Hackers and the contested ontology of cyberspace

Helen Nissenbaum

New Media Society 2004; 6; 195
DOI: 10.1177/1461444804041445

new media & society

London, Thousand Oaks, CA and New Delhi
Vol6(2):195–217 DOI: 10.1177/1461444804041445

ARTICLE

Hackers and the contested ontology of cyberspace

HELEN NISSENBAUM
New York University

Abstract

This article analyzes the transformation in our conception of hacking over the past few decades to the current point where hackers are conceived as miscreants, vandals, criminals, and even terrorists. It argues that this transformation is more a function of contextual shifts than of changes in hacking itself. In particular, the hacker ethic, which eschews centralized, restricted access to computers and information, is inimical to the interests of established corporate and government powers, including particularly intellectual property and order. Central to this article's argument is that the transformation has been achieved not through direct public debate over conflicting ideals and interests, but through an ontological shift mediated by supportive agents of key societal institutions: legislative bodies, the courts, and the popular media.

Key words

ethics and information technology • hacking/cracking • free software • intellectual property • internet • Linux • open source • political protest

INTRODUCTION

Information technology is an arena of rapid change where much is unsettled. The technology itself has evolved at a striking pace and, in its wake, affects individual lives, societies, and political, social, and economic

institutions. Moreover, as a series of public struggles over design and policy has demonstrated, these agents are far from unanimous regarding the way in which they would judge and shape these social and technological changes. People, communities, and institutions jostle to promote their own visions, controversial policies, competing technologies, and technological standards, seeking the dominance of their own interests and values over others. Much of the contestation is explicit, public, and vocal: the fate of Napster, the digital divide, the promise (or lack) of proposed technical standards (e.g. platform for privacy preferences – P3P; and platform for internet content selection – PICS), the fair allocation of domain names, and much more.

This article brings to light a form of contestation and a form of settling disputes that is much quieter, almost invisible. And the reason for its stealthy quality is that, on the face of it, these disputes are not explicitly about the way things ought to be but about what is, the nature of the things that inhabit both the world online and a world that is increasingly ordered through information technology (IT). Nevertheless, because the results of such ontological or conceptual disputation is, or can be, ultimately normative, it is important to recognize its power and remain vigilant to its presence. One of the richest analogies to illustrate this point is that of hackers, a category that has undergone radical transformation over a period of four decades.

HACKERS: BACKGROUND

Hackers were never part of the mainstream establishment, but their current reputation as cyberspace villains is a far cry from decades past when, first and foremost, they were seen as ardent (if quirky) programmers, capable of brilliant, unorthodox feats of machine manipulation. True, their dedication bordered on fanaticism and their living habits bordered on the unsavory. But the shift in popular conception of hackers as deviants and criminals is worth examining, not only because it affects the hackers themselves and the extraordinary culture that has grown around them – which is fascinating as a subject in its own right[1] – but because it reflects shifts in the development, governance, and meaning of the new information technologies. I will argue that these shifts should not only be studied, but should be questioned and resisted.

In *Hackers: Heroes of the Computer Revolution* (1984), Steven Levy traces the roots of evolving hacker communities to the Massachusetts Institute of Technology (MIT) in the late 1950s. Here, core members of the Tech Model Railroad Club 'discovered' computers first as a tool for enhancing their beloved model railroads and then as objects of passion in their own right. These early hackers turned their considerable creative energies to the task of building and programming MIT's early mainframes in uneasy, but relatively peaceful co-existence with formal employees of the university's

technical and academic staff. In parallel, hacker communities flourished in other academic locales, particularly Carnegie-Mellon and Stanford, spilling over into nearby cities of Cambridge, Palo Alto, and Berkeley.

As formidable programmers, the hackers (who were almost always young men) produced and debugged code at an astonishing rate. They helped to develop hardware and software for existing functionalities and invented, sometimes as playful challenges, many novel algorithms and applications that were incorporated into subsequent generations of computers. These novel functions not only extended the recreational capabilities of computing and IT – gaming, virtual reality, and digitized music – but also increased practical capabilities, such as control of robots and processing speed. Obsessive work leavened with inspired creativity also yielded a host of basic system subroutines and utilities that improved operating capacities and efficiency, steered the field of computing in novel directions, and became a fundamental part of what we experience – the ubiquitous Windows interface, for example – every time we sit in front of a computer (see Raymond, 2000 for other examples of hacker contributions).

Levy and others who have written about this early hacker period (see, e.g. Hafner and Markoff, 1991; Sterling, 1992; Thomas, 2002) describe legendary hacking binges – days and nights with little or no sleep – leading to products that surprised and sometimes annoyed colleagues in mainstream academic and research positions. The 'pure hack' did not respect conventional methods or theory-driven, top-down programming prescriptions. To hack was to find a way, any way that worked, to make something happen, solve the problem, invent the next thrill. There was a bravado associated with being a hacker, an identity worn as a badge of honor. The unconventional lifestyle did not seem to discourage adherents, even though it could be pretty unwholesome: a disregard for patterns of night and day, a junk-food diet, inattention to personal appearance and hygiene, the virtual absence of any life outside of hacking. Neither did hackers come off as very 'nice' people; they did little to nourish conventional interpersonal skills and were not particularly tolerant of aspiring hackers with lesser skills or insufficient dedication.

It was not only the single-minded attachment to their craft that defined these early hackers but their espousal of an ideology informally called the 'hacker ethic'. This creed included several elements: commitment to total and free access to computers and information, belief in the immense powers of computers to improve people's lives and create art and beauty, mistrust of centralized authority, a disdain for obstacles erected against free access to computing, and an insistence that hackers be evaluated by no other criteria than technical virtuosity and accomplishment (by hacking alone and not 'bogus' criteria such as degrees, age, race, or position).[2] In other words, the

culture of hacking incorporated political and moral values as well as technical ends.

In the early decades – the 1960s and 1970s – although hackers' antics and political ideology frequently led to skirmishes with the authorities (for example, the administrators at MIT), generally, hackers were tolerated with grudging admiration. Even the Defense Advanced Research Projects Agency (DARPA), the funding agency in the US which is widely credited for sponsoring invention of the internet,[3] not only turned a blind eye to unofficial hacker activities but indirectly sponsored some of them. For example, the research that it funded at MIT's artificial intelligence laboratory was reported online in 1972 in HAKMEM, as a catalog of 'hacks' (ftp://publications.ai.mit.edu/ai-publications/pdf/AIM-239.pdf). This report is prefaced, tongue-in-cheek, as follows:

> Here is some little known data which may be of interest to computer hackers. The items and examples are so sketchy that to decipher them may require more sincerity and curiosity than a non-hacker can muster.[4]

Eric Raymond, prolific philosopher of the Open Source movement, suggests that for DARPA, 'the extra overhead was a small price to pay for attracting an entire generation of bright young people into the computing field' (Raymond, 2000).

FROM HEROES TO HOOLIGANS

Nowadays, when we hear about hackers it is usually as anti-social, possibly dangerous individuals who attack systems, damage other people's computers, compromise the integrity of stored information, create and distribute viruses and other harmful code, invade privacy and even threaten national security. They flout the law by cracking into communications networks, copying and distributing copyrighted software and other intellectual works, caring nothing for the norms of common morality. They stay up all night and take on strange and menacing names like Legion of Doom, Acid Freak, The Knights of Shadow, Scorpion, Terminus, Cult of the Dead Cow, and The Marauder. To top it off, the essential credo of old-style hackerdom – creative brilliance above all – has given way to a culture of 'script kiddies' or 'copycats', who merely mimic the technical ingenuity of a few creative hackers in order to further anti-social and often selfish ends.

In inter-office memoranda, government advisories, and stories in the popular media and trade press, systems administrators and security experts stress the need to protect vulnerable systems and users against hackers, peppering their rhetoric with cautionary tales (and all of them true): the hacker, 'Maxim', who threatened to post 300,000 stolen credit-card numbers on the internet unless the online music retailer CDUniverse paid him US$100,000; master hacker-addict Kevin Mitnick (at one point the most

wanted hacker in the world), who gained access to corporate trade secrets worth millions; the loss of a ship at sea when a hacker brought down the weather forecasting system for the English Channel, and so forth. Each story is a reminder of the damage done, the millions of dollars lost in equipment, time, and productivity, and our disturbing vulnerability; the distribution of damaging viruses such as Klez, Nimda, Melissa, and ILOVEYOU; denial-of-service attacks on Yahoo!, America OnLine (AOL); and more.

ACCOUNTING FOR THE SHIFT

What accounts for the transformation in our conception of hackers from Levy's 'heroes of the computer revolution' to white-collar criminals and terrorists of the Information Age? One straightforward speculation is that hackers themselves have changed. They no longer discriminate in their targets; they victimize not only centralized bureaucracies, which are carefully chosen for their obstruction of the 'hacker ethic', but also unsuspecting users and consumers of the digital media. Having cut themselves adrift from their idealistic moorings, they are no better than other common criminals, intruders, vandals, and thieves. We see them as villains now because now they are villains. Another speculation points not to a change in hackers themselves but to a change, largely, in us. Because our standards and values have changed, what we used to admire or tolerate we now deplore. Value shifts such as these are not unprecedented; consider the cases – more significant, obviously – of slavery, racism, sexism, sexual mores, and corporal punishment.

These suggestions hold some truth, but they form a dualism that begs for synthesis. My own account seeks such middle ground by reading the transformation against the backdrop of a shifting social context. However, before considering this account we should review two other accounts that have drawn contextual phenomena into their stories. One, offered by Deborah Halbert, hypothesizes that the shift in our evaluation of hackers is the result of a conscious movement by mainstream voices of governmental and private authority to demonize and portray hackers as abnormal, deviant bullies, who victimize the rest of ordered society (Halbert, 1997). Hackers are presented as the new enemy of the Information Age, an age in which old enemies (for example, the Soviet Union) have dissipated and the world order has shifted. Mainstream media, law, and government focus on the destructive acts of hacking in an effort to construct a new enemy and to justify systematic lines of action, such as very public indictments of particular hackers (e.g. Kevin Mitnick, Robert Morris, and Craig Neidorf).

Demonizing hackers serves two ends that are important to government and established private powers. The first is to control the definition of normalcy in the new world order of computer-mediated action and

transaction; the good citizen is everything that the hacker is not. According to Halbert:

> It is the role of the deviant to mark the boundaries of legitimate behavior. Hackers, constructed as deviants, help [to] define appropriate behavior and appropriate identities for all American citizens, especially in a computer age where ethical guidelines are still ambiguous. (1997: 362)

The second is the justification of further expenditures in security, vigilance, and punishment. To the extent that established powers can persuade us of the severity and urgency of hacker threats, they are likely to elicit support for security measures, including governmental vigilance over the internet, greater financial investment in safeguarding computer systems and information, and tougher sanctions on hackers.

In a similar vein, Andrew Ross[5] portrays the changing moral status of hackers as a cultural regrouping, with hackers pitted against the corporate and government mainstream (Ross, 1991). He suggests that, in entrenching the association between hackers and viruses, mainstream culture linked the hacker counterculture with sickness and disease, particularly with such stigmatized diseases as AIDS. According to Ross, making this link helped mainstream forces to generate equivalent hysteria in the casual user and moral indignation in the legislature. At the same time, software vendors benefited from public distrust of unauthorized copies of computer programs. In the process, 'a deviant social class or group has been defined and categorized as "enemies of the state" in order to help rationalize a general law-and-order clampdown on free and open information exchange' (Ross, 1991: 81).

As with the explanations proposed by Halbert and Ross, my own account brings into the foreground various contextual and historical factors, although it does so from a different vantage point, with some greater specificity and the benefit of a larger temporal arc. The core thesis is that changes in the popular conception of hacking have as much to do with changes in specific background conditions, changes in the meaning and status of the new digital media, and the powerful interests vested in them, as with hacking itself. Supplementing this thesis is a proposal about the mechanism by which this shift has been achieved, namely, that it is mediated through a manipulation of the ontology of cyberspace, rather than through only direct influence on policy and prescription.

HISTORICAL CONTEXT

It is generally acknowledged by IT observers and scholars that many of its significant developments were incubated in a collaboration between the military establishment (particularly through its funding agencies) and institutions of academic research, rapidly diffusing out into general use from

these specialized and closely-knit communities (see for example, Abbate, 1999; Hafner and Lyon, 1996; Rosenzweig, 2003). Writers such as John Perry Barlow, Howard Rheingold, and Nicholas Negroponte, chronicled the rapid and popular adoption of the technology through deeply optimistic interpretive frames (see, for example Barlow, 1991; Rheingold, 1993; Negroponte, 1995). Writing in the 1980s and mid-1990s, they elaborated a mythology of cyberspace – the internet and world wide web – a new frontier where great freedoms and opportunities lay, where brave (if sometimes bizarre) cowboys and 'homesteaders' would create a space distinct from conventional physical space, embodying ideals of liberty and plenty. Their work both echoed and nurtured the earlier hacker ideals.[6]

But this was only half the story; the other half is a story of normalization. Technologies of information quickly passed from early obscurity and mythological idealism into the mainstream of everyday experience and the early demographics of cyberspace, populated by the exotic constellation of camgirls, BBS (electronic bulletin boards), avatars (graphical icons representing characters in online games and other exchanges), internet service providers (ISPs), chatrooms, portals, MUDs (multi-user dungeons/domains/dimensions – online computer-managed games or structured social experience involving many players, bearing some resemblance to the game 'Dungeons and Dragons'), MOOs (multi-user object-oriented settings, a further variation of MUDs), and hackers expanded to include familiar transplants – collective and individual – from physically-bounded space. Local retailers, global corporations, credit card companies, traditional media corporations, governments (local, state, and federal), grandmothers, preachers, and lonely hearts sought their fortunes online. Pragmatic economic visions (from the likes of US vice-president Al Gore) competed with the romantic mythologies of futurists as cyberspace became increasingly domesticated, encompassing the mundane and being encompassed by it. These familiar presences, in turn, brought with them familiar practices and modes of interaction and associated norms and institutions.

By far the most vigorous and important of these transplants was the commercial marketplace and supporting institution of private property. Indeed, private property leached into and became central to all the multiple layerings of the online world, from physical infrastructure upwards. Global telecommunications corporations took over from the government agencies' possession and oversight of the fiber-optic cables, airwaves, and switches. Commercial ISPs (such as AOL) and others, including cable and phone companies, became dominant providers of popular online access. Even ubiquitous, open, non-proprietary protocols, such as TCP/IP, the fundamental building blocks of the internet and web, are threatened with replacement by proprietary standards (for a discussion of this issue, see Sandvig, 2002).

The property metaphor has also crept into the informal culture of the web. Increasingly conceived as spaces *belonging* to people and organizations, websites may be visited and viewed but largely under the terms that are defined by website owners: wander but do not touch (unless authorized), link but do not deep-link (see Elkin-Koren, 2001),[7] and receive cookies as a condition of entry. The weight of property claims in computerized environments has also tipped the balance against other claims, for example, in the case of electronic surveillance in the workplace (employers reading employee email and keeping track of their web-surfing). A survey of 1000 adults, reported by the Angus Reid Group in May 2000, found that three out of four workers believe employers are within their rights to monitor employee email and internet use at work, a dramatic turnaround from a few years before. More surprising than the result itself, however, was the robust acceptance by most survey subjects that employers' ownership over computer resources gave them the right to monitor (Friedman, 2000).

Owners of content, who for a long time have been a dominant force in more established media, are increasingly demanding in their property claims over software, images, music, movies, and other intellectual works in digital electronic form, exploiting existing laws and sponsoring new ones, such as the controversial Digital Millennium Copyright Act of 1998 in the US, which was tailored for the online environment. They lobby for international treaties that would protect their interests beyond and across national boundaries. Scholars of intellectual property law in new media, such as James Boyle (1997) and Yochai Benkler, frame this progression as a second enclosure movement, where the enclosure, this time, is not of land and physical property, but of the creations of the intellect and the digital networks across which it travels.

In other arenas besides property, computerized networks have undergone changes due to efforts at restrictive regulation: online speech, online gambling, the assignment of domain names, access itself, to name a few. Taken together, they have contributed to the transformation of a relatively intimate and mildly anarchistic environment to one governed by institutionally-imposed order. Larry Lessig has described this transformation, with some nostalgia, as the passage from Net95 – the open online world that readily evinced Barlow's new frontier – to the enclosed, gated, regulated world of Net01 (Lessig, 1999: 27).

It may be obvious how this sea-change strands hackers. While the exotic personae of cyberspace can be tolerated so long as they play by the rules of the new order, hackers are fundamentally inimical to it. The credo of their early years – which included a commitment to the free flow of information, unrestricted access to computer resources, and the idea of computer technology as an instrument of the public good – runs counter to these

rules. For corporate and government agents, this remnant of the old anarchy constitutes an unsettling threat.

SOCIAL ONTOLOGY: THE CONSTRUCTION OF SOCIAL REALITY

Before returning to the question of hackers, I would like to introduce a vocabulary drawn from John Searle's work about the nature and sources of the entities and facts that constitute social life, or what we might call a social ontology. Although the details of Searle's substantive picture fall outside the core purposes of this article, it generates a vocabulary that is useful for framing our discussion of hackers. According to Searle, it is useful to posit a social ontology, including social entities and facts, in addition to a natural ontology of natural entities and facts.[8] A social ontology (which could include, for example, money, marriage, property, and government) is defined by conventions, practices, and institutions of social life. These sets of rules, which may vary enormously in their constitution as well as degree to which they are explicitly codified, define a great variety of institutions that each define, in turn, sets of entities with particular status and functionality: a lump of metal attains the status of money and takes on particular functions, a person attains the status of president of the USA and fulfills a variety of functions that this role incurs, a ball swishing through a basketball hoop attains the status of a goal and functions to increase one team's score.

In terms of Searle's vocabulary, we would describe the decades-long developments as the emergence (or construction) of a social reality online, a variety of social institutions both quirky and conventional, and not always in easy co-existence. Each defines populations of social agents such as 'webcam girls', BBS operators, web surfers, webmasters, website owners, content owners, consumers, vendors, security agents, and so on. Beyond more-or-less explicitly-defined roles, accorded status, and function within these institutions, others evolve in natural or even subversive ways in a manner not unique to cyberspace. As in marriage, where we have not only husbands and wives, but also honeymoons, marriage therapists, and adulterers; and in property we have not only owners, buyers, sellers, and realtors, but thieves, trespassers, and so forth; in contemporary, thickly-institutionalized cyberspace, beyond the social agents mentioned above, we also have hackers. I will argue that the status of hackers in the social ontology of cyberspace is as agents who willfully defy the rules; as adulterers are to marriage, thieves to property, so hackers are to the set of interlinked institutions that have colonized the online world.

HACKERS AS BAD ACTORS OF CYBERSPACE

From the late 1950s through the mid-1980s, to be a hacker was to participate in a set of activities with a single-minded passion, to possess a set

of skills, to hold a certain set of beliefs, and to hold *to* a set of norms. Although there was no single, identifiable organization representing hackers and no formal entry requirements, there was a scattered 'association' of hackers, a sense of solidarity among comrades, a loosely-networked group and, especially when numbers were small enough, a sense that to be a hacker was to be vetted by a cohort of cultural peers. (Sterling, 1992: Part 2). As with any natural category,[9] it is possible to wonder whether one or another of these properties was essential to it, but details aside, many would have agreed that the cluster or properties picked out a readily identifiable category, or at least one identifiable by members and knowledgeable colleagues and observers.

However, with the growing importance of institutions online, and the emergence of a social ontology defined by them, hackers have taken on new significance – not as a self-identified group or subculture, but as bad-actors in the new social reality. Cast as the 'bad guys' of computerized and computer-mediated social reality, they are sociopaths, thieves, opportunists, trespassers, vandals, peeping toms, and terrorists. More than stirring negative public relations, these labels transform social meaning, refashioning the concept of hacking into one imbued with negative content. Our language is full of normative terms: 'murder' when we mean an unlawful, wicked, premeditated killing; 'theft' when we mean the wrongful taking of something that one does not own; 'weed' when we mean a wild and unwanted plant. Words such as these constrain what a speaker can say without stumbling into awkward inconsistencies; they foreclose certain moral discussions. To ask whether murder is wrong is odd, for by conceding that a killing is a murder we have already passed moral judgement. In some cases, terms such as murder, usefully enable expressive precision – in courts of law or in strong personal judgements: 'As far as I'm concerned factory owners who dump toxins into drinking water are murderers.' But in others, affixing a moral label can stunt exploratory deliberation as it does, I believe, in the case of hacking. If hackers are thieves, vandals, and terrorists, it makes no sense to ask whether hacking is good or bad, whether we are for or against it.

What I am trying to suggest is that normative disputes can be settled in at least two ways. One is to tackle disagreements head-on, debating whether a given act, decision, or policy is good or bad, acceptable or unacceptable, and so forth. But normative points can also be scored in an insidious way by somehow meddling with an ontology or conceptual schemata. Conceptual schemas carve the world into perceptible and intelligible chunks. Concepts determine ontology by individuating constitutive entities, defining what there is in our world and what, therefore, we can readily talk about. If the conception of hacker as transgressor dominates, our capacity to ask in a

meaningful way whether hacking is bad, or good, or morally neutral is limited. To call a hacker good becomes virtually oxymoronic.

In their book on classification and standardization, Bowker and Star (1999) explore this capacity of schemes of classification to serve not only epistemological ends – organizing the world into useful chunks – but also political ones. Political ends may be served when:

(1) overly inclusive categories merge differences, causing a variety of entities to appear to be of one kind and, by consequence, deserving of a common treatment;
(2) a distinctive set of marginal entities are made to disappear in a scheme that lumps them together with a dominant set (e.g. as described by Bowker and Star, the Nursing Interventions Classification was careful to include explicit categories for frequently overlooked nursing functions, such as providing spiritual support and cheering up patients through humor);
(3) borders are drawn in politically-charged ways (e.g. when a fetus is to count as a person); and
(4) important commonalities are missed – when a meaningful aggregate is disaggregated into several parts (e.g. finally recognizing a variety of activities as belonging together in the single category of 'sexual harassment'; see Bowker and Star, 1999, especially Chapter 7).

James Boyle (1997) brings to light another case where categorization carried political clout. According to Boyle, significant progress in the effort to protect the environment politically was made when proponents succeeded in classifying together in the single category of environmentalism the set of diverse concerns of nature lovers, hikers, opponents of pollution, campers, birdwatchers, conservationists, and hunters: 'in one very real sense, the environmental movement invented the environment so that farmers, consumers, hunters and birdwatchers could all discover themselves as environmentalists' (Boyle, 1997: 113). When these previously disparate groups were able to see themselves as having something in common – the environment – they could consolidate diverse streams of energy and activism (1997: 108–9).

Behind such conceptual shifts must be a diverse range of causes about which I can only speculate here. Boyle's account suggests that intellectual enlightenment was a key to the shift: namely, the discovery that two new analytic frameworks, ecology on the one hand, and welfare economics on the other, could be applied in common to apparently disparate concerns of the various interest groups. Looking for the epistemological mechanism behind the establishment of social facts, Searle posits collective assent, or

'collective intentionality' (1995: 97) which occurs when 'sufficient numbers of members of the relevant community continue to recognize and accept the existence of such facts' (1995: 117). In a similar vein, Bowker and Star stress community agency when they identify naturalization (as articulated in the field of science and technology studies), as the key mechanism by which a community ceases to think of a particular entity as artificially constructed and accepts it as an element of the natural or untheorized environment.

Although a comprehensive and systematic account of what moves collective assent (or naturalization) is, again, beyond the scope of this article, we will draw on conventional wisdom about institutional agents that have been implicated historically in shaping and changing collective conceptions of reality – namely, public policy, the courts, and of course, the media. Focusing on activity within the USA, we see Congress addressing the hacker 'problem' with the Computer Fraud and Abuse Act of 1986 which was followed by continuous refinements and increasingly harsh punishments, culminating in the Digital Millennium Copyright Act of 1998. Law enforcement agencies enforced these newly-rigorous rules in the well-publicized 'sting' operations of the 1980s, which Bruce Sterling calls 'hacker crackdowns'. Police and Federal Bureau of Investigation (FBI) agents arrested hackers and 'Phreaks' (hackers who break into telecommunications networks), confiscated equipment, and pursued public indictments of infamous hackers such as Kevin Mitnick, Robert Morris, and Craig Neidorf. Hacker arrests and incarcerations have become commonplace.

Courts have demonstrated their willingness to cooperate in such crackdowns by handing down guilty verdicts and imposing stiff punishments, from fines to jail sentences. In highly visible and expressive cases, courts shut down Shawn Fanning's Napster and prohibited publication of DeCSS, a program that decrypts DVD discs for Linux machines, in Eric Corley's *2600 Magazine* (known as a magazine for hackers). Some observers believe that the pendulum has swung too far: for example, the National Association of Criminal Defense Lawyers has argued that sentences for hackers are now disproportionately harsh (Lemos, 2003).

Finally, the media has played a critical role in bringing the matter of hacking to public attention by presenting and framing countless stories, including some that have been already mentioned earlier, about hackers sending destructive viruses, initiating denial-of-service, breaking into highly sensitive utilities of military systems, and distributing pirated software and other electronic property. According to Eric Raymond, this trend can be traced back as early as 1984, when mainstream press began covering episodes of unauthorized break-ins into computer systems and 'journalists began to misapply the term 'hacker' to refer to computer vandals, an abuse which sadly continues to this day' (see Raymond, 2000: Section 5). Samples drawn from the print media illustrate this trend:

- *The New York Times*, 13 June 1999: 'Computer hackers attacked the United States Senate's main web site on Friday, the second such electronic assault on the high profile internet page in just over two weeks.' Later in the same article: 'In an obvious taunt directed at the F.B.I. – which is conducting a national crackdown on computer hackers – they wrote on part of the page: "You can stop one, but you cannot stop all."'
- *Buffalo News*, 29 June 1999 headline: 'Web Site of U.S. Army is invaded by Hackers.'
- *Boston Herald*, 1 August 1999: 'It was the kind of threat for which computer hackers are famous, a declaration of war dripping with the risk-free bravado so common on the anonymous internet. The warning, which appeared on a hacked web page of the U.S. Interior Department in late May, promised unrelenting attacks against government computers to avenge an FBI roundup of hackers associated with the group Global Hell.'
- LA Times.com, 7 November 2000: 'A 20 year-old hacker who seized control of sensitive computer programs at the Jet Propulsion Laboratory in Pasadena and at Stanford University pleaded guilty to federal charges Monday' (http://www.latimes.com/cgi-bin/print.cgi).
- *Time* magazine (Canadian edition) 22 May 2000, headline: 'School for Hackers: The Love Bug's Manila birthplace is just one of many Third World virus breeding grounds', suggests that De Guzman, who is suspected of unleashing the virus, is an example of a growing force of hackers in the 'Third World'. Law-enforcement officials warn that 'small cells of hackers – some at colleges, others in contact only electronically – pose an unprecedented threat to the computer systems of the industrialized world . . .'.
- *San Jose Mercury News*, 10 July 2002: 'Security Flaw Afflicts Popular Technology for Encrypting Email: the flaw allows a hacker to send a specially coded email – which would appear as a blank message followed by an error warning – and effectively seize control of the victim's computer. The hacker could then install spy-software to record keystrokes, steal financial records, or copy a person's secret unlocking keys to unscramble their sensitive emails.'
- CNET News.com, 15 July 2002 headline: 'House OKs Life Sentences for Hackers: The House of Representatives on Monday overwhelmingly approved a bill that would allow for life prison sentences for malicious computer hackers . . . The CyberSecurity Enhancement Act had been written before September 11 terrorist

attacks last year, but the events spurred legislators toward Monday evening's near-unanimous vote.'

- *The New York Times*, 17 January 2003, headline: 'Increase in Electronic Attacks Leads to Warning on Iraqi Hackers and U.S. Safety.'
- *The New York Times*, 12 August 2002, headline: 'Hacker Obtains Shuttle Design Files, Baffling NASA. Cybercrime investigators for the National Aeronautics and Space Administration are trying to figure out how 43 megabytes of sensitive design data about planned space vehicles got into the hands of a hacker . . .'.
- *Washington Post*, 19 February 2003, headline: '8 Million Credit Accounts Exposed; FBI to Investigate Hacking of Database. A hacker broke into a computer database containing roughly 8 million Visa MasterCard and American Express credit card numbers earlier month, prompting an FBI investigation into one of the largest intrusions of its kind.'

A steady stream of media reports in which vandals, burglars, thieves, terrorists, and trespassers are labeled as hackers does more than shift our focus, it establishes a new prototype.[10] The more times people hear about hackers in these terms, the more they are led to see these hackers not as the exceptions but as the rule. A category shift occurs not as a result of revised formal definitions, nor at the edges where boundaries are carved, but at the center where the *typical* hacker is drawn. The accumulation of stories constructs the prototype of a newly-defined category.

We do not have to posit a massive conspiracy to understand why the media have followed this path. As Todd Gitlin has argued, established institutions (as compared with opposition movements) exert a formidable influence on the way in which the mass media construe reality (Gitlin, 1990). Besides the obvious advantages of wealth and power, established institutions are able to nominate official spokespersons who present a coordinated, authoritative account of these institutions' positions and perspectives. By contrast, opposition movements typically lack such mechanisms. Although a sense of solidarity binds together many hacker-comrades, and a dispersed, loosely-associated network of small bands convene around electronic discussion groups (such as Slashdot.com), magazines (such as *2600: The Hacker Quarterly*), and even annual conferences (such as Defcon), yielding what Bruce Sterling called a 'digital underground' (1992), there are no formal entry requirements and no organizations or individuals who stand for, or can legitimately claim to represent, *the* hacker perspective. In such circumstances, as Gitlin (1990) would predict, even when it is not explicitly manipulated by establishment voices, media presentation of hackers falls prey to serendipity and the media's taste for celebrity and melodrama.

TELEOLOGY

It remains to ask why established institutions would promote this particular transformation in the social ontology of the online world. For law enforcement and security agencies, including national security agencies, hackers represent anarchy and disobedience, and for corporate agents they represent stubborn resistance to the imposed order of private property, borders, and restricted access. Hackers are not readily 'tamed'; they explicitly eschew the rules of centralized authorities. This is a bad enough threat. How much worse if the rest of us were to identify with hackers and their 'ethic'? The 70 million people who downloaded Napster, and the even greater numbers who ignore the threats of established authorities and subscribe to filesharing services such as Aimster, Kazaa, and others, are a corporate executive's nightmare, not only because of the direct impact on the record industry's profitability and power but because they signal a normative seepage, the beginnings of shifting loyalties and commitment.[11]

Searle highlights the capacity of collective intentionality to sustain as well as to break down institutional structures, in some instances overpowering direct force itself. Pointing to the cases of the 1992 riots in Los Angeles and the dissolution of the Soviet Union, Searle speculates that the turning-points in each occurred when protesters (rioters and dissidents, respectively) induced sufficient sympathy among large portions of their respective collectives and could be relegated no longer to the status of deviants. At this point, the police could no longer sustain authority over them. When collective intentionality deserts prevailing institutional norms, when there is massive identification with radically dissident voices, then the very institutions themselves are at risk of dissolution. Although, ideally, such upheaval would become a staging ground for productive public examination of issues, norms, and policies, this has not occurred in the case of hacking. Instead, established institutions have tried to increase the distance between hackers and the rest of us by means of an ontological transformation that reconceives hackers as deviants, and hence fair targets for repression and punitive action. Such efforts seem to have gained considerable public acceptance in the wake of the 11 September 2001 terrorist attacks on the World Trade Center, at least in the short term.

Albert Hirschman's exit and voice provide an interesting framework for expressing the clash between hackers and established powers (Hirschman, 1990). Hirschman posits exit and voice as two of the ways in which people (consumers, members, clients, etc.) can try to shape business institutions, political and religious organizations, and other forms of organized community. Dissatisfaction is expressed through *exit* in such cases when customers cease to buy a product, members leave a church, participants resign from an organization, and parents remove their children from a school. According to Hirschman, *voice* by contrast involves:

> any attempt at all to change, rather than to escape from, an objectionable state of affairs, whether through individual or collective petition to the management directly in charge, through appeal to a higher authority with the intention of forcing a change in management, or through various types of actions and protests, including those that are meant to mobilize public opinion. (Hirschman, 1990: 30)

Although the ideal response to deterioration in the quality of a product or service is for organizations or corporations to heed the messages of exit and voice, according to Hirschman (1990: 93), managers tend to prefer to shun efforts to change, preferring to 'act as they wish, unmolested as far as possible by either desertions or complaints of members'. At the same time, they seek ways to make themselves less vulnerable to either forms of dissidence, by devising mechanisms for defusing the power of voice and exit, focusing on ways to 'strip the members-customers of the weapons which they can wield' (1990: 124). The possibilities that Hirschman discusses include playing collusive games with competitors to diminish the effects of exit, making exit exceedingly difficult, 'domesticating' voice, even silencing it altogether by excommunication or expulsion.

Institutional responses to hackers are illuminated well by Hirschman's framework as we can see in the case of Napster, for example. The story is familiar: in 1999, Shawn Fanning, a freshman at Northeastern University, grew dissatisfied with poor accessibility of music online. He *exited* the constraints of the music industry by hacking an alternative system of distributing music based on peer-to-peer filesharing. To date, the music industry has responded precisely as Hirschman's theory would predict, not by heeding the message of dissatisfaction but seeking what Hirschman would call excommunication and expulsion. In this case, it involved prosecuting Fanning in a court of law, signaling to one and all that exit from their system would be exceedingly costly. Their move is equivalent to pushing the protesters to the margins of good society where they can be dealt with as deviants. Another case is open-source software, which can also be read as an exit from commercialized, closed code. To date, we have witnessed two types of reactions. One, led by Microsoft, aggressively tries to quash it (make exit difficult), famously calling the open-source movement a 'cancer'. Others have tried to domesticate it by portraying the hackers of open source not as dissidents but as workers who can be folded into their system of property and control (see Wayner, 2000).

THE VALUE OF HACKING

Hirschman's framework is not purely descriptive, but conveys a strong normative message as well. The tactics that are employed by managers to avoid facing up to the substantive complaints of dissidents and deserters are shortsighted and unwise, most likely leading to the long term decline of the

organizations (firms, states, etc) that they represent. I contend that this lesson is worth heeding in the case of hackers. Although in the short-term, the ontological transformation of hackers from heroes to hooligans might suppress uncomfortable and inconvenient disruptions, the long-term effects are less clear, especially for society at large. Long term outcomes of the various blocking strategies are worth studying. To this end, I conclude the article by considering some consequences of giving way to the reformation of the concept of hacking from earlier meanings of fanatical programmer and adherent of the hacker ethic to destructive deviant, a common criminal, or even a terrorist.

The finding I wish to stress is this: although shifting the meaning of hacking does not immediately cause those identified with the earlier hacker ideology to disappear, it causes them *effectively* to disappear into what Bowker and Star call the marginal residual: namely, atypical members of a category that do not fit salient characterizations. Lodged at the margins, these hackers lose their robust identity and with that goes recognition of their ideas, ideals, and ideologies that comprise an alternative vision for a networked society. The cases outlined below illustrate the valuable contributions that these hackers have made to society and, by inference, what we stand to lose as they are pushed into the margins.

Most significant, perhaps, are the remarkable technical contributions that self-identified hackers have made outside the framework of the commercial marketplace. Many scoffed when Richard Stallman and his followers in the Free Software movement (quintessential hackers in the old sense) insisted that software should be free – 'as in speech,' Stallman regularly quips, 'not beer' – but the enormous body of free software, including Linux, poses a formidable challenge to glib truisms about intellectual property and innovation. In referring to the origins of the phenomenal open source movement, Eric Raymond notes that 'the hacker culture, defying repeated predictions of its demise, was just beginning to remake the commercial software world in its own image' (Raymond, 2000; see also Wayner, 2000). Hacker ideology also inspired such luminaries as Tim Berners-Lee, dubbed 'the inventor of the world wide web'. In his account of constructing a remarkable global information system, he has situated his efforts within the purview of projects and ideologies of such early hackers as Ted Nelson (Berners-Lee and Fischetti, 1999). The contributions that hackers have made to social welfare extend beyond free code to include access to technology and information; Raymond writes, 'many of the hackers of the 1980s and early 1990s launched Internet Service Providers selling or giving access to the masses' (Raymond, 2000: Section 7).

Hackers have also contributed in the political arena, supporting causes of liberty and individual autonomy in policies involving IT. In 1994–95, for example, they were part of the concerted opposition to the Clinton

administration's misguided Clipper proposal, which would have limited individual access to strong encryption. In 1996, they joined the broad coalition opposing, and ultimately defeating, the Communications Decency Act, on the grounds that it would lead to unacceptable censorship of the internet.

Generally, hackers have also contributed to efforts against political oppression, devising ingenious forms of political protest. In an historic case in 1998, 'hactivists' supporting Mexican Zapatista rebels developed Floodnet, a coordinated bombardment of client-requests which temporarily shut down the website of Mexican president Ernesto Zedillo. The attack was carefully planned and controlled in the tradition of peaceful civil disobedience not to destroy but, as described by Ricardo Dominguez, one of its leaders, 'To create a disturbance that becomes symbolic, so a certain community can gain a voice in the media' (Ricardo Dominguez quoted in Romano, 1999).[12] More recently, hackers have focused attention on the growing presence of video surveillance technologies in private and public spaces. For example, the hacktivist group Institute for Applied Autonomy, charts the routes of least surveillance through Manhattan streets, and an anonymous website (http://rtmark.com/cctv/) offers advice on how to disable surveillance cameras. The journalist Stuart Millar (2001: 4) has characterized hacktivism as a 'highly politicized underground movement using direct action in Cyberspace to attack globalization and corporate domination of the internet', and, as such, an ideological heir to the great protest movements of the 19th and 20th centuries.[13]

If there is something political that ties together these descendents of early hackers, it is protest – protest against encroaching systems of total order where control is complete, and dissent is dangerous. These hackers defy the tendencies of established powers to overreach and exploit without accountability. With their specialized skills, they resist private enclosure and work to preserve open and popular access to online resources, which they consider a boon to humanity. Ornery and irreverent, they represent a degree of freedom, an escape hatch from a system that threatens to become overbearing. In societies striving to be liberal and democratic, this is a significant part of the value of hacking and an important reason to resist obfuscation of the category.

However, it is important to note that sustaining the positive meaning of hackers does not require denying or turning a blind eye to those who turn their skills and know-how towards stealing information or money, damaging and vandalizing information or systems, or placing critical systems at risk of malfunction. We deplore these actions, just as we would deplore any actions that deliberately harm others. Nevertheless, the problematic consequence of viewing these actors as prototypical hackers is that it marginalizes the

remainder; they are 'left dark' (Bowker and Star, 1999: 321) without a robust presence in the social ontology of cyberspace.

CONCLUSION

Recognizing, as others have done before, the transformation in the way hackers are viewed, I have argued that it is not merely a matter of a change in evaluative judgements of hackers and hacking, but in the very meaning of the terms. Hacking is now imbued with a normative meaning whose core refers to harmful and menacing acts, and as a result it is virtually impossible to speak of, let alone identify, the hackers that engage in activities of significant social value. Because the old hackers eschewed centralization of authority and invasive property boundaries, the ontological shift is convenient for those who seek to establish control in the new order and economy of cyberspace. Not only does it vilify early hackers by association with evil hackers, but it becomes virtually impossible even to perceive them, for we have lost the vocabulary with which to identify them. As a collateral loss, it is harder to deliberate over the conflicting substantive principles.

Concepts carve the world into meaningful chunks and serve particular ends, whether they are explicitly crafted, as the case of the International Classification of Diseases (Bowker and Star, 1999), or emerge naturally as the meaning of everyday language. As Searle (1995: 4) remarks, 'social reality is created by us for our purposes and seems as readily intelligible to us as those purposes themselves'. In the extreme, the evolution of appropriate conceptual schema may even be seen to serve the flourishing of a species, for example, as some have suggested in the case of vervet monkeys that are able to warn troop members about the presence of predators with special 'words' conveying something about the nature of these predators – whether airborne (say an eagle) or terrestrial (say a snake). (Cheney and Seyfarth, 1990).[14]

In this sense, our concepts are teleological, not only shaping our thoughts and utterances but facilitating, making awkward, or even depriving us of the facility to think and talk about certain things. In some cases, such as the vervets' refined conception of predators, these conceptual schema serve shared or common ends within a community of agents, thinkers, and speakers. But this is not universally true of all conceptual and classification schema which, as discussed above, may favor some members' interests at the expense of others. In this way, by skewing the meaning of hackers, established institutions of cyberspace have enlisted the power of conceptual schema in their quest for order and control. The recognition of contested ends is partly what impassions Bowker and Star, when they declare:

> One of this book's central arguments is that classification systems are often sites of political and social struggles, but these sites are difficult to approach.

> Politically and socially charged agendas are often first presented as purely technical and they are difficult even to see. (Bowker and Star, 1999: 196)

I have argued that we are not all well served by the transformation of 'hacker' into a category which includes only at its edges those who espouse the hacker ideology (or, 'hacker ethic'). These hackers have much to offer to individual users of cyberspace, and ultimately, to contribute to the public good. Nevertheless, to many of the institutions invested in strong property rights and traditional ordering, even these hackers constitute a threat. They challenge institutional strongholds and are sufficiently skilled at manipulating the underlying technologies to meet their ideological commitments. All the better if this irksome group and its causes would fade from public consciousness into the margins of a larger category typified by vandals, terrorists, and criminals. All the better for the institutions if they can craft an enemy in common with individual users and consumers so as to subordinate *all* who might challenge them.

Computers and the internet have extended our modes of association, action, expression and access to information, and have conjured into existence many wondrous entities and interactions. The precise nature of these entities is not always understood, and questions about them arise that have implications for policy and values – questions such as: what is a border in cyberspace? Where are the edges of a hypertext document? What is it to be an owner of something online? What is public; what is private? What is identity online; what are identities? Is virtual friendship, friendship, virtual war, war, virtual sex, sex? As with the question about hacking, these ontological questions have normative implications. The general thesis of this article, with implications beyond hacking, is that questions such as these – about what there is online – can be seminal to basic concerns about what ought to be.[15]

Acknowledgements

This article has incubated over a long period, originating with Jeroen van den Hoven's invitation to a July 2000 Conference on Social Ontology, Erasmus University, Rotterdam. Versions were also presented at Carnegie-Mellon University and at the Institute for Advanced Study, Princeton, NJ, and a short version was prepared for *Dissent* magazine. Along the way, I received invaluable research assistance and editorial and substantive advice from: Robert Cavalier, Brian Cogan, Debra Keates, Eben Moglen, Maxine Phillips, Greg Pomerantz, James Rule, Michael Walzer, audiences at the various venues where the article was presented, and, not least, the editors and anonymous reviewers of this journal. Work on this article was supported by the National Science Foundation, Grant SBR-9729447.

Notes

1 See, for example, interesting work by Douglas Thomas (2002), P. Himanem (2001), and W. Schwartau (2000).
2 See Levy (1984), especially Chapter 2.

3 See, for example, historical accounts in Rosenzweig (2004) and Hafner and Lyon (1996).
4 Thanks to Greg Pomerantz for directing me to this delightful document.
5 An anonymous reviewer helpfully drew my attention to this work.
6 For example, Barlow's 'Coming into the Country' (1991), Rheingold's *The Virtual Community: Homesteading on the Electronic Frontier* (1993), and Negroponte's *Being Digital* (1995).
7 To deep-link is to bypass the front page of a website, linking directly to desired content on another page within it, for example, bypassing *The New York Times* front page and linking directly to a particular story. Owners of commercial websites fear the loss of revenues from advertisements on their front-page portals and argue that deep-linking constitutes a copyright violation.
8 Some readers of this essay have claimed this to be an unconventional usage of 'ontology'.
9 Here I depart from Searle's usage. Searle uses natural ontology as a contrast with social ontology. I am invoking more standard usage here, referring to natural categories as contrasted with artificially constructed categories and classification schema.
10 One of the fundamental questions asked by cognitive scientists is how people categorize or conceptualize their worlds. Eleanor Rosch rose to prominence in the field by articulating 'prototype theory' as a compelling answer to this questions. George Lakoff, Mark Johnson, John Taylor, and others have developed and extended this theory into neighboring fields such as linguistics. In addition to developing the theory, Rosch and others have generated a formidable body of confirming experimental results. For my purposes, it is sufficient to note about prototype theory that it offers an alternative view of categorization to the Aristotelian idea that members of a category share a common set of necessary and sufficient, or defining, properties. Instead, Rosch argues that most, if not all, natural categories have fuzzy borders and, typically, no set of properties that all members share in common. She suggests that for these categories, we hold a prototype in mind and move from the prototype to other members of the category by analogy.
11 Specific legal considerations are based on the US context and might be different in relation to the legal codes of other countries.
12 See also http://www.eco.utexas.edu/Homepages/Faculty/Cleaver/chiapas95.html and http://www.eco.utexas.edu/Homepages/Faculty/Cleaver/chiapas95.html for further documentation of this case.
13 And still, there are those driven simply for the love of the pure hack, such as Robin Malda (one of the founders of Slashdot) who writes on his homepage: 'The Internet: What can I say? I'm an addict. The 'net for me was the point for computers . . .' (see http://cmdrTaco.net/rob.html).
14 I thank Dan Rubenstein for pointing me to this reference.
15 Said in respectful disagreement with G.E. Moore's naturalistic fallacy.

References

Abbate, J. (1999) *Inventing the Internet*. Cambridge, MA: MIT Press.

Barlow, J.P. (1991) 'Coming Into the Country', *Communications of the ACM* 34(3): 12–21.

Berners-Lee, T. and M. Fischetti (1999) *Weaving the Web: the Original Design and Ultimate Destiny of the World Wide Web by Its Inventor*. San Francisco, CA: HarperCollins Publishers.

Bowker, G.C. and S.L. Star (1999) *Sorting Things Out: Classification and its Consequences*. Cambridge, MA: MIT Press.
Boyle, J. (1997) 'A Politics of Intellectual Property: Environmentalism for the Net', *Duke Law Journal* 47: 87–116.
Cheney, D.L. and R.M. Seyfarth (1990) *How Monkeys See the World: Inside the Mind of Another Species*. Chicago, IL: University of Chicago Press.
Elkin-Koren, N. (2001) 'Let the Crawlers Crawl: On Virtual Gatekeepers and the Right to Exclude Indexing', *Dayton Law Review* 26: 180–209.
Friedman, S. (2000) 'Most Workers Don't Mind Workplace Online Monitoring – Poll', Newsbytes, URL (consulted 3 May 2000): http://www.newsbytes.com/pubNe ws/00/148466.html.
Gitlin T. (1990) *The Whole World is Watching: Mass Media in the Making and Unmaking of the New Left*. Berkeley, CA: University of California Press.
Halbert, D. (1997) 'Discourses of Danger and the Computer Hacker', *The Information Society* 13: 361–74.
Hafner, K. and M. Lyon (1996) *Where Wizards Stay up Late: the Origins of the Internet*. New York: Touchstone Books.
Hafner, K. and J. Markoff (1991) *Cyberpunk: Outlaws and Hackers on the Computer Frontiers*. New York: Simon and Schuster.
Himanen, P. (2001) *The Hacker Ethic and the Spirit of the Information Age*. New York: Random House.
Hirschman, A. (1990) *Exit, Voice and Loyalty: Responses to Decline in Firms, Organizations, and States*. Cambridge, MA: Harvard University Press.
Lakoff, G. and M. Johnson (1980) *Metaphors We Live By*. Chicago, IL: University of Chicago Press.
Lemos, R. (2003) 'Lawyers: Hackers Sentenced too Harshly', CNet News.com, URL (consulted 20 February 2003) http://news.com.com/2100-1001-985407.html
Lessig, L. (1999) *Code and Other Laws of Cyberspace*. New York: Basic Books.
Levy, S. (1984) *Hackers: Heroes of the Computer Revolution*. New York: Doubleday.
Markoff, J. (1993) 'Keeping Things Safe and Orderly in the Neighborhoods of Cyberspace', *The New York Times*, 24 October, p. E7.
Millar, S. (2001) 'For Hackers, Read Political Heroes of Cyberspace!', the *Guardian*, 8 March, p. 4.
Negroponte, N. (1995) *Being Digital*. New York: Knopf Publishing Group.
Raymond, E. (2000) 'A Brief History of Hackerdom', 17 November, revision 1.24, URL (consulted 17 November): http://catb.org/~esr/writings/hacker-history/.
Rheingold, H. (1993) *The Virtual Community: Homesteading on the Electronic Frontier*. New York: HarperCollins.
Romano, M. (1999) 'The Politics of Hacking', *Spin* (November): 168–74.
Ross, A. (1991) *Strange Weather: Culture, Science and Technology in the Age of Limits*. London: Verso/New Left Books.
Rosenzweig, R. (2004) 'How Will the Net's History Be Written? Historians and the Internet', in H. Nissenbaum and M. Price (eds) *Academy and the Internet*. New York: Peter Lang Publishing.
Sandvig, C. (2002) 'Communication Infrastructure and Innovation: the Internet as the End-to-End Network that Isn't', paper presented at the American Association for the Advancement of Science Research Symposium with the Next Generation of Leaders in Science and Technology Policy, 23 November, Washington, DC (available at: http://research.niftyc.org/Communication_Infrastructure_and_Innovation.pdf).

Schwartau, W. (2000) *Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists, and Weapons of Mass Disruption*. New York: Thunders Mouth Press.
Searle, J. (1995) *The Construction of Social Reality*. New York: Free Press.
Sterling, B. (1992) *The Hacker Crackdown*. New York: Bantam Press.
Taylor, J.R. (1995) *Linguistic Categorization: Prototypes in Linguistic Theory* (2nd edn). Oxford: Clarendon Press.
Thomas, D. (2002) *Hacker Culture*. Minneapolis, MN: University of Minnesota Press.
Wayner, P. (2000) *Free for All: How Linux and the Free Software Movement Undercut the High-Tech Titans*. New York: HarperBusiness.

HELEN NISSENBAUM is Associate Professor of Culture and Communication and Computer Science, and Senior Fellow of the Information Law Institute, New York University.
Address: Department of Culture and Communication, New York University, 239 Greene Street, 7th floor, New York, NY 10003, USA. [email: Helen.nissenbaum@nyu.edu]