

**Muckraking in the Digital Age:
Hacker Journalism and Cyber Activism in Legacy Media
([pdf version](#))**

[Bret Schulte](#)

University of Arkansas

[Stephanie Schulte](#)

University of Arkansas

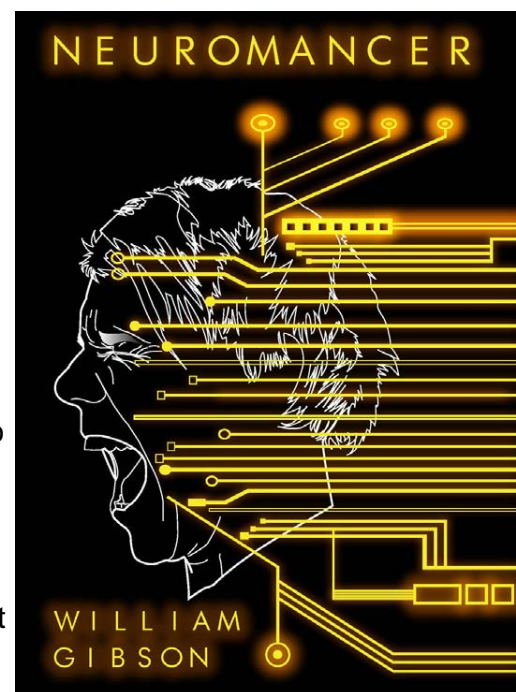
Abstract

This article traces the legacies and cultural contexts of the growing hacker journalist movement, combining historical analysis with interviews of hackers themselves. Hacker journalists, computer programmers who assume roles as journalists in order to affect social change, are at once data miners, news producers, and idealistic computer vigilantes pushing a renaissance of cyberactivism. Hacker journalism is becoming institutionalized. Hacker journalists are “hacking” into legacy news establishments. But they are also hacking into cultural tropes of “hacking” itself, re-appropriating the term “hacker.” Early hackers operated under a particular moral code, a “hacker ethic,” and, steeping their activities in Americanism, they imagined themselves “console cowboys” settling the new digital frontier. Hacker journalists gather at “hackathons” to work toward change in real and virtual worlds. An answer to Silicon Valley’s capitalism, hacker journalists pursue non-monetary rewards and seek personal fulfillment through moral interventionism. Hacker journalism exists in a tense relationship to information: Hacker journalists are themselves deregulating information flows, but at a time when economic deregulation is, paradoxically, facilitating the reaction of multimedia conglomerates that are also privatizing information. Hacker journalists emerged in a moment characterized by anti-media and anti-government (Tea Party) and anti-corporate (Occupy Wall Street) movements as well as by idealistic notions of participatory culture and citizen journalism. Traversing many conflicting ideologies—conservative, libertarian, socialist, post-capitalist—these hackers offer informational efficiency, governmental and corporate accountability, and “Do It Yourself” empowerment to citizens but risk changing the foundations of journalism, a historic pillar American democracy.

Keywords: hackers, journalism, media, information, technology

Introduction

In 2010, researchers estimated that society produced as much information in two years as it did between the dawn of humankind and 2003 (Siegler, 2003). With information streaming out of foreign and domestic institutions, newsgathering traditions left many journalists unprepared. While technology made some elements of reporting easier, one reporter noted, “What remains difficult is filtering, scanning and picking out novel signals: the far-out stuff that the net, en masse, would never find on its own”



(O'Brien, 2011, p. 10). By developing digital means to understand, translate, manipulate, and consolidate information to be consumed or re-purposed by distinct audiences, hacker journalists are not only news reporters but also architects of novel information platforms. This article investigates the evolution of so-called [hacker journalism](#) the self-given name of computer programmers who assume roles as journalists to affect social change. They are at once data miners, news producers, and idealistic vigilantes pushing a renaissance of individualist cyberactivism. In this sense, hacker journalists resemble Digital Age muckrakers in the ways they combine the libertarian and utopian [Hacker Ethics of the 1980s](#) and 1990s with the high calling of journalism as civic watchdogs. Many hacker journalists now work within institutionalized news production, where they provide journalists and news consumers tools with which to cope with the digital era's information overload. Hacker journalists are idealistic. They believe they can make government and corporations more transparent, empower news organizations with new weapons of inquiry and new wares to sell, and promote a more informed and active citizenry.

To do this, this article combines interviews with hacker journalists and scholars alongside history and theory scholarship. First, the article explicates the historical and cultural legacies of hacker journalism. Second, it contextualizes the movement by differentiating it from related movements such as computer-assisted and open-source journalism. Finally, this article theorizes hacker journalism's critique of both traditional media and democracy, illustrating the ways the movement works to reinvigorate computer culture's past to redefine journalism's future. Hacker journalism movement reveals dominant assumptions about the relationship between technology, journalism and democracy. In deeming both journalism and democracy as problematic, or in computerese as "problem spaces," in need of technological fixes, hacker journalists work to affect change by merging analog and digital worlds, computer programming and journalistic practices. Ultimately, this article illustrates the problematic and paradoxical ways that contemporary cultural critiques remain primarily focused on journalism and democracy, but not on the technology assumed central to the future health of both journalism and democracy.

Hacking The System: Hackers, hacks, and hacker journalists

As Steven Levy (1984) famously wrote, in the early days of “hacking” the term did not indicate criminal activity but described solving a computer problem cleverly. The term “hacker” originated at MIT in the 1950s as a name for computer users who best understood the technology’s revolutionary potentials. In the 1970s, hacking began to indicate romantic passion and a higher calling, or “to distinguish obsessive and unplanned work styles from those that were rigorous and carefully planned” (Streeter, 2011, p. 90). Over time, hackers developed a moral code that Levy called a “Hacker Ethic,” which advocated unlimited computer access, setting information “free,” and mistrusting authority. Hackers were deemed heroes not “because they struck it rich but because of their passion and technical contributions” (Streeter, 2011, p. 90).

Although the hacking phenomenon originated in recognized institutions such as [MIT](#), historically hackers chose to remain ideologically outside institutional frameworks. They reveled in rebellious identities, steeped their activities in Americanism as they imagined themselves “console cowboys” settling the new digital frontier (Schulte, 2013). As Fred Turner (2006) argued, hackers believed in “techno-libertarianism” (p. 259). The Hacker Ethic eschewed affiliation and organizations, insisting instead that labor “be organized in a decentralized manner and that individual ability, rather than credentials obtained from institutions, should determine the nature of one’s work and one’s authority.” In this model, “information was to circulate openly through the community of hackers, simultaneously freeing them to act as individuals and binding them in a community of like minds” (Turner, 2006, p. 135). Hackers appropriated and popularized the term “cyberspace” from William Gibson’s (1984) science fiction novel [Neuromancer](#), further signify the ways they imagined the internet as a space of self actualization and liberation. Thus, original hackers and their ethic helped both formulate and promote the cybercultural fantasies that dominated in the 1980s and 1990s, which imagined post-national, post-capitalist futures of disembodied cybercitizens building, traversing, and settling a new digital frontier.

Although hackers fancied themselves iconoclasts, their rebelliousness also ultimately solidified a vision of popular dissent that was perhaps paradoxically crucial to mainstream American-style democracy and capitalism (Medovoi, 2005). Hackers are renown for their anti-corporate activities—in particular for violations of corporate copyrights and privacy rights—but the rise of hackers in the 1980s and 1990s paralleled the rise of American corporate power and global economic dominance. In many ways the cultural work done by early hackers enabled the ascension of American corporate power (Ross, 2000). Some individuals, such as Steve Jobs, came from within hacker ranks, capitalizing on the rebellious image of hacking and of the counterculture to sell computing and networking technologies (Schulte, 2013). By capitalizing on hacker visions of the internet as rebellious, democratic, self-actualizing, and liberatory, individuals like Jobs masked the global enforcement of American corporate power (Schulte, 2013). In short, hackers were a community of rebels, but their rebellion was crucial to a certain manufactured consent about corporate prosperity in the 1980s and 1990s. Thus, historically hacking has signified both “bad” and “good” entrepreneurialism.

This signification made “bad” hackers the regulatory targets while corporations and the U.S. government paradoxically exploited the innovations produced by hackers in the service of soaring profits and global economic influence (Medovoi, 2005; Ross, 2000; Turner, 2006). The ideologies (and practices) of “freeing” information and decentralized labor caused hackers to tangle with

authority, souring public positive connotations of “hacking.” As rebels, hackers imagined authorities commodifying information (i.e. copyright) as impeding the public good. Through the 1980s and 1990s, a “hacker underground” emerged amongst individuals, who imagined themselves “an anarchistic elite.” Using names like “Master of Deception,” they cracked into telephone, credit card, and military networks, attacking corporate and government organizations alike. High-profile cases—including the 1994 “infamous hacker” Kevin Mitnick case—resulted in Congressional hearings (Freedman, 2005, p. 173; Schulte, 2013). The hacker-as-criminal frame dominated news media coverage thereafter. Other early hackers such as Steve Jobs, however, effectively distanced themselves from the tainted label, transforming themselves from rebel into entrepreneurs and venture capitalists.

Understanding both these cultural and corporate legacies of historical hackers is important to understanding today’s incarnations of hacking. “Hacker journalism,” in particular, comes from [Brian Boyer](#), a computer programmer dissatisfied with corporate work who says he found his true calling in journalism (Boyer, 2010). As the news application editor for [The Chicago Tribune](#), he created a number of service-journalism programs for the Tribune website. On one occasion, he saw reporters struggle with 44,000 documents related to a nursing home investigation. Boyer wrote a program to scan the documents for key words, then built a searchable [database](#) for the Tribune website that allowed readers to find reports of crimes, health violations and the number of resident felons (Schulte, 2011). Hacker journalists, Boyer says, “have one goal: impact,” he says. “The more [data] you give out, the wider you can spread the message” (Boyer, 2010). Thus, hacker journalists revive the idealistic and libertarian origins of hacking and do so by deliberately sacrificing big computer industry paychecks. These hacker journalists found that the most idealistic elements of their code also exist in journalistic values, such as a belief in freedom of information and holding the powerful accountable. Through journalism, programmers are finding that they can manipulate more than data or cyberspace. By engaging journalism, hackers realize the hacker ethic of leveraging computers to affect social change, empowering individuals through informational access and enabling them to speak truth to power. For example, Boyer’s searchable tool allows citizens to investigate the records of every nursing home in Illinois. His platform, along with the accompanying [print stories](#), led to an overhaul of how Illinois regulates institutionalized care for the elderly. Furthermore, a new law required that the state replicate the searchable tool created by Boyer on its own government website. He called it the most important work of his career (Boyer, 2010).

Historical hackers and their contemporary counterparts converge and diverge in key ways. In an interview, Boyer mentioned having read Gibson’s science fiction, which became a central cultural trope for hackers of yore. However, Boyer does not share the same disembodied cyberculture fantasies of historical hackers. These contemporary hackers want to change the analog world, not escape it. Their fantasy is not a virtual commune made of information, but instead embodied intimacy and communal information that serve the public good. For hacker journalists, there is one central question, Boyer said. “Is this work making the world a better place” (Boyer, 2010)? In addition, hacker journalists are increasingly operating inside major American legacy institutions instead of dismantling them or innovating competitively outside them. Thus, programmers like Boyer are not only hacking into journalism and traditional news establishments, they are also hacking into cultural tropes of “hacking” itself. By re-appropriating the term “hacker,” these journalists explicitly engage a deep history of computer culture and revive the historically idealistic visions of hackers, but rather than the iconoclasm of their predecessors, hacker journalists deviate by massaging established systems of power. This works within the manufactured consent about computing as value-neutral, as increasing efficiency and transparency, and as entrepreneurialism that helps smooth the destructive fissures of capitalist expansion.

The institutionalization of hackers in journalism is likely to increase. One journalist noted, “Large forces in the traditional world of journalism are betting that technologists and reporters work together in the future more than they work against each other” (O’Brien, 2011, p. 10). The “gamblers” include the [Knight Foundation](#), which funded a program at Northwestern University that gave big scholarships

to computer programmers willing to pursue a master's in journalism; Boyer was in the first class in 2009. The scholarships were funded through [Knight's News Challenge Grants](#), which aim to "accelerate media innovation by funding the best breakthrough ideas in news and information" and "seeks new ways to meet community information needs in the digital age" ("About," 2012). The Northwestern University grant was the result of years of frustration trying to turn journalists into programmers, according to Rich Gordon, a professor and Director of Digital Innovation at Northwestern. His grant-winning application reversed the idea by turning programmers into journalists. "When this program was announced [in 2007], the prevailing response was, 'This is a kind of joke,'" Gordon said. "Now, three or four years later, this is almost a mainstream idea" (Gordon, 2010). Gordon cites [Columbia University's](#) dual journalism and computer science master's degree as an example of how journalism education is better serving an industry desperate for computing help.

Although increasingly institutionalized, hacker journalism retains a social-movement element: "Hacks/Hackers." This social movement plays not only on the history of hackers, but also on the history of the "hack," a derivation of the word "hackney" that refers to a person writing (badly and often shamelessly) for money. This creates a whimsical double-entendre for computer programmers who take up journalism. The [Hacks/Hackers](#) movement, co-founded by Gordon, unites traditional journalists and programmers in chapters across the United States and Canada. They hold "hackathons," in which they collectively work toward real world change. One Ottawa chapter meeting attendee described the symbiotic relationship between programmers and journalists: "Hacks are good at: discerning news from info, interviewing subjects, providing context, writing, offering a big platform. Hackers are good at: obtaining data, processing it, analyzing it, building better platforms to present it" (deVilla, 2011). Hacks/Hackers and hacker journalists share a goal: to change the shape of public information by becoming "hacking hacks." They also share a dream with each other and with hackers of yore: empowered, informed citizens liberated through information technology.

The Information Glut: Computer-assisted reporting, database and open-source journalism

The hacker journalist's historical and cultural roots lie not only in the hacker and the hack, but also in the long-standing use of computing in journalism. Since the 1970s, computer technologies have streamlined journalism. Indexed databases of what was called the "news morgue," or the reference works collection in a newspaper office, meant journalists could search deep story archives in seconds for the first time. The technology not only changed researching practices for existing stories, it prompted journalists to begin using computers to generate stories. This technological shift ushered in "computer-assisted reporting" (CAR) and "database journalism," or "the science of sifting through information to deliver informative reports" (Moynihan, 2010, p. 17).

Data journalism made for good copy. Several high profile data journalism successes in the 1980s ushered in a period of optimism about the revolutionary potential of entrepreneurial journalists using computers in the news production process. For example, The Atlanta Journal and Constitution series, "[The Color of Money](#)," "showed that whites were at least five times as likely to get home loans as blacks." Less than two weeks after the stories ran, banks made \$65 million available to black neighborhoods in Atlanta (Miller, 1988, p. 35). As Miller noted, "computer analysis was crucial to the authority of the series," in particular because the investigation used the bank's data sets, but analyzed them along racial valences. Computers allowed journalists to expand their watchdog roles and to produce sexy stories that exposed systematic and corrupt practices in private and public sectors.

In spite of their potential to revolutionize reporting practices, computing systems in this era remained costly and difficult to use. In the 1980s, newsrooms needed \$10,000 to set up a "microcomputers system" and data sets on "tapes" cost extra (Miller, 1988, p. 38). Even in the mid-1990s, when computing became more cost-effective, the technology was neither user-friendly nor efficient. For instance, one journalist "started a database search" as he left at night hoping for data in the morning.

Sometimes he had “six computers, side-by-side, all tied up in the newsroom” as he struggled to manage the “huge masses of information” that, for example the Food and Drug Administration (FDA) “dumps” online. Eventually, he exposed drug companies exploiting the FDA’s “weak” authority over advertisements, but even his successful stories could take months of tedious work and costly computing resources (Adams, 2003, 12-13). Editors accustomed to daily deadlines were impatient with the pace and cost, and they were skeptical of the results. Furthermore, reporters often struggled to find a narrative among the numbers that would maintain a reader’s interest. As a result, news media were slower than other industries to incorporate computing. Author Philip Meyer lamented this. “A whole generation of editors had to die off before [computer-based journalism] could really catch on” (Miller, 1988, p. 36, citing Meyer).

By the late 1990s, journalists began using computers to incorporate news consumers into the production of news itself. Often called the “open-sourcing” of news, this tactic is related to but distinct from computer-assisted or database reporting. “Open sourcing” has a long history in the public production of knowledge. The Oxford English Dictionary was to some extent “open sourced” after 1857, when volunteers “provided lexicographers with quotations that show words’ usage” (“Hacker,” 1999, p. 66). Open sourcing, according to Siva Vaidhyanathan (2012), is “closer to how human creativity has always worked” and was “the default,” the privatization of information has, however, erased collective memories of “tools and habits unencumbered by high restrictions on sharing, copying, customizing, and improving” (p. 24).

The open-source movements in the 1990s were actually a reemergence of a set of principles originating as far back as the integration of hacker ethics into computer technology development in the 1970s (Vaidhyanathan, 2012, p. 26-27). By the 1990s, the movement gathered steam as hackers collectively “struggled to build the holy grail of free software: an operating-system kernel that would allow an array of programs to work in coordination.” The resulting program, Linux, became “the chief threat to the ubiquity and dominance of Microsoft” (Vaidhyanathan, 2012, p. 26-27, citing Benkler, 2002, p. 372-373). [Linux](#) is open source, open application. Its ethos of collective betterment and utilitarianism through collective computing means, in some respects, Linux is the embodiment of the Hacker Ethic. As Yochai Benkler has noted, although participants in Linux are by no means anti-capitalist, “the critical mass of participation in projects cannot be explained by the direct presence of a command, a price, or even a future monetary return” (Vaidhyanathan, 2012, p. 26-27, citing Benkler, 2002, p. 372-373). Hacker ethics, romanticism and open-source ideals “disarticulated the metaphor of the market from conventional capitalist modes of production and reconnected it with a form of voluntary labor, of labor done for its own sake” (Streeter, 2011, p. 158). Even as the internet financial bubble inflated, the hacker legacy ensured cultural space for desires outside money, such democratic participation, social justice or governmental and corporate transparency.

If Linux was a touchstone in open-source computing, [Slashdot.org](#) is a touchstone for open-source journalism. In the 1990s, Slashdot.org offered a “news for nerds” section of user-generated content. As with Linux, Slashdot users were motivated by non-monetary extrinsic rewards. Users, especially hackers, wanted cultural capital, or recognition as a “high-quality ‘poster’” and the “admiration of other hackers and techie editors” (“Hacker,” 1999, p. 66). Journalists began “soliciting feedback” from the “geeks who hang out” on Slashdot. This combination of open-contribution platforms plus journalistic interaction meant Slashdot was “heralded as a flagbearer for a new kind of journalism,” whose value came from “concentrating so much expertise in its commentary sections, and by centrally aggregating so many useful links to news stories” (Leonard, 1999). It became an hourly “must stop” for technology journalists (Leonard, 1999). Key to open-source journalism was a sort of intellectual populism, one that valued stories that “bubble up from the masses rather than being imposed by smart-aleck media types” (Kurtz, 2004, p. C01).

Journalism as “Problem Space:” Hacker journalism’s technological fix for democracy

Computer assisted reporting/database journalism, open-source journalism and hacker journalism—three discrete but related concepts and practices—emerged as means to address a common problem: making sense of information in the digital age. Hacker journalism develops as legacy news media organizations perceive an existential crisis. Dan Gillmor, [Center for Citizen Media and Knight Center for Digital Media Entrepreneurship Director](#), cites many reasons for the industry's financial distress, including the "arrogance built up over years of monopoly and oligopoly practices" in media institutions (Hogg, 2009). As Herbert Gans noted in the 1980s, journalists often wrote not with their audience members in mind, but "for their superiors and themselves," assuming that "what interested them would interest the audience" (Anderson, 2012, p. 78, citing Gans, 2004, p. 229-230). This practice emerged, according to Gans, in part because of the difficulty in conceptualizing aggregated individuals and in part because journalists trusted their own news judgment over consumers'.

Clearly the interactivity offered by the internet provides journalists with greater insight into the desires and practices of audience members. Consumers may not only help journalists produce the news through open-source journalism, they may also become news producers themselves, independent of news industries. Technological developments such as [Blogger](#) in 1999 allowed individuals to easily become publishers or "prosumers" in which "producers" and "consumers" hybridized (Bruns, 2008, p. 11; Drezner, 2008). Indymedia advocated consumers to "Don't hate the media, become the media" (Anderson, 2012, p. 82). These citizen journalism movements built on (and reinforced) assumptions that internet technologies were essentially democratizing. Communication researcher C.W. Anderson noted that "audience responsiveness is represented as a democratic advance" and the "increasing journalistic attention paid to audience wants framed as concomitant with the general democratizing trends afforded by the internet" (Anderson, 2012, p. 77). This shift matters because the ways in which journalists conceptualize audiences has consequences for the public and for the health of democracy" (Anderson, 2012, p. 78).

In some ways, hacker journalism fuels citizen journalism, although the two are distinct movements and practices primarily because citizen journalism presumes amateur status. In an interview, Boyer said, "Instead of trying to make something that works for everyone, just give away the data, and let them do what they want to do with it. We're never going to imagine everything that everyone can think of to do with this information" (Boyer, 2010). Boyer designs for openness. His goal is audience-directed consumption, which means that his platforms facilitate user flexibility and data manipulation, a departure from designing with the self in mind that Gans identified in traditional journalism. In keeping with the hacker ethos, hacker journalists value the news judgment of consumers. "At every step, we've given away the data and documented our processes here so that other teams may follow in our footsteps," Boyer said (Boyer, 2010). Through this power-to-the-people mantra and crowd-sourced data interpretation practice, hacker journalists bypass traditional gatekeepers. Matt Waite, co-creator of the Pulitzer Prize-winning [PolitiFact](#) website and professor of practice at the University of Nebraska, said in an interview that hacker journalists are "quite literally taking control of the means of production" (Waite, 2011). This Marxist revival within the realms of journalism rearticulates the elements of the Hacker Ethic that focused on "freeing" information and empowering people with information and that facilitated the contemporary open-source movement. These journalists emerge in response to new economic demands and economic crises and are in some ways a new economic class—highly educated and culturally privileged but also economically dispossessed.

Hacker journalists eschew their potential earnings in computer industries and operate within legacy media because of the intersections between journalism ethic and hacker values. Waite said, "If journalism is to work and survive on the Web, then journalists need to be involved in defining how that journalism is going to appear on the Web." Waite believes hacker journalists are "doing product development as an act of journalism" meaning they create new income streams for media industries. "If you were a print reporter, you were not building a new print product. With hacker journalists, you are more intimately involved in all phases of development" (Waite, 2011). These products may be problematic. For example, journalists no longer need to produce attributed statements from sources

because they can provide data. Journalists (their persons, their programs, and the data itself) become authorities. This presents one conflict between hacker ethics, which advocate for direct and revolutionary change, and journalistic ethics, which advocate for transparency and exposure but not necessarily journalist-directed change. As a result, some hacker journalists felt exposed and found a “face,” or someone to speak the data (deVilla, 2011).

Hacker journalism infuses journalism with a libertarian flavor transplanted from computing cultures. For Brian Boyer, “The self-proclaimed hacker journalist has carried the open-source ethos into his work for a legacy news outlet.” Hacker journalists hope to shift the balance of power between those agencies that create the data and those trying to decipher it. They honor the shared belief system of journalism and hacking: empowering people with information. The populist hacker ethos is manifested in the target audience of Boyer’s work – ordinary citizens, rather than “decision makers” like politicians or executives. Boyer says, “We’re always trying to provide people with information, and we’re trying to let people find their own story in this information” (Boyer, 2010). Instead of journalists operating as the hedge against tyranny in the traditional sense, they are “primarily counted on to provide the information, or data, that is used by citizens to register informed preferences” (Anderson, 2012, p. 91). Journalism becomes a platform instead of interpreter, meaning the public must be actively engaging data and therefore performing some of the important legwork of democracy. This distinction removes the journalist from a central position in the news making process and is one of the hallmark differentiations between hacker journalism and its predecessors within news industries.

For hacker journalists, journalism is broken. And technology is the fix. As Rich Gordon said, journalism is “as people in computer science like to say” an “interesting problem space” (Gordon, 2010). This vision appeals to the find-and-fix-it mentality of engineers and computer scientists, but it also appeals to a gamer spirit present in computer communities since the late 1960s (Brand, 1972). Gaming is increasingly becoming a part of journalism. For instance, in 2009, the United Kingdom’s government released four years of accounting records of members of parliament, but in “the most unhelpful format possible.” Because Guardian editors were overwhelmed, they enlisted readers by creating a game called “[Investigate Your MP’s Expenses](#),” which was the “world’s first massively multiplayer investigative journalism project” (McGonigal, 2011, p. 220). In three days, more than 20,000 players analyzed over 170,000 documents (McGonigal, 2011, p. 221). The game determined that “on average, each member of parliament expensed twice his or her annual salary,” costing taxpayers over £88 million annually (McGonigal, 2011, p. 223). The game resulted in real political and policy change. More than two-dozen members of parliament resigned, several were criminally prosecuted, and produced new financial policies. As Clay Shirky noted, if the global population spent 1 percent of the time it spends watching television “producing and sharing” on the internet, that would equal “more than one hundred Wikipedias’ worth of participation each year” (Shirky, 2010, p. 23).

Hacker journalists hope to harness this resource and direct it toward journalistic enterprise. Thus, hacker journalism participates in a historical moment characterized by high-profile social and political “power to the people” movements, including anti-media and anti-government (Tea Party) and anti-corporate (Occupy Wall Street). Like the social movements, hacker journalists arms citizens with information, hoping to galvanize change. For idealistic and populist hacker journalists, fixing journalism via technology is an avenue to fixing democracy itself. By relying on crowds rather than authorities, hacker journalists share libertarian flavors with many of the social movements as well as the hackers from which they draw their name.

Akin to social protest movements, hacker journalists advocate for governmental and corporate transparency. For instance, founded in 2006, [WikiLeaks](#) provides a platform for the anonymous circulation of confidential documents, forever altering the idea of privileged information through several high-profile leaks of military, diplomatic, and corporate information (“WikiLeaks,” 2012). WikiLeaks claims it provides “a new model of journalism” that corrects the problem of legacy media because they have become “less independent and far less willing to ask the hard questions of

government, corporations and other institutions” (“What,” 2012). WikiLeaks shares a methodological persuasion with hacker journalism in that it publishes raw data and information and allows anyone interested the opportunity to interpret it. WikiLeaks is an organization that enables the hacking of secret information, but in pairing with legacy media like [The New York Times](#) and [The Guardian](#) it operates like hacker journalists. In these partnerships, WikiLeaks reaffirms legacy media’s control over public attention in the attention economy and their credibility as interpreters and agenda setters. Although similar, hacker journalism and WikiLeaks differ in that hacker journalism focuses more on reforming data, making it broadly usable and providing forums for communities to connect with data sets. WikiLeaks concerns itself primarily with accessing information, cracking open infrastructures of secrecy and exposing corruption and fraud.

Hacker journalism illustrates the potential impacts and risks of the hybridization of Hacker Ethics and journalistic ethics. On the one hand, adding Hacker Ethics to journalistic practices may help stabilize the economics of news by creating new informational wares, by pushing the industry to take more risks, and by involving audiences to greater extents. The press is the citizen’s hedge against governmental corruption and fascism (Dreyfus, 2012). In the era of big-data information flow, the First Amendment’s promise of a “free press” can seem an empty one if that press is overwhelmed. In the era of big data and in a historical moment in which corporate power is supplanting governmental power, the legacy press is ill equipped to report in a way that protects citizens. Hacker journalists illustrate what is possible when the First Amendment power of the press is combined with the technical power of programming.

On the other hand, adding a Hacker Ethic of radical openness and collective production to journalistic practice risks privacy violation, security breaches, and the breakdown of economic news institutions. These concerns are not new to the use of computing in journalism. Even in the 1980s, journalists expressed concerns about how database investigations might violate privacy. As one [Seattle Times](#) systems editor said, “once reporters get a gleam in their eye, they sometimes want to know everything about everybody” (Miller, 1988, p. 38). A former contributing editor to [Wired](#) wrote, “Careers will be made and undone by hacker journalism. Sometimes the information that comes out of these will be for the public good... but it’s certainly also going to be abused” (Honan, 2011). The conflict between transparency and privacy brings into contrast the difference between hacker journalists and journalists who hack illegally, such as those at the heart of the News of the World voicemail scandal. One could argue that WikiLeaks advocates a similar style of journalism, despite the professed idealism of its mission to shed light on powerful entities.

Thus, hacker journalist practices exist within a series of tensions about information. Hacker journalists are themselves deregulating information flows, but at a time when economic deregulation is, paradoxically, facilitating the reaction of multimedia conglomerates that are also privatizing information. In addition, questions remain whether crowdsourced oversight relieves public institutions of the burden of oversight. If the FDA posts information online, does it need to process it, or does that become the job of gamers and hacker journalists? Furthermore, the assumption that a merging of hacker and open-source ethics with journalistic ethics will improve media and democracy ignores the issue of technology itself. Technologists such as Jaron Lanier (2010) and academics such as Carolyn Marvin (1988) have long critiqued the idea that technology is ideologically neutral and have illustrated how technological design carries cultural assumptions and values. Lanier (2010) in particular has critiqued the increasing reliance on technology and what he calls “digital Maoism,” the deification of technology and data over humans and the idea that computer data and humans in aggregate are preferable to individual judgment (p. 24). Lanier cites the open-source movement and the Hacker Ethic’s deification of information in the “information wants to be free” mantra and enabling digital Maoism. Lanier writes, “Information of the kind that purportedly wants to be free is nothing but a shadow of our own minds, and wants nothing on its own” (p. 29). To extend Lanier’s argument, as we increasingly unseat the judgments of individual journalists and rely on the skill of the computer programming formatting the data and the volunteerism of crowds to process or provide the data, we

increasingly rely on algorithms and computing to assess our collective reality. Our news and therefore our sense of reality, then, depend on the increasingly “meta” datasets so large no one human can comprehend them (Lanier, 2010, p. 28). As writer Tim O’Brien noted, “What felled the financial industry is that, in the end, they were pursuing the same goals, listening to the same signals, deriving the same conclusions.” O’Brien remains hopeful, however, for although “there is often an element of groupthink among geeks, just as with journalists,” if journalists hold their ethical ground and operate “in pursuit of novelty and innovation, technologists might be their best friend in creating the tools that might lead them to find it” (O’Brien, 2011, p. 10).

References

About The Knight News Challenge. The Knight Foundation. Retrieved July 11, 2012 from <http://newschallenge.tumblr.com/about>

Adams, C. (2003). Using technology to uncover medical stories: With computer-assisted reporting: Think small and big. Nieman Reports, 3, Retrieved July 11, 2012 from <http://www.nieman.harvard.edu/reports/article/101193/Using-Technology-to-Uncover-Medical-Stories.aspx>

Anderson, C.W. (2012). From indymedia to demand media: Journalism’s vision of its audience and the horizons of democracy. In Michael Mandiberg (Ed.), *Social Media Reader* (77-98). New York: New York University Press.

Benkler, Y. (2002). Coase’s Penguin, or, Linux and the nature of the firm. *Yale Law Journal*, 112(3), 372-373.

Boyer, B. (2010, December 16). Interview with Bret Schulte. Telephone. Fayetteville, AR.

Brand, S. (1972, December 7). Spacewar: Fantastic life and symbolic death among the computer bums. *Rolling Stone*. http://www.wheels.org/spacewar/stone/rolling_stone.html

Bruns, A. (2008). *Blogs, Wikipedia, Second Life, and beyond: From production to produsage*. New York: Peter Lang.

deVilla, J. (2011, May 13). Notes from Hacks/Hackers Ottawa: May 12, 2011. Published <http://www.joeydevilla.com/2011/05/13/notes-from-hackshackers-ottawa-may-12-2011/>

Dreyfus, S, Lederman, R., Bosua, R., and Milton, S. (2011). Can we handle the truth? Whistleblowing to the media in the digital era. *Global Media Journal*, 5(1). Retrieved July 11, 2012 from http://www.commart.uws.edu.au/gmjau/v5_2011_1/dreyfus_truth_Essay.html

Drezner, D.W. and Farrell, H. (2008). Introduction: Blogs, politics and power. *Public Choice* 134, 1–13.

Freedman, T. (2005). *Electric dreams: Computers in American culture*. New York: New York University Press.

Gans, H. (2004). *Deciding what’s news*. Evanston, IL: Northwestern University Press.

Gibson, W. (1984). *Neuromancer*. New York: Ace Books.

Gillmor, D. (2004). *We the media: Grassroots journalism by the people, for the people*. Sebastopol, CA: O’Reilly.

Gordon, R. (2010, December 31). Interview with Bret Schulte. Telephone. Fayetteville, AR.

Hacker journalism: Could 'open-source projects one day be to information what the assembly line has been to manufacturing? (1999, December 4). *The Economist*, 66.

Hogg, C. (2009, May 11). Did the internet kill journalism? *Digital Journal Reports*.
<http://digitaljournal.com/article/271696>

Honan, M. (2011, July 5). Rise of the hacker journalist. *Gizmodo*. <http://gizmodo.com/5818184/rise-of-the-hacker-journalist>

Kurtz, H. (2004, December 13). From the guy next door. *Washington Post*, C01.

Lanier, J. (2010). *You are not a gadget*. New York: Alfred Knopf.

Leonard, A. (1999, October 8). Open-source journalism: Slashdot members' vicious response to a cyberterrorism story spurs a rewrite and questions about geek-influenced journalism. *Salon*.
http://www.salon.com/1999/10/08/geek_journalism/

Levy, S. (1984). *Hackers: Heroes of the computer revolution*. New York: Doubleday.

Marvin, C. (1988.) *Old technologies: Thinking about electronic communication in the late nineteenth century*. New York: Oxford University Press.

McGonigal, J. (2011). *Reality is broken: Why games make us better and how they can change the world*. New York: Penguin Press.

Medovoi, L. (2005). *Rebels: Youth and the Cold War origins of identity*. Durham: Duke University Press.

Meyer, P. (2002). *Precision journalism: A reporter's introduction to social science methods*. New York: Rowman & Littlefield Publishers.

Miller, T. (1988, Sept/Oct). The data-case revolution: A look at how reporters are making use of powerful new technology. *Columbia Journalism Review*, 35-38.

Moynihan, S. (2010). WikiLeaks: Setting the 'agenda?' *Editor & Publisher*, 143(9), 17.
 O'Brien, D. (2011, June 24). Technologist could yet prove best friends to journalists. *The Irish Times*, 10.

Ross, A. (2000). Hacking away at the counterculture. In *Electronic Media and Technoculture*. J. Thornton, ed. New Brunswick: Rutgers University Press.

Schulte, B. (2011, March/April). The hacker, off the couch. *Columbia Journalism Review*. Retrieved July 11, 2012 from http://www.cjr.org/currents/the_hacker_off_the_couch.php

Schulte, S. (2013). *Cached: Decoding the internet in global popular culture*. New York: New York University Press.

Shirky, C. (2010). *Cognitive Surplus: Creativity and generosity in a connected age*. New York: Penguin Books.

Siegler, M. Eric Schmidt: Every 2 days we create as much information as we did up to 2003. *TechCrunch*. Retrieved July 11, 2012 from <http://techcrunch.com/2010/08/04/schmidt-data/>

Streeter, T. (2011). *The net effect: Romanticism, capitalism, and the internet*. New York: New York University Press.

The Matrix. (1999). Dirs. Andy Wachowski and Larry Wachowski. Groucho II Film Partnership.

Turner, F. (2006). From counterculture to cyberculture: Stewart Brand, the Whole Earth Network, and the rise of digital utopianism. Chicago: University of Chicago Press.

Vaidyanathan, S. (2012). Open source as culture/culture as open source. In Michael Manidberg (Ed.), *Social Media Reader* (24-31). New York: New York University Press.

Waite, M. (2011, January 8). Interview with Bret Schulte. Telephone. Fayetteville, AR.

What is WikiLeaks? WikiLeaks. Retrieved July 11, 2012 from <http://wikileaks.org/About.html>
WikiLeaks Topic Page. New York Times. Retrieved July 11, 2012 from <http://topics.nytimes.com/top/reference/timestopics/organizations/w/wikileaks/index.html>

Bret Schulte is an assistant professor of journalism at the University of Arkansas. He has a BA in English Literature from the University of Nebraska and an MFA in narrative nonfiction from George Mason University. He worked as a journalist for the *Arkansas Democrat-Gazette*, *The Washington Post*, and *U.S. News & World Report*. He freelances for *The New York Times* and wrote about hacker journalism for *Columbia Journalism Review*.

Stephanie Schulte is an assistant professor of communication at the University of Arkansas. Her research focuses on networking technologies, specifically the cultures and policies associated with them. She authored *Cached: Decoding the Internet in Global Culture* (NYU Press, 2013) and has published in *Television and New Media*, *Journal of Transnational American Studies*, *Journal of New Media and Culture*, *Feminist Studies*, and *Mass Communication and Society*.

[About](#) | [Issues](#)

© NMEDIAC & individual NMEDIAC authors, editors, and programmers.