalty. How much penalty? Demonstrators or civil disobedients are commonly charged with disorderly conduct, trespass, or resisting arrest. Occasionally, protestors are charged with more serious crimes, which can include assault, rioting, and racketeering. If property damage occurs, protesters may be charged with criminal mischief, which is defined as "intentionally interfering with the lawful use, enjoyment or operation of property" (Herngren, 1993).

So, if civil disobedience compels us to accept the penalties for our actions, and if the law does not recognize civil disobedience as a legal right to break the law, one would expect sentences to be quite harsh. In fact, courts have considerable discretion in deciding how high a fine or how long a jail sentence to impose on those convicted of acts of civil disobedience. In most cases the courts have not pursued criminal sanctions against civil dissidents, and in so doing have informally established that penalties for civil disobedience should be lessened due to the ethical motivation supporting the action.

In contrast to older forms of civil disobedience such as trespass and blockade, hacking has not yet been recognized as a political activity having ethical motivations. Consequently, the penalties for breaking into computers can be extreme (Jaconi, 1999). For example, the hack of China's "Human Rights" website by the Hong Kong Blondes, attacks on Indian Government websites regarding policy in Kashmir, and on India's nuclear weapons research center websites to protest nuclear testing are all subject to felony prosecution if the perpetrators are apprehended. It is important to remember that in many countries any form of protest against the government is a capital offense. Seen in this light, the predominantly anonymous nature of hacktivism can perhaps be understood.

Penalties for hacktivism are meted out with the same degree of force as for hacking in general, regardless of the motivation for the hack or the political content of messages left at hacked sites. In fact, since many acts of hacktivism have been perpetuated against government websites, hacktivism is increasingly being equated with acts of information warfare and cyber-terrorism (Kovacich, 1997, Furnell & Warren, 1999). Under U.S. law, terrorism is defined as an act of violence for the purpose of intimidating or coercing a government or civilian population. Hacktivism clearly does not fall into this category, since it is fundamentally non-violent. Nevertheless, in August of 1998, the Center for Intrusion Control was established by a coalition of various government agencies to respond to these "cyber-warfare threats" (Glave, 1998b). Similarly, organizations such as RAND and the NSA have categorically ignored the existence of hacktivism as an act of civil disobedience and repeatedly refer to all acts of hacking as info-war or info-terrorism in an attempt to push for stronger penalties for hacking regardless of ethical motivations (Bowers, 1998; Gompert, 1998).

Power, Property, and Computerization

One rationalization for the vilification of hacktivism is the need for the power elite to rewrite property law in order to contain the effects of the new information technologies (Halbert, 1997). As a result of the newly evolving intellectual property laws, information and knowledge can now be held as capital. Since new information technology supports easy reproduction of information, the existence of these laws effectively curtails the widest possible spread of this new form of wealth. Unlike material objects, information can be shared widely without running out. Therefore, the intellectual-property laws help create a distribution of wealth that is unnecessarily limited.

Moreover, financial and banking institutions have gone digital, converting money itself into pure information. Traditional, sedentary forms of power and tangible capital are being replaced by capital constituted in electronic form that is fluid, mobile, and dispersed (Critical Art Ensemble, 1994). The result is the concentration of wealth in the hands of those most skilled at the appropriate manipulation of symbols. Hence any resistance to this power must take this fluidity, mobility, and dispersion into consideration; effective resistance must mirror these attributes.

The changing nature of authoritative and repressive power has necessitated qualitative changes in resistance to this power. Power/Capital, having constituted itself in a new electronic form in cyberspace, requires that opposition movements have to invent new strategies and tactics that counter this new nomadic power of capital. This entails that certain old ways of trespass and blockade — such as street demonstrations are being modified through hacktivism to meet the new conditions (Critical Art Ensemble, 1996).

The commercial control of computers and information technology will deepen class divisions nationally and internationally, as people divide into those who can afford the technology, services, and content — the information rich — and those who cannot — the information poor. The promise of freedom from work, participatory democracy, and global community, once hailed as the hallmarks of the computer revolution are nowhere to be found. The only entities that seem to benefit from the computer revolution are large transnational business corporations.

Technophilic Optimism v. Technophobic Pessimism

Every technology releases opposing possibilities towards emancipation or domination, and information technology is no different. This conflict is often couched as a distinction between two worldviews: technophilic optimism and

technophobic pessimism. For technophiles, technology is the ultimate liberator of human freedom: freedom from the vicissitudes of nature and freedom from political oppression. Computer technology is seen as the utopian promise of total human emancipation and freedom. For technophobes, on the other hand, advanced technology may lead to an Orwellian nightmare of totalitarian domination and control or the dystopian nightmare of complete repression of free thought and behavior control. The Internet has been subordinated to the predatory interests of the techno-elite, who merely pay lip service to the growth of electronic communities and teledemocracy. These interests are devoted to shutting down the anarchy of the Net in favor of virtualized commercial exchange. The power elite must destroy the public cyber-sphere for its own survival. That is why the charges against hacktivism are so high.

Participatory Democracy and Participatory Technology

Computerization fosters great individual empowerment. One example is the hacktivist claim that a single individual can be as powerful as an entire government agency in effecting change. This requires that every person be a participant, creator, and producer rather than just a consumer of information. Active participation in information democracy leads to the creation of a more informed citizenry, and the reinvention of institutional functions and services (Friedland, 1996).

Hacktivism can affect changes in the democratic process through "disintermediation," or the elimination of control over communication by traditional intermediaries. These institutions have historically monopolized access to the flow of information and knowledge to the rest of society. The marriage of hacktivism to participatory democracy leads to (1) the empowerment of individuals—participatory democracy, (2) the breakdown of barriers—participatory pluralism, and (3) disintermediation of channels of communication—direct democracy.

Proposals

The following four proposals are presented in defense of an ethic of hacktivism.

1. Hacktivism, in its advocacy of civil disobedience, demonstrates the necessary relationship between ethics and politics. Computerized activism and electronic civil disobedience offer the potential for civic input into the political

process that is at once empowering and challenging. The role of civil disobedience is to act as an ethical check and outlet against governmental and corporate wrongdoing.

2. Establishing the validity of grass-roots activism reinforces the potential of computerization for civic empowerment. Resistance to the oppressive and unjust use of information technology, based on sound ethical principles and rooted in some sense of moral revolution, is not only possible, but also necessary. The multiplicity of tactics and forms of resistances of hacktivism attests to this.

3. The debate over control of intellectual property demands that we address issues of social justice such as wealth distribution and equality of opportunity. Politically, the resistance to domination must force not only the question of privacy and property, but it must also place the critique of the technological society itself at the center of pubic consciousness and debate. Hacktivists must put the issue of techo-control on the political agenda, laying out as clearly as possible the costs and consequences of computerized technologies. They must force awareness of the principle beneficiaries of the new technology and try to make public all the undemocratic ways they make the technological choices that affect us all. This will demonstrate the necessity for direct citizen participation in technology policy making.

4. Information technologies must not be conceptualized as mere neutral tools that can be used for good or evil; they must be understood as exhibiting an internal logic, a logic that bears the purposes and the values of the economic system that spawns them. Hacktivism, with its focus on pluralism, relativism, and pubic control of information and technology, reinforces and legitimates a "social constructivist" reading of (future) technological progress.

Conclusion

The power elite, often synergistically intertwined with the design and operation of information technologies, will always come to the aid and defense of technologies of control, making revolt difficult and reform hard. Intellectual Property laws attest to this, as do the excessively stringent laws against hacking. Nevertheless, if we say that we support civil disobedience and the power of people to organize themselves collectively for non-violent change, then we must support the computerization of these efforts as well. This means bringing penalties for hacking as an act of civil disobedience in line with penalties for traditional mechanisms for trespass and blockade.

Philosophically, resistance to political repression and oppression must be embedded in a well-articulated theory, one that is morally informed, and widely shared. Movements acting out of rage and outrage often dissipate. They need

to be durable and sustain a commitment lasting through adversities of repression. This leads to the necessity of creating a form of technocultural activism and practice that can bring to reality the ideals of human emancipation. Activism today is no longer a case of putting bodies on the line; it requires and involves putting minds and virtual bodies on-line. This is the promise of combining the political consciousness of the activist with the technical expertise of the hacker — the promise of hacktivism.

References

Arquilla, J. and Ronfeldt, D. (1993). Cyberwar is coming. *Comparative Strategy, 12*, 2, 141–165.

Bowers, S. (1998, August). Information warfare: The computer revolution is altering how future wars will be conducted. *Armed Forces Journal International*, 38–39.

Cleaver, H. (1998). The Zapatistas and the electronic fabric of struggle. (accessed 5/18/99). *http://www.eco.utexas.edu/faculty/Cleaver/zaps.htm*

Critical Art Ensemble. (1996). *Electronic civil disobedience and other unpopular ideas.* Brooklyn, NY: Autonomedia.

Critical Art Ensemble. (1994). *The Electronic Disturbance.* Brooklyn, NY: Autonomedia.

Friedland, L. (1996). Electronic democracy and the new citizenship. *Media, Culture & Society, 18*, 185–212.

Furnell, S. & Warren, M. (1999). Computer hacking and cyberterrorism: The real threats in the new millennium. *Computers & Security, 18*, 28–34.

Glave, J. (1998a). Crackers: we stole nuke data. *Wired News <http://wired.com>*

Glave, J. (1998b). Hacker raises stakes in DOD attacks. *Wired News <http://wired.com>*

Gompert, D. (1998, Autumn). National security in the information age. *Naval War College Review, 51*, 4, sequence 364, 22–41.

Halbert, D. (1997). Discourses of danger and the computer hacker. *The Information Society*, 13, 361–374.

Harmon, A. (1998, October 31). Hacktivists of all persuasions take their struggle to the web. *New York Times*, 1.

Herngren, P. (1993). *Path of resistance: The practice of civil disobedience.* Philadelphia: New Society Publishers.

Hesseldahl, A. (1998). Hacking for human rights? *Wired News <http://wired.com>*

Jaconi, J. (1999). Federal Cybercrime Law, Section 1030 "Computer Fraud & Abuse Act. (accessed 6/17/99). *<http://www.antionline.com>*

Kovacich, G. (1997). Information warfare and the information systems security professional. *Computers & Security, 16*, 14–24.

Wray, S. (1998). Electronic civil disobedience and the world wide web of hactivism: A mapping of extraparliamentarian direct action net politics. (accessed 2-22-99). *http://www.nyu.edu/projets/wray/wwwhack.html*

About the Contributors

Colleen Angel (MLIS University of Wisconsin at Milwaukee) is currently pursuing a master's degree in Organizational Communication at the University of Wisconsin at Stevens Point where she works in the Reference and Interlibrary Loan Departments of the University Library.

Elizabeth Buchanan, Ph.D., is Assistant Professor at the School of Library and Information Science at the University of Wisconsin-Milwaukee, where she is also Co-Director of the Center for Information Policy Research. In addition, she is Chair of the Computer Professionals for Social Responsibility Ethics Working Group.

Elia Chepaitis, a professor of information systems at Fairfield University, has a doctorate in social and economic history and master's degrees in Russian studies, international business, and information systems. Dr. Chepaitis has had three Fulbright research and teaching fellowships and holds numerous international patents for an alternative to braille.

Abby A. Goodrum is Assistant Professor in the College of Information Science and Technology at Drexel University. She teaches in the areas of visual information retrieval, the Internet, and social and professional aspects of information service. Her research focuses on non-textual information seeking and use.

Avi Janssen holds a master's degree in Hebrew and Judaic Studies from New York University, and is currently pursuing a master's degree in Library and Information Science at the University of Illinois at Urbana-Champaign via distance learning. He is Information Services Manager at the Spertus Institute of Jewish Studies.

Sandy Karnold is a Masters student at the University of Wisconsin-Milwaukee School of Library and Information Science.

Tomas Lipinski is Assistant Professor and Co-Director of the Center for Information Policy Research at the School of Library and Information Science, University of Wisconsin-Milwaukee. He holds a JD from Marquette University and an LLM from the John Marshal School of Law. He received his Ph.D. from the School of Library and Information Science, University of Illinois, Champaign-Urbana.

Larry Lockway has worked in the information services for more than 15 years.

Mark Manion teaches in the Humanities Department and the College of Engineering at Drexel University. Manion's current research interests include the ethics and politics of risk assessment, the social impact of technology, and ethical issues in risk communication and crisis communication.

Barbara Rockenbach is the Instructional Services Librarian in the Arts Library at Yale University. She received her MLIS from the University of Pittsburgh.

Lawrence Ross holds a BA in Philosophy from Brown University, J.D. from the American University, Washington College of Law, and is currently pursuing his MLIS, at the University of Illinois at Urbana-Champaign.

Herman Tavani (Ph.D., Temple University) is Associate Professor and Chair of the Philosophy Department at Rivier College. He is past president of the Northern New England Philosophical Association, Associate Editor of *Computers and Society* and Book Review Editor of *Ethics and Information Technology*.

Eva Turner is Senior Lecturer, School of Computing Science, Middlesex University.