2009

Cookie Monsters: Seeing Young People's Hacking as Creative Practice

Gregory T. Donovan
CUNY Graduate Center

Cindi Katz
CUNY Graduate Center

Children, Youth and Environments 19(1), 2009

Cookie Monsters: Seeing Young People's Hacking as Creative Practice

Gregory T. Donovan
Cindi Katz
Environmental Psychology Program
City University of New York

Citation: Donovan, Gregory T., and Cindi Katz (2009). "Cookie Monsters: Seeing Young People's Hacking as Creative Practice." *Children, Youth and Environments* 19(1): 197-222. Retrieved [date] from http://www.colorado.edu/journals/cye.

Abstract

This paper examines the benefits and obstacles to young people's open-ended and unrestricted access to technological environments. While children and youth are frequently seen as threatened or threatening in this realm, their playful engagements suggest that they are self-possessed social actors, able to negotiate most of its challenges effectively. Whether it is proprietary software, the business practices of some technology providers, or the separation of play, work, and learning in most classrooms, the spatial-temporality of young people's access to and use of technology is often configured to restrict their freedom of choice and behavior. We focus on these issues through the lens of technological interactions known as "hacking," wherein people playfully engage computer technologies for the intrinsic pleasure of seeing what they can do. We argue for an approach to technology that welcomes rather than constrains young people's explorations, suggesting that it will not only help them to better understand and manage their technological environments, but also foster their critical capacities and creativity.

Keywords: children, youth, Internet, cyberspace, security, hacking

Introduction

Technological innovation promises exhilaration with a backbeat of panic—everything will be NEW and DIFFERENT! EVERYTHING will be new and different! Of course neither promise nor peril are ever fully warranted or realized. When it comes to U.S. children and youth, adult responses to technology are intertwined with a sprawling panic about children's safety and well being, yet met with a differentiated and even nuanced response. In the 1980s, for instance, there was much discussion regarding how to teach children computer code (Turkle 2005; Papert 1993). The logic at the time was that if a child learned how to program a computer, the computer would have a harder time programming the child. This idea led to large-scale educational projects such as Logo that aimed to incorporate coding into play. In the No Child Left Behind (NCLB) era at the start of the 2000s, however, we have witnessed a reversal of such efforts. Attempts to produce media and technology literacy in classroom pedagogy run counter to the routinized and exam-oriented interests of NCLB curricula. In the contemporary educational environment where student scores on standardized tests determine a school's standing and funding, not to mention individual children's advancement, technology has become more of a vocational tool for efficient test preparation than a means of encouraging critical and creative thinking.[1] Under these circumstances, playing with technology—particularly code—or "hacking" is recast as deviant behavior.

Meanwhile, parents and teachers—frequently insecure and relatively inexpert in the realms of computers and other digital technologies—all too often compensate for their lack of knowledge and skills with private surveillance and censorship technologies such as Net Nanny or CyberPatrol, which are intended to filter out putatively harmful content and interactions on children's behalf. As in other realms of contemporary life, insecurity in one arena galvanizes security practices in another (Katz 2008). These practices imagine and invoke broad threats to children and youth, whom they cast more as witless victims than as thoughtful, informed, and often quite capable social actors. The other side of the security discourse around children and youth calls for protection *from* them, fostering a panoply of strategies to monitor them and their actions (Katz 2001).

Amidst such practices, *hacking*—discussed here as play, curious exploration, or as a puzzle solution that helps young people to better understand and control their environments (technological and otherwise)—emerges as a site of invention and discovery as well as resistance to various technological fetters. When young people circumvent web filters and surveillance technologies, freely download and circulate music, or falsify information through, for example, entering incorrect information on their social profiles or trading or simply turning off their cell phones to disable GPS tracking capability, they take steps towards demystifying their technological environment.

This paper examines the tension associated with children and youths' use of the Internet and computer technologies in school and at home, and the various

[1] The "Enhancing Education Through Technology Act of 2001" can be found at http://www.ed.gov/policy/elsec/leg/esea02/pg34.html

commercial and governance practices that channel, monitor, and restrict their virtual engagements. We hope to show the benefits of young people's open-ended and unrestricted access to technological environments, the value of their learning how to manage and engage these environments and their associated technologies in an informed way, and the limits of technological strategies that filter, monitor, censor, and otherwise restrict young people's free and open engagement with their technological environment.[2] As we point to various household, corporate, and governmental encroachments on children and youths' technological encounters, we want to suggest that there is a fine and often blurry line between school and parental strategies for (over)protecting youth in their everyday and technological environments and the sort of policing strategies associated with things like the Semantic Web or proprietary software.[3] These practices—the former associated with parents and others responsible for young people's well being, and the latter associated with the state and corporate capital—reinforce and provide alibis for one another, compromise claims to privacy by young people and others, and lubricate modes of hypervigilance that have become the new normal in the U.S. since September 11, 2001. But these relationships are anything but monological, as children and youths' playful engagements with the technological environment have made clear. Drawing upon our research with young people, we will identify some of the opportunities for and practices of reworking technological environments and their claims on children and youths' time, space, and subjectivity.

A Laptop on Every Lap

The intersection of young people and technology is a double whammy; each part of the pair is a site of anxiety. While youth are often seen as vulnerable to predators, distraction, and failure among other risks to healthy development and appropriate socialization, they are also cast as a threat to the smooth functioning of the larger society and its normative values. Likewise, technology is commonly scripted as a means to resolve social and political economic problems if not as a panacea for them, but it is also understood as a threat to social relations and wellbeing. That all of these understandings are flawed or at best partial makes them no less captivating.

Here we examine the ways the relationship between young people and technology brings to the fore concerns regarding children and youth's vulnerability in and to technological environments, as well as their (mis)use of and capacities in these

---

[2] Our criticisms of the apparatus and strategies devised for restricting young people's access to the Internet is not meant to suggest that all of the Web's content is appropriate for young people (or anyone else for that matter). We are pointing to the limits of technological fetters and the sort of blanket assumptions about children's critical capacities that often accompany them. As in every arena, these sorts of practices are no substitute for the social engagement of parents, teachers, and others in assisting children to mediate and manage their environments, technological and otherwise.

[3] The Semantic Web (SW), primarily conceptualized and developed by Tim Berners-Lee, can be understood as an extension of the World Wide Web (WWW) that semantically codes information so it can be processed and interpreted across various platforms and programs through "automated" analysis. Whereas the WWW is designed so humans can read it, the SW formats information so computers can read it.

environments. Our concern here is with the ways information technologies are deployed and understood in young people's environments, and particularly with the ways that children and youth's access to these environments is scripted and surveilled, encouraged and contained. We start with the encouragement, with a look at the vaunted One Laptop per Child Program (OLPC).[4]

OLPC is a case ripe for analysis due to its explicit focus on laptops as a means for education in developing nations. Its laudable aims notwithstanding, OLPC fashions the laptop as a silver bullet capable of penetrating the social, historical, and political economic factors that have hindered education in these environments. Yet, as two recent analyses highlight, OLPC's failure to address the full range of environmental factors associated with young people's learning in the global South is already limiting the project's influence (Kraemer, Derrick and Sharma 2008), and even has the potential to have a "chilling effect" on children and youth's privacy and free speech (Patterson, Sassaman and Chaum 2008).

"Why do children in developing nations need laptops?" This seemingly rhetorical inquiry can be found atop a list of "frequently asked questions" on the One Laptop per Child website, the organization perhaps best known for its "$100 laptop," the XO Children's Machine.[5] Nicholas Negroponte, a founder of the MIT Media Lab and chairman of the OLPC initiative, responds:

> *Laptops are both a window and a tool: a window out to the world and a tool with which to think. They are a wonderful way for all children to learn learning through independent interaction and exploration.*[6]

As a window implies a transparent opening and a tool implies a device used to implement certain functions, the statement warrants some unpacking with regard to the intended transparency and function of the XO. A follow-up question might ask Mr. Negroponte how transparent this metaphorical window is, and what kind of thinking this tool is intended to afford. We might ask what lessons these technologies teach young people and what we can learn from a better understanding of their playful interactions with them. As socially produced artifacts, technologies such as laptops are embedded in a particular social, historical, and political economic context. They bring with them a set of values and normative ideas that shape and are shaped by their production. What social relations these technologies in turn produce, reproduce, or challenge are objects of our concern here, and are of great importance to discussions of children and youth's technological environments.

---

[4] One Laptop per Child is a non-profit organization founded to develop low-cost but rugged and efficient laptops for children in developing countries.

[5] The Original Design Manufacturer (ODM) of the XO is Quanta Computer Inc of Taiwan. As of July 6th, 2008, OLPC reports that they have shipped 400,000 XO's with Peru and Uruguay receiving nearly half of all shipments (One Laptop per Child 2008).

[6] Source: "Frequently Asked Questions." One Laptop per Child (http://laptop.org/vision/mission/faq.shtml), retrieved May 17, 2008.

A look at the recent shift from free and open-source software (FOSS) to proprietary software at OLPC serves as a useful starting point in this endeavor. Our focus on OLPC's recent shift is not to argue that FOSS environments are more beneficial to children and youth, although such a case could probably be made. Rather, our intent is to unpack this particular decision in order to articulate how such a shift brings with it a set of values and normative ideas that we contend shape young people's engagement with their technological environments. Although our focus here is on OLPC, and thus children and young people's access to and use of these technologies in the global South, the concerns we address pertain more generally.

With its antecedents in the 1960s, OLPC was founded in 2001 on the constructionist philosophy of learning popularized by the MIT Media Lab Professor Seymour Papert, which argues that children learn best through collaboration and creation (e.g., Papert 1991; Ackermann 2001). At its inception, the initiative's goal, at least according to its public statements, was to mass-produce low-cost FOSS laptops that would work in and be accommodated by the environments of children in underdeveloped countries and promote a constructionist learning model.[7] The XO is very light, extremely durable, and quite energy efficient. It can be foot- or solar-powered, and so can be used anywhere.[8] Most notable, and arguably most relevant to the constructionist model, is the XO's mesh-networking capability. This capability allows the machine to relay existing Internet connections, thus extending coverage via Wi-Fi, or to create autonomous wireless networks with other XOs when no Internet connection is available.

All of this creative effort and thoughtful investment makes clear that at its inception, OLPC was intent on democratizing access to the technological environment by providing means to incorporate children and youth from the so-called third world. Moreover, the program—true to its constructionist philosophy—encouraged children and youth's critical engagements in and with that environment. Yet, if these were OLPC's founding principles, they seem to have gotten lost along the way and even subverted in practice. Begun with FOSS, the "window" these laptops now make available to young people is increasingly a proprietary one—most notably, Microsoft's Windows operating system. Until recently OLPC had pointedly and publicly resisted bundling Windows with the XO. Even with (or perhaps because of) numerous corporate partners, OLPC insisted that "software freedom" was central to their constructionist learning philosophy and necessary to give "children the opportunity to use their laptops on their own

---

[7] Walter Bender, the former President and Chief Operating Officer of OLPC, was an advocate Papert's constructionist learning model, noting "children learn best when they are in the 'active role of the designer and constructor' and that this happens best in a context where the child is 'consciously engaged in constructing a public entity.'" Following Papert, Bender argued that "the creation process and the end product must be shared with others in order for the full effects" of the constructionist learning model "to take root" (Open Education 2008).

[8] Information retrieved on May 17, 2008 from: http://www.laptop.org/en/laptop/hardware/specs.shtml

terms."[9] Sugar, a Linux based FOSS operating system designed by OLPC for the XO, had been described by OLPC as the "core" of their laptop's interface and essential to the sharing and learning affordances of the machine.[10] And, it works beautifully. Yet in spring 2008, Microsoft, which with its legendary proprietary clout is the antithesis of OLPC's founding principles, succeeded in getting Windows onto the XO. According to a May 15, 2008 Microsoft press release, Windows will be available for the XO with "trials to begin in *key emerging markets* as early as next month" (Microsoft 2008).[11]

The move to include Windows is both material and ideological. It is sure to have a profound impact on future recipients of the XO and the continued unfolding of the OLPC project as we detail below. Its significance is underscored by a recent change in leadership at OLPC. Walter Bender, who was the president and chief operating officer of the organization until April 2008, was the lead developer of Sugar, a supporter of constructionist learning methods and principles, and a strong proponent of FOSS as congenial to these (Lohr 2008). The incoming president and COO, Charles Kane, was OLPC's finance chief and is a former software company executive. The change in leadership is not coincidental. In an interview with one industry magazine, Mr. Bender attributed his resignation to OLPC's decision to support the Windows operating system.

> *Nicholas [Negroponte] has made it clear, at least to me, that OLPC needs to be strategically agnostic about learning—that it can't be prescriptive about learning... Nicholas had that wonderful quote in* BusinessWeek *about a month ago—that OLPC is going to stop acting like a terrorist and start emulating Microsoft. If you read between the lines, the idea is to stop trying to be disruptive and to start trying to make things comfortable for decision-makers* (Roush 2008).

Meanwhile, Mr. Kane noted the following in a separate interview with another industry magazine:

> *The OLPC mission is a great endeavor, but the mission is to get the technology in the hands of as many children as possible... Whether that technology is from one operating system or another, one piece of hardware or another, or supplied or supported by one consulting company or another doesn't matter... It's about getting it into kids' hands* (Talbot 2008).

Of course, which software or hardware we deal with and which corporations supply or support them *do* matter. Kids are, after all, a rather large "emerging market." Moreover, an "agnostic" approach to either learning or technology—strategic or otherwise—further mystifies its production and "built pedagogy," which Torin

---

[9] Source: "Software." One Laptop per Child (http://www.laptop.org/laptop/software/index.shtml). Retrieved May 17, 2008.
[10] Source: "Sugar." One Laptop per Child wiki (http://wiki.laptop.org/go/Sugar). Retrieved May 17, 2008.
[11] Emphasis added.

Monahan (2005, 8) defines as the "lessons taught by technological systems and spaces." The "built pedagogy" of a proprietized OLPC is utterly different than a FOSS one, and as the project goes increasingly global, virtually reaching the next generation worldwide, the consequences of these decisions will be profound.

The rationale provided for this shift is revealing and central to our concerns. Mr. Negroponte cites a desire by decision-makers to see Windows on the XO before they agree to buy into the program. Indeed, Microsoft's press release includes a quote from the governor of Cundinamarca, Colombia, stating:

> *Windows support on the XO device means that our students and educators will now have access to more than computer-assisted learning experiences. They will also develop marketable technology skills, which can lead to jobs and opportunities for our youth of today and the work force of tomorrow* (Microsoft 2008).

The priorities implicit in such rationalizations are that an *educational* machine that affords learning and collaboration is not enough to warrant investment, whereas a *vocational* machine that will train a generation of young people for a future tech-based workforce is worthwhile. This helps explain the decision to incorporate Windows even though it "cripples" the XO's mesh-networking capabilities (Krstić 2008). This is an unfortunate casualty considering that preliminary results from evaluations underway in New York City and rural Uruguay have highlighted the educational value of this feature in classroom activities (Lowes and Luhr 2008; Hourcade et al. 2008).

John Dewey (1916, 319) argued that vocational training reinforces the existing industrial regime, suggesting that if it were incorporated into education it "would give to the masses a narrow technical trade education for specialized callings, carried on under the control of others." Although Dewey was discussing "industrial life," the same holds true of informational life. OLPC's aim seems more and more to be to put a laptop on the lap of every child, with less concern about how that laptop is mediated. When education takes a backseat to vocational training, it is not surprising that learning-oriented features of the XO such as Sugar or its mesh-networking capability take a backseat to corporate interests and security—after all, both Sugar and mesh-networking "terrorize," to borrow Mr. Negroponte's phrase, the security of Microsoft's intellectual property.[12] With these moves, OLPC's broad and exciting educational goals have been compromised—a curious position for an

[12] It should be noted that Microsoft's Windows is widely pirated in the global South, so providing controlled versions for the XO can be seen as a counteraction to this. Additionally, by crippling the mesh-networking feature, they compromise the peer-to-peer communicative features of the machine, a feature that Microsoft has opposed in general. Finally, FOSS runs counter to the corporate philosophy of Microsoft and to the commodification and privatization of software in general. If people can get it free, why would they pay? One can read "Bill Gates's Open Letter to Hobbyists" (http://www.digibarn.com/collections/newsletters/homebrew/V2_01/homebrew_V2_01_p2.jpg) to get a sense of his personal sentiments as well as the undergirding philosophy upon which Microsoft was built.

organization whose website hypes the mantra, "It's an education project, not a laptop project."[13] It took just one year for this shift to materialize and take hold against the profoundly idealistic founding principles of OLPC, which many of its supporters and participants still cherish.

If the window is clouded increasingly by proprietary software and corporate interests, what sort of tool are these laptops for children? Ivan Krstić (2008), the former top security architect for OLPC, responded to the impending switch from the FOSS platform to Windows by arguing:

> *OLPC can't claim to be preoccupied with learning and not with training children to be office computer drones, while at the same time being coerced by hollow office drone rhetoric to deploy the computers with office drone software.*

Perhaps the answer to our question is: a tool of corporate subjugation. Not one that "programs the child" per se—after all, children and youth are never passive recipients of technology or knowledge but rather active participants and co-constructors—but one that by its very design privileges vocational training and seems to hamper creative play through the overlay of restrictive intellectual property rights. Close attention to the built pedagogy of the XO is needed as it shifts from an entirely FOSS machine (with the exception of a proprietary firmware program for Wi-Fi access) designed for the promotion of open learning and sharing in the social and structural environments of the global South, to one that increasingly adopts proprietary software for the vocational training of a future global workforce. The lessons being taught—implicitly as much as explicitly—are of great importance to young people and the social formations in which they are coming of age.

From the outset, thinkers and teachers like Seymour Papert could intuitively see the connections between hardware, software, learning, and knowledge together with their possibilities for creative engagement. Yet, this critical vision has been compromised by some of the recent decisions of OLPC, which appear to separate the means though which the hardware is produced and distributed from the ends to which it is, and can be, put. That OLPC seems increasingly to isolate its distribution goals from its learning goals raises the question of whether the program is *reworking* traditional modes of development, production, and use of computing or *reinforcing* them in the global South among the populations served by OLPC. The very subjects of computing—now and of the future—are at the heart of these matters.

The almost utopian vision that initially spurred OLPC has increasingly and disconcertingly devolved to dovetail with much of the routinized and exam-oriented curricula associated with NCLB in the U.S. To treat the technological components of social formation as ends in themselves sidesteps the crucial questions of the built

[13] Source: "Vision." One Laptop per Child (http://laptop.org/en/vision/index.shtml). Retrieved on May 17, 2008.

pedagogy of these materials for youth North and South. Simply taking the XO at face value mystifies its production and operation within particular communicative environments saturated with social relations of production and reproduction. And yet, as scholars such as Monahan (2005) argue, quite the opposite is possible if a critical approach to built pedagogy is taken.

These "tools" and "windows" of young people's computing are produced and encountered within historically and geographically specific social formations, and should be engaged critically. Yet critical engagement with these technologies—in classrooms of the global North as much as in OLPC—is exactly what is now being discouraged in subtle and sometimes overt forms. Immersing people, particularly during their youth, in proprietary environments where information circulation is tightly controlled and intellectual property rights are strictly enforced helps to socialize a generation that will continue to play (and cheat) by the old rules for appropriation, distribution, and consumption, rather than imagine new rules and opportunities. When alternative social and technological relationships are imagined and enacted, such as in the case of the FOSS XO, they are typically perceived as a threat by government and private business, whose representatives have not hesitated to associate the supposed threat with "terrorism" in their zeal to squelch it.

In this view, children and other young users are cast typically as both threatening and threatened. But it is play that is being threatened and co-opted here. Children's play in technological environments, including but not limited to the XO, is increasingly being shaped and channeled to socially reproduce behaviors and attitudes appropriate for future work in an informational economy. Again, young people are not passive in their encounter with this web of relationships and material social practices. What they do in these proprietary environments, and how they may (or may not) reclaim and rework play for other creative and innovative purposes, is precisely what is at stake in key contemporary debates on youth and technology.

Hacking It

Hacker and *hacking* are terms that evoke wildly divergent meanings depending upon the context. In the contemporary lexicon, *hacker* is commonly defined in relation to computer/network security, the free and open-source software (FOSS) movement, and/or general computer hobbyists. Its most frequent—and deceptive—frame of reference in the post-9/11 security state has been in the context of computer/network security.[14] In this context, *hacking* is understood as cyber crime—politically motivated or otherwise—that is a threat to national security, corporate security, and personal safety. Websites often post a "hacker safe" or "hacker proof" banner to assure cyber-surfers that their transactions are "secure." An advertisement promoting the newly formed U.S. Air Force Cyber Command

[14] Of the top 20 news stories retrieved through a Google News search of "hacker" on June 1, 2008, 14 were used in the context of computer/network security, one was used in the context of computer hobbyists, and the remaining five referred either to golf or an individual's surname.

displays footage of the Pentagon while announcing, "This building will be attacked three million times today," and describing itself as "America's only Cyber Command protecting us from millions of cyberthreats everyday" (Air Force Cyber Command 2008). Meanwhile, network security firms such as Comodo, Network Solutions, and McAfee all offer security services to online businesses, promising them and their customers safety from the criminal activities of pesky hackers. Such framing runs counter to that of the hacker culture itself, which refers to these sorts of activities as "cracking," a neologism constructed during the early 1980s to distinguish computer crime from "hacking." The Jargon File, a prominent online resource for hacker terminology, defines a "cracker" as "one who breaks security on a system" and notes that:

> *…while it is expected that any real hacker will have done some playful cracking and knows many of the basic techniques, anyone past larval stage is expected to have outgrown the desire to do so except for immediate, benign, practical reasons (for example, if it's necessary to get around some security in order to get some work done).*[15]

Thus, while *hacking* is the term most often used by those involved in "protecting" computer/network security, engendering a pejorative and criminal connotation, it would be more accurate to distinguish these activities as *cracking*.

With "cracking" understood as the realm of criminal behaviors, the playful element of hacking associated with the FOSS movement or among general computer hobbyists comes to the fore. The MIT hackers, chronicled in Turkle's (2005) *The Second Self*, for instance, are presented as a geeky group of mostly young men more interested in "Ugliest Man on Campus" pageants and the wonders of technology and its possibilities than, say, cyber-attacking the Pentagon or corporate America. Turkle describes hackers as "loving the machine for itself." Torvalds (2001, xvii) suggests that for the hacker, "the computer itself is entertainment." In both cases the computer as a technological system is the object of interest—and play—for the hacker, and hacking emerges as a self-motivated and intrinsically pleasurable act. As The Jargon File presents it, "hack value" is

> *often adduced as the reason or motivation for expending effort toward a seemingly useless goal, the point being that the accomplished goal is a hack.*[16]

Sounds a lot like play.

Indeed, explaining how the MIT hackers were often expert lock pickers, many of whom carried picks on their key chains, Turkle (2005, 213) notes how pleasure was derived from "beating the lock" rather than breaking-and-entering. Associating lock

---

[15] The Jargon File is developed and maintained by Eric Raymond, an early figure in the FOSS movement, and has been published as *The New Hacker's Dictionary* by the MIT Press. See http://www.catb.org/jargon/html/C/cracker.html.

[16] See http://catb.org/~esr/jargon/html/H/hack-value.html.

picking with the cliché that Mount Everest is there to be climbed, Turkle explains that to the hacker, a "closed system is a challenge." Richard Stallman, founder of the Free Software Foundation, states as much during an interview in the documentary *Revolution OS* (2002). Marking his and other hackers' aversion to computer passwords and other modes of computer/network security, Stallman insists that computers should be open and available to everyone at anytime, not secretive and locked down. Turkle (2005) tells of a hacker who worked in a conservative corporate environment with a typical nine-to-five schedule, but realized that he was most efficient on a 36-hour schedule (24 awake, 12 asleep). To address the mismatch between his rhythms and the conventional spatial-temporality of his office, the hacker would pick the locked desks, file cabinets, and office doors at night, not to steal, but to work his preferred hours, achieving what he called "standard hacker time."

In the prologue to Pekka Himanen's *Hacker Ethic,* Linus Torvalds, the creator of the Linux operating system and a famous hacker, formulates "Linus' Law" to help explain the world of hackers.[17] Linus' Law proposes that hacker motivations fit three successive stages: *survival*, *social life*, and *entertainment*. According to Torvalds, hackers are not motivated to use their computers for *survival* but for *social life* and *entertainment*. Using the communal development of the Linux operating system as an example, Torvalds (2001, xvii) elaborates:

> *The reason that Linux hackers do something is that they find it to be very interesting, and they like to share this interesting thing with others. Suddenly, you get entertainment from the fact that you're doing something interesting and you also get the social part. This is how you have this fundamental Linux networking effect where you have a lot of hackers working together because they enjoy what they do.*

As the Jargon File indicates, to "hack" is "to interact with a computer in a playful and exploratory rather than goal-directed way."[18] It was in this sense that OLPC held so much promise for children and young people.

The computer itself as a technological system is an object of passion and entertainment for the hacker, at least in the context of the FOSS movement and among general computer hobbyists. This object-oriented pleasure and amusement along with the playfulness they promote, underlie what Himanen (2001) calls "the hacker ethic." Such modes of engagement are in a tense and even oppositional relationship with the "Protestant work ethic," which continues to undergird most corporate notions of productivity, though famously not in much of the high-tech industries. As Himanen (2001, 39) argues,

> *...the information economy's most important source of productivity is creativity, and it is not possible to create interesting things in a constant hurry or in a regulated manner from nine to five. So even for purely*

[17] Linux is the most popular FOSS operating system.
[18] See http://www.catb.org/jargon/html/H/hack.html.

> *economic reasons, it is important to allow for playfulness and individual styles of creativity since, in the information economy, the culture of supervision turns easily against its desired objectives.*

The tensions associated with this "culture of supervision" obtain in school and other settings where children and young people have access to electronic technologies.

Getting the Hack of It

We can see the rehearsals for and ricochets of these sentiments and practices in and around young people's lives, schooling, and computer use where the "culture of supervision' all too frequently thwarts playful learning and creative engagement with the technological environment. While space does not permit an extended discussion of children's play here, we want to underscore how thickly and fully it is intertwined with learning and experimentation and with the exploratory assimilation of knowledge. Parents, teachers, and others often hinder children's means of playing with knowledge—akin to hacking—by monitoring and channeling children's interactions with computers and the technological environment more broadly, or by not recognizing the charged relays among activities formally distinguished as work, play, or education. Apart from the ways the intrinsic pleasures of play are integral to healthy childhood development, play can also be quite "workful," while the best kinds of work share many of the attributes commonly associated with play (cf., Katz 2004; see Ginsberg et al. 2007 for an excellent review of the literature on the importance of children's play in healthy development).

While this much may be obvious in the upper echelons of the high-tech industry, there does not seem to be much "trickle down" to the technological environments of young people's everyday life. Beyond this nexus between work and play but of a piece with it is recognition that in the course of play, youth enter a world of meaning, imagination, and symbolic engagement that they encounter and rework more or less on their own terms and in their own time. In the process, young people acquire all sorts of knowledge, but perhaps more importantly, they learn what it means to negotiate a social field and "move in a field of meaning" (Bateson 1956; Vygotsky 1978). These qualities of play mesh exactly with learning how to make sense of and build upon the capacities and possibilities offered by computers. Yet, rather than recognize and support the fine weave that joins work, play, and learning in children's technological lives, many adults—parents as much as teachers, as well as programs such as NCLB—harden the divide between what seems to be play and what seems to be the serious business of learning.

The blurred boundaries between work, play, and learning—whether in time-space, in meaning, or in outcomes—are routinely ignored if not sharpened in many school settings. For example, in many computer labs, it is common for teachers to offer "play time" or "fun time" to help motivate students to do their school "work." This enticement usually boils down to ten minutes of unstructured time in the lab at the beginning or end of class when students are free to "play" on the computers. While it's meant as an incentive, this practice frames part of the class as "fun" or "playful" and the other as "work" and "educational"—separating the two realms in theory and practice as well as in time. Hiving off play from work not only drains all of the

playfulness out of schoolwork, but creates a community of practice geared more to standardized tests than to learning (cf., Lave and Wenger 1991). These regimes of practice carry over to the workplace where surveillance and censorship are often used to make sure that employees don't "goof off" at the computer while on the clock.

ITS

These monitoring systems notwithstanding, there is still plenty of "play" in the workplace, and sometimes it produces terrific "work." An example from the early days and heart of workplace computing makes the case. In the late 1960s at MIT's Artificial Intelligence Lab, hackers developed an operating system they called the "Incompatible Time-sharing System" (ITS), a play on the "Compatible Time-sharing System," an operating system in use at the time. ITS was motivated by an aversion to the development and use of Multics, an operating system that was one of earliest to be designed as a "secure" system. ITS did not require users to log on, it had no passwords, and any user could edit any file. A command called "OS" for "output spy" permitted anyone to view another's terminal while those "spied" on were notified. ITS was an example of how hacking—and the playful spirit that often accompanies it—allowed a group of people to develop a virtual time-sharing environment that was conducive to their needs and desires. Using ITS, they could really be co-workers with a more productive process than allowed by the systems that promoted security and hierarchy over cooperation and lateral connections in the electronic work environment. As Sherry Turkle (2005, 188) put it, the development of ITS "became a model for a mode of production different from the standard, a mode of production built on a passionate involvement with the object being produced." And, one might add, with those with whom one works (and plays). Indeed, "The language, humor, and values developed by the ITS hackers form the foundation of our contemporary understanding of hacker culture" and suggest the richness of the hacker imagination (Chopra and Dexter 2007, 9). If, as Raymond (2000, 3) suggests, the ITS hackers simply wanted a practical solution to address their immediate needs it was also the case that "ITS, quirky and eccentric and occasionally buggy though it always was, hosted a brilliant series of technical innovations and still arguably holds the record as the single time-sharing system in longest continuous use." The outcomes of such playful work and workful play shows the productivity of their combination, a productivity enhanced rather than diminished for being pleasurable.

These connections and outcomes are as true for children as for adults. Indeed, this sort of philosophy drove the early development of educational technologies such as Logo and the inception of OLPC, and much in between. While youth may not hack at the same level as members of the Artificial Intelligence Lab at MIT, they are curious, creative, and capable. It is on these grounds that we urge an understanding of *hacking* as play, as curious exploration, and as a sort of demystifying activity that helps young people to better understand and manage their environments (technological and otherwise). The case of the "mosquito" demonstrates how adeptly young people can manipulate a controlled and monitored technological environment as they put their play to work.

The Mosquito

Mosquito is a classic example of a struggle between adults trying to shape the spatial-temporality of childhood in what has become increasingly a security state, and children shaping it themselves in part by hacking technology. In 2006, the New York City Department of Education began enforcing a long-standing ban on cell phones in school. Parents were vociferous in their objections, turning the ban into a safety issue that tapped easily into the free-floating terror talk of post-9/11 New York. Parents went so far as to sue the Department of Education, arguing that cell phones were "a vital communication link" between them and their children, but the courts upheld the ban. For quite other reasons, students were not about to leave their phones at home, nor forgo their use entirely during school hours. The students found an ingenious means to evade the authorities. (That the strategy they devised came from another quarter of monitoring young people makes it all the more delicious.) The "mosquito" is an ultrasonic teen deterrent that was designed to promote "kid free" commercial zones by emitting a high-pitched noise that can only be heard by young ears, generally people under 30. Some students realized that they could use this ultrasonic sound for their own purposes, and made it the ring tone for their cell phones. With their phones out of earshot of most teachers, the students were able to continue to use them in school, mostly to exchange text messages. The fact that the students could have probably gotten around the restrictions by setting their phones to vibrate underscores the "hack value" of the mosquito: it was predicated on its social and entertainment value over questions of "survival." While teachers and school administrators may not have appreciated it, the students' adaptive re-use of the mosquito was deft and creative, the very essence of hacker culture, which many have argued is a key driving force of creativity and innovation in an information economy (Castells 2001; Himanen 2001). Imagine if educators built upon such activities and the sensibility that accompanies them, encouraging these sorts of hacker ethics and practices in the classroom rather than shutting them down and continuing to sequester what they see as work from what they understand as play.

Hacking, as we've suggested, can be a demystifying act that simultaneously comes out of and leads to experience-based shared learning about one's technological environment. Such collaborative cultural forms and practices create a "zone of proximal development" (Vygotsky 1978) in which children are able to negotiate, playfully experiment with, and thus more fully understand some of the ideas, structures, and rules of the technological environment and the social practices that produce, reproduce, and alter them. Through playful exploration a young person can experience the limitations as well as the potentials of technological systems, leading to a greater awareness of their built pedagogy and social entailments. As a result, young people can begin to engage and understand the more problematic and even ominous elements of power operating in their environment, including those elements associated with government and corporate interests. An exceptional yet instructive example of this sort of engagement is provided in the case of AriX, the 13-year-old iPhone hacker.

AriX and the iPhone

On June 29, 2007, Apple released the iPhone in the U.S. to much fanfare, selling 1 million during its first 74 days on the market (Crum 2007). Apple had signed an exclusive multi-year deal with AT&T, designating the telecommunications giant as the only carrier supported by the iPhone in the U.S.[19] —i.e., anyone who wants to "activate" an iPhone purchased in the U.S. is required to subscribe to AT&T's wireless service. In today's emerging informational economy this arrangement should be understood as a monopoly-inducing partnership.

However, when Apple and AT&T began releasing sales figures for the iPhone, there was a noticeable and growing gap between the numbers of iPhones sold by Apple and the number of iPhone owners who signed up for AT&T's wireless service. According to CNET, there was a gap of 124,000 after the first weekend of sales, with that gap ballooning to 1.7 million by the end of 2007 (Krazit 2008). While part of this can be attributed to the approximately 350,000 iPhones sold in European countries in which Apple signed exclusive deals with other wireless services, there was still a gap of about 1.35 million iPhones.

By design, the operating system on the iPhone discourages individuals from developing and installing third party applications. Functioning much like "parental controls," individuals are allowed to use an off-the-shelf iPhone only as Apple deems appropriate.[20] Nonetheless, the owners of the 1.35 million U.S. iPhones not using AT&T were not doing without telephone service. Rather, the majority of the phones had been hacked to allow their owners to use them with any GSM wireless provider they chose.[21]

Immediately following the iPhone's release, a large and ever-growing community of hackers began to develop methods for "jailbreaking," "hacktivating," and "unlocking" it. "Jailbreaking" opens up the operating system so that third party applications can be installed, while "hacktivating" augments or bypasses the iTunes-based activation process in order to trick the iPhone into "thinking" it has been activated with the officially designated wireless carrier. "Unlocking" an iPhone releases the SIM card lock and allows an individual to use any wireless network.[22] While these interventions are practical in that they give individuals freedom of choice in regard to wireless service providers and the kinds of applications they

---

[19] Similar deals were signed with carriers in other countries and in a few cases, such as Italy, Apple signed a deal with more than one carrier.

[20] While a number of countries including Germany and France require Apple and their locally designated wireless carrier to make unlocked versions of the iPhone available to customers, albeit often at twice the price, no such requirement exists in the U.S.

[21] GSM (Global System for Mobile communications) is the leading mobile communication standard in the world. Currently, of the four major wireless service providers in the U.S., only two (AT&T and T-Mobile) support GSM.

[22] While the exact definitions of "jailbreak," "hacktivate" and "unlock" vary and at times overlap, the definitions used in this paper attempt to summarize those used most often within the online hacker community. In particular, the post "Jailbreak is not Activate is not Unlock" from the Hackint0sh Forums, was a useful guide. The post was accessed on June 9, 2008 and can be found here: http://www.hackint0sh.org/forum/showthread.php?t=32703

want installed on their devices, they are also forms of political engagement because they challenge—often quite intentionally--the monopolistic business practices of Apple and AT&T.

It was a 13-year-old boy known as "AriX" who developed iJailBreak, the first of its kind available for the iPod Touch and one of the most popular jailbreak applications available for the iPhone. iJailBreak is a FOSS application that once downloaded to and run from an individual's computer, uses an automated process to "jailbreak" an iPod Touch or iPhone. The iJailBreak application is available to all as a free download and is licensed under the GNU General Public License v2, which ensures its status as a free and open-source program.[23] At just 13 years of age, AriX had an influential and expansive digital footprint, including iJailBreak.com, the website jointly maintained by AriX and his 13-year-old friend Ben.[24]

Two interviews conducted recently with AriX reveal not only a playful hacker who developed iJailBreak through personal exploration and community contacts, but also a young person who understands his own experiences in opening up and demystifying the iPhone in relation to the broader politics at play in his technological environment. Displaying a hacker ethic, AriX appears to be less interested in material gain than in the joy of hacking itself, though he also seems to enjoy the notoriety and regard associated with it as well.

In one interview conducted on March 26, 2008 with a British blogger and made available as a podcast, AriX sounded every bit your ordinary 13-year-old boy. In between laughter, self-deprecating apologies, and the background screaming of his younger brother, however, AriX displayed an extraordinary knowledge of both the iPhone and the corporate policies of Apple, particularly when discussing Apple's plan to allow third-party applications on the iPhone through a more controlled and commodified process officially facilitated through an iPhone Application "Store." This sort of privileged arrangement is, of course, intended to limit the free-flowing exchange of FOSS applications available to those who have jailbroken iPhones.

At the time of this interview, Apple had released an iPhone Software Development Kit (SDK) that allowed programmers to build programs for use on the iPhone once Apple made its move to sanction and even facilitate third party applications. When the interviewer noted that SDKs tend to be closed, meaning that the application programming interfaces provided to participants are often heavily regulated by their provider, AriX hesitated to reply. Aware of the Non-Disclosure Agreement to which

---

[23] The GNU General Public License v2 can be found here: http://www.gnu.org/licenses/gpl-2.0.txt. Interestingly, "GNU" itself is a hack, it is a recursive acronym crafted by Stallman who made the "copyleft." It stands for "GNU's Not Unix" since GNU is the free OS he developed in contrast to the proprietary Unix (which AT&T owned).

[24] As of June 8, 2008, iJailbreak.com was linked to by 507 people on *del.icio.us* (a popular social bookmarking service- http://del.icio.us), had a rank of 1,092 on *Digg It* (a popular social-ranking service- http://www.digg.com) and had received 541 blog reactions according to *Technorati* (the most popular blog search engine- http://www.technorati.com). AriX's *Twitter* (a simplified social-networking service) account boasted 355 "followers" (http://twitter.com/AriX).

he was bound as a user of the iPhone SDK, AriX proceeded with a measured yet interesting insight:

> *Ok, this is hard… at the announcement they said these were the same tools that they were using to develop their applications. That's not true. I'm not going to go any further. The applications that are on the iPhone are more powerful than what you can do with the SDK.*

At just 13, AriX had already experienced the "world of difference" Papert (1993, 5) noted "between what computers can do and what society will choose to do with them." Continuing on this theme, the interviewer noted that he had heard rumors suggesting that only Apple's applications would be able to "multitask." AriX replied,

> *The truth is that that's just a guideline. They are suggesting that you don't do that. Now, the sad truth may be that they won't let applications on the app store [iPhone Applications Store] that will stay open in the background; that may happen.*

AriX then proceeded to discuss how another SDK programmer used the jailbreak method to develop a hack that allows programs to stay open, and concluded:

> *I'm 100 percent sure that Apple will let AOL run their AIM program in the background.*

The speculation among programmers and raised by the interviewer is that applications produced by third parties will not be able to run simultaneously with other programs on the iPhone, requiring the user to close one program completely before running another one. AriX's response is notable because he refutes this rumor as a "guideline" not a limitation and cites an example of a programmer who has figured out how to create a program that "multitasks." Additionally, he points out that Apple may "choose" to restrict such applications from their online store and acknowledges the likelihood that America On Line (AOL) would be allowed to create an AOL Instant Messenger (AIM) application that runs in the background. AriX is clearly astute in his understanding that the power of closed proprietary systems lies in controlling who has access. While corporations like AOL aren't likely to find themselves restricted by the iPhone, the "mom and pop" operations that generate the majority of FOSS applications available through hacktivated iPhones at present may well be shut out.

In an article entitled "Hacking: The New Child's Play?" posted on an IT security website, AriX is associated with a list of young crackers who have engaged in malicious and clearly criminal activities. With the subtitle "Researchers worry as teens and pre-teens play an increasing role in illegal online exploits," the piece makes no distinction between the hacking of AriX and the reported computer crimes of the other youth profiled, even though the latter's activities included derailing trains in the Polish city Lodz and stealing considerable sums of money from people's bank accounts (Wilson 2008). The distinction between these activities and hacking

like AriX's is clear. But even at that, the U.S. Librarian of Congress granted six exemptions to the DMCA in 2006. The fifth exemption was

> *Computer programs in the form of firmware that enable wireless telephone handsets to connect to a wireless telephone communication network, when circumvention is accomplished for the sole purpose of lawfully connecting to a wireless telephone communication network* (Librarian of Congress 2006).

While jailbreaking, hacktivating, or unlocking an iPhone may void its warranty, it is not illegal. Wireless telephone communication networks such as AT&T are legally entitled to "lock" hardware into their services, but they cannot stop individuals from unlocking that hardware and legally using it with another wireless telephone communication network.

Torin Monahan (2006) points out that within much of the security discourse young people are framed as either "criminals" in need of policing or "victims" in need of protection. With the criminal side of this binary inapplicable, perhaps AriX is a victim caught up in a complex and dangerous technological environment beyond his understanding? Not so, according to his mom. Dropping in for a guest appearance at the end of one interview, AriX's mother was asked how she felt about his hacking. She responded:

> *Well, we've had some concerns about repercussions, but in general we are very proud of what he has accomplished. And he has been really careful about explaining all of the potential repercussions. And when he is not concerned, we are not concerned… he's a good kid* (Helm 2008).

In a separate interview with another blogger on February 1, 2008, AriX is joined by his friend/co-hacker Ben. When asked by the interviewer what their favorite movie was, Ben exclaimed,

> *I don't watch movies—I won't support the MPAA or RIAA—same reason I won't buy from iTunes* (Jordan 2008).

Based on the limitations of this particular interview it's impossible to assess whether Ben's resistance towards the MPAA (Motion Picture Association of America) or the RIAA (Recording Industry Association of America) motivates his hacking or if his hacking has motivated his resistance. What we can deduce is that there is a relationship between the two. As powerful trade groups representing the U.S. recording and motion picture industries, the RIAA and the MPAA have been at the forefront of promulgating means of ensuring copy and content protection known as Digital Rights Management (DRM). They were prominent backers of the Digital Millennium Copyright Act (DMCA), which sets tight controls on the use of copyrighted works and criminalizes the circumvention of those controls. It seems that Ben would rather forgo watching movies than capitulate to the MPAA's control

of their circulation. Likewise, his boycott of iTunes is due to Apple's reluctant policy of encrypting the music it sells to control the music files' circulation.[25]

AriX is a skilled and savvy actor in an evolving technological environment. He is neither a victim nor a criminal. As his environment becomes increasingly proprietary and privatized, hackers like AriX and Ben make sure that vibrant avenues for free play and experimentation are still available. Through playful exploration of the technological environment they are empowered, not endangered. AriX's mom understands this, but perhaps more surprisingly, so do the researchers at the Crimes against Children Research Center (CCRC) whose recent findings challenge the perception of young people as naïve victims-in-waiting online.

Narratives of young people victimized by sexual predators through the Internet have become commonplace, typically highlighted by politicians and sensationalized in the media. Yet a study published in 2008 by CCRC challenges this received wisdom (Wolak et al. 2008). Among the study's findings was that the discourse around young people as "vulnerable" to online sexual predators due to "naïveté about the Internet itself is not accurate." The authors note that by early adolescence young people "generally understand the social complexities of the Internet at levels comparable to adults." Young people, it seems, are more commonly informed and self-possessed around the Internet than they are its helpless or naïve victims. Any intervention in the name of protecting young people from unwanted electronic contact should acknowledge their agency and promote their critical thinking skills. Protectionist measures such as surveillance, "filtering," and outright censorship are antithetical to this understanding and work against its grain. In the long run, such strategies can debilitate young people's critical capacities and encourage their attenuated dependence on parents and others to make social judgments and decisions on their behalf.

Moreover, as the case of PeaceFire.org clearly demonstrates, filtering and censorship measures draw on methodologies that are not only somewhat omnivorous in what they block, but also can be subverted pretty easily by young people. Started by Bennett Haselton when he was 16 years old, PeaceFire.org has helped to expose the flawed practices of filtering software by revealing the blocking of human rights websites such as Amnesty International, candidate websites from the 2000 elections, and even pro-blocking websites such as FilteringFacts.org. PeaceFire.org also helps to connect children and young people with proxies that

[25] We use the word "reluctant" to describe Apple's encryption policy since Steve Jobs, Apple's founder and CEO, has openly called for its change. Digital music files are typically found in MP3 format, yet digital music downloaded from iTunes includes an extra layer of Digital Rights Management (DRM) encryption in the MP4 format. This extra layer of encryption limits to five the number of machines one is allowed to copy the file. Jobs wants to remove the DRM encryption layer and has cited the major record labels as the reason why Apple must include it. Steve Jobs' letter, "Thoughts on Music," can be found here: http://www.apple.com/hotnews/thoughtsonmusic/.

allow them to circumvent filters.[26] While protectionist measures are often flawed and ineffective, the message they send to kids is unmistakable: you are being monitored and your access to information is being filtered, and/or censored. Whether they "work" or not, such strategies are built upon and foster a basic distrust of young people and their capacity to understand information and read social situations. Restricting the choices available to youth in their technological environments, these strategies narrow the ambit of their engagements and reinforce the tired notion that kids are always threatened and threatening.

Conclusion

The "Cookie Monster" is one of the earliest known computer viruses. Once installed on an individual's computer it would periodically interrupt computing and present a message demanding a "cookie," much like the Sesame Street muppet with whom the virus shares a name. When the individual typed "cookie," the virus would recede to the background only to return for more cookies later. According to Turkle (2005, 212), the Cookie Monster was used as a "hacker harassment" program to test new hackers at MIT. If an individual could slay the Cookie Monster, and thus prevent it from seeking future cookies, they proved themselves as a hacker.

In the contemporary commercial and security environment we confront a new breed of "cookie monsters," much less amusing and potentially quite harmful. Most obvious are the digital cookies that have become so ubiquitous in cyberspace that few people take notice of them, which is exactly the problem. "Cookies" are digital files automatically placed on an individual's computer upon visiting most websites. These files then communicate information about an individual's online activities and preferences back to the server of the website that planted the cookie. Teens and college students combined spend nearly $400 billion a year, and now spend more time in cyberspace than in front of the TV (Harris Interactive and Teenage Research Unlimited 2003). The information gathered by these cookies on their computers is an invaluable commodity to business and government. Classifying cookies as one of many "technologies of control," Castells (2002, 173) notes that such technologies work only under the condition that "controllers know the codes of the network" while "the controlled do not." Ensuring that this condition is maintained, capital and the state pursue policies and programs that are dedicated to what can only be called "hacker harassment." Overcoming these "hacker harassment" programs not only would make someone a hacker but also an empowered player—an informed citizen—in the technological environments of contemporary life. And it is these sorts of possibilities, and their impediments, that we have been detailing here.

Whether it is the proprietary shift in the OLPC project, the monopolistic business practices of AT&T and Apple, or the separation of play and work in the computer lab, the spatial-temporality of children and youth's technological environments is often configured to restrict their freedom of choice and behavior. These measures dovetail with others taken around children's technological and everyday

[26] While web filters aim to block access to certain websites deemed "harmful" to young people, proxy servers function to allow access to these blocked websites by accessing the site on an individual's behalf.

environments in the name of "security." Whatever the impulse, these managed environments serve to produce and reproduce an informational ideal wherein youth are cast as complacent and vulnerable "users," with much of their potential agency underestimated and undermined rather than encouraged. Yet as we have shown, young people are often informed, savvy subjects of their technological environments who have time and again proven themselves quite capable of negotiating the various changes and challenges these environments pose. Through hacking and other strategies, young people can better comprehend and assert control over their environments (technological and otherwise), at once learning as they go and helping to ensure that the effects of the forces structuring these environments remain indeterminate.

Whether playful, political, geeky, or all three, when young people manage to hack their technological environments through practices such as Logo and its descendents, subverting the Mosquito, or jailbreaking the iPhone, they are reclaiming some degree of freedom regarding their choices and behaviors in these and other settings (cf., Proshansky, Ittelson and Rivlin 1972). When they develop organizations such as PeaceFire.org or create collaborative mechanisms like ITS, young people produce opportunities for better understanding and reworking technological environments and the claims they place on their time, space, and subjectivity. As a hacker, AriX was neither threatening nor threatened in his technological environment. Rather, by challenging the "cookie monster," in this case, Apple and AT&T's lock on the iPhone, he became both empowered and empowering. Empowered by his experiential knowledge, which allowed him to increase his freedom of choice and behavior with the iPhone, AriX was simultaneously empowering—and surely inspiring—to others with his iJailbreak application.

In this context, hacker culture can be understood as a source of power in the economic restructuring motivated by informationalism, as well as with regard to what Zuboff (1988) dubbed informating.[27] Informating refers to the sorts of data that become available through the use of information technologies in the workplace to transform information into action. Zuboff notes that while this information is available to people such as workers who are engaged directly in processes subject to informating, it is simultaneously available to those who would monitor and/or supervise those interactions. Zuboff's focus was the workplace and the new modes of labor, supervision, and discipline informating made possible. At a whole other scale, the Semantic Web and digital "cookies" work in a similar fashion, with similar contradictory effects on people's privacy and thus their freedom of choice and behavior as well. The extensive information aggregated by cookies, which helps open the sluices of commerce around young people, and the way the Semantic Web makes such information more circulatory, paves the way for greater state surveillance and more intimate, targeted, and seductive product marketing.

[27] According to Manuel Castells (2001, 159), "informationalism" is "a technological paradigm based on the augmentation of the human capacity in information processing around the twin revolutions in microelectronics and genetic engineering."

Hacking can be understood as part of a struggle to subvert or neutralize such attempts to control and circulate information and the myriad assaults on privacy that they represent. This is why corporate and state regulation of hacking—through the criminalization of certain behaviors in certain spaces and the commodification and privatization of technological environments through such things as proprietary software and careful restrictions around intellectual property rights—is intent on rationalizing, aggregating, and using such power to reinforce "security" rather than call it into question. If hacking, in its broadest and most creative sense, is encouraged among young people in their encounters with the technological environment at home and school, then maybe everything will be new AND different, as security measures that erode privacy and thwart autonomous initiative start to give way to open and collaborative work, play, and learning that expand kids' freedom of choice, and thus just might secure the future.

Gregory T. Donovan *is a Ph.D. candidate in Environmental Psychology and a certificate candidate in Interactive Technology and Pedagogy at the Graduate Center of the City University of New York. He has held fellowships at the Center for Place, Culture, and Politics, the Macaulay Honors College, and the Stanton/Heiskell Center for Telecommunication Policy, and has conducted research at the CUNY New Media Lab, the Public Space Research Group, the Housing Environments Research Group, and with several children's educational media groups. His research operates at the intersection of Urban Studies, Youth Studies, and Internet Studies, with a focus on understanding the mutual shaping of digital environments and young people's communication, political engagement, play, and self-expression.*

Cindi Katz *teaches at the Graduate Center of the City University of New York. Her book,* Growing Up Global: Economic Restructuring and Children's Everyday Lives, *won the AAG Meridian Award in 2004. Her work on social reproduction and the production of space, place and nature has been published in* Society and Space, Signs, Antipode, Social Text, Social Justice, Annals of the Association of American Geographers, Cultural Geographies, Transactions of the Institute of British Geographers, Gender, Place and Culture, *and* Feminist Studies. *Her current projects include a study of contemporary U.S. childhood as spectacle, research on the intertwined spatialities of homeland and home-based security, and a project on activism, social reproduction, and the enduring effects of Hurricane Katrina in New Orleans.*

References

Ackermann, Edith (2001). "Piaget's Constructivism, Papert's Constructionism: What's the Difference?" Available from: http://maggiehu.china.googlepages.com/EA.Piaget_Papert.pdf.

Air Force Cyber Command (2008). "Air Force Cyber Command Recruiting Video." Online video clip. YouTube. Available from: http://www.youtube.com/watch?v=t849CYRd2Ak&eurl.

Bateson, Gregory (1956). "The Message 'This is Play'." In Schaffner, Bertram, ed. *Group Processes*. New York: Josiah Macy Jr. Foundation, 145-242.

Castells, Manuel (2001). "Informationalism and the Network." In Himanen, Pekka, ed. *The Hacker Ethic and the Spirit of the Information Age*. New York: Random House, 155-178.

-----(2002). *The Internet Galaxy: Reflections on the Internet, Business, and Society*. New York: Oxford.

Chopra, Samir and Scott Dexter (2007). *Decoding Liberation: The Promise of Free and Open Source Software.* New York: Routledge.

Crum, Rex (2007). "Apple Hits iPhone Sales Target Ahead of Forecast." *MarketWatch*, 10 September. Available from: http://www.marketwatch.com/news/story/apple-hits-iphone-sales-target/story.aspx?guid={4A58F9DF-D43E-4958-8862-FB38E4A676D2}.

Dewey, John (1916). *Democracy and Education: An Introduction to the Philosophy of Education.* New York: The Macmillan Company.

Ginsberg, Kenneth R., the Committee on Communications, and the Committee on Psychosocial Aspects of Child and Family Health (2007). "The Importance of Play in Promoting Healthy Child Development and Maintaining Strong Parent-Child Bonds." *Pediatrics* 119(1): 182-90.

Harris Interactive and Teenage Research Unlimited (2003). *Born to Be Wired: The Role of New Media for a Digital Generation—A New Media Landscape Comes of Age*. Executive Summary. Sunnyvale, CA: Yahoo! and Carat Interactive.

Helm, Stu (2008). "BUMP 031: iPhone SDK & Jailbreaking with AriX." 26 March. Podcast. "British Users of Mac Podcast." Available from: http://bump.i-believe.biz/podcast/bump031.mp3.

Himanen, Pekka (2001). *The Hacker Ethic and the Spirit of the Information Age*. New York: Random House.

Hourcade, Juan Pablo, Daiana Beitler, Fernando Cormenzana, and Pablo Flores (2008). "Early OLPC Experiences in a Rural Uruguayan School." In *CHI '08 Extended Abstracts on Human Factors in Computing Systems* (Florence, Italy, April 05-10, 2008). ACM, New York. 2503-2512. Available from: http://doi.acm.org/10.1145/1358628.1358707.

Jordan, Patrick (2008). "What's It Like to Be a 13-Year Old iPhone Jailbreak Creator." *Just Another iPhone Blog*, 01 February. Available from http://justanotheriphoneblog.com/wordpress/2008/02/01/interview-whats-it-like-to-be-a-13-year-old-iphone-jailbreak-creator/.

Katz, Cindi (2001). "The State Goes Home: Local Hypervigilance and the Global Retreat from Social Reproduction." *Social Justice* 28(3): 47-56.

-----(2004). *Growing Up Global: Economic Restructuring and Children's Everyday Lives*. Minneapolis: University of Minnesota Press.

-----(2008). "Me and My Monkey: What's Hiding in the Security State." In Sorkin, Michael ed. *Indefensible Space: The Architecture of the National Insecurity State*. New York: Routledge, 305-23.

Kraemer, Kenneth, Jason Dedrick, and Prakul Sharma (2008). "One Laptop Per Child (OLPC): An Education Project or a Laptop Project?" *Personal Computing Industry Center*, University of California, Irvine. Available from: http://pcic.merage.uci.edu/papers/2008/OneLaptop.pdf.

Krazit, Tom (2008). "iPhone Unlocking Explodes Despite Apple's Countermeasures." *CNET News.com*, 30 January. Available from: http://news.cnet.com/8301-13579_3-9860766-37.html.

Krstić, Ivan (2008). "Sic Transit Gloria Laptopi." *code culture*, 13 May. Available from: http://radian.org/notebook/sic-transit-gloria-laptopi.

Lave, Jean and Etienne Wenger (1991). *Situated Learning: Legitimate Peripheral Participation*. Cambridge and New York: Cambridge University Press.

Librarian of Congress (2006). "Statement of the Librarian of Congress Relating to Section 1201 Rulemaking." *U.S. Copyright Office*, 22 November, Washington, D.C. Available from http://www.copyright.gov/1201/docs/2006_statement.html.

Lohr, Steve (2008). "Why Walter Bender Left One Laptop Per Child." *The New York Times*, 27 May. Available from: http://bits.blogs.nytimes.com/2008/05/27/why-walter-bender-left-one-laptop-per-child-edited-hold-for-wed-am/.

Lowes, Susan, and Cyrus Luhr (2008). "Evaluation of the Teaching Matters One Laptop Per Child (XO) Pilot at Kappa IV." *Institute for Learning Technologies*, Teachers College/Columbia University. Available from: http://www.teachingmatters.org/evaluations/olpc_kappa.pdf.

Microsoft (2008). "Microsoft and One Laptop per Child Partner to Deliver Affordable Computing to Students Worldwide." Microsoft Corp. 15 May, 2008 Press Release. Available from: http://www.microsoft.com/presspass/press/2008/may08/05-15MSOLPCPR.mspx.

Monahan, Torin (2005). *Globalization, Technological Change, and Public Education*. New York: Routledge.

-----(2006). "The Surveillance Curriculum: Risk Management and Social Control in The Neoliberal School." In Monahan, Torin, ed. *Surveillance and Security: Technological Politics and Power in Everyday Life.* New York: Routledge, 109-124.

Moore, J.T.S., dir. (2002). Performances by Linus Torvalds, Richard M. Stallman, Eric Raymond, Bruce Perens, and Larry Augustin. *Revolution OS* (DVD). Wonderview Productions.

Open Education (2008). "Walter Bender Discusses Sugar Labs Foundation." *Open Education*, June 3. Available from: http://www.openeducation.net/2008/06/03/walter-bender-discusses-sugar-labs-foundation/.

Papert, Seymour (1991). "Situating Constructionism." In Harel, Idit and Seymour Papert, eds. *Constructionism*. Norwood, NJ, Ablex Publishing, 1-11.

-----(1993). *Mindstorms: Children, Computers, and Powerful Ideas*. New York: Basic Books.

Patterson, Meredith L., Len Sassaman, and David Chaum (2008). "Freezing More Than Bits: Chilling Effects of the OLPC XO Security Model." In Churchill, E. and R. Dhamija, eds. *Proceedings of the 1st Conference on Usability, Psychology, and Security* (San Francisco, California, April 14 - 14, 2008). Berkeley, CA: USENIX Association, 1-5.

Proshansky, Harold M., William H. Ittelson, and Leanne G. Rivlin (1972). "Freedom of Choice and Behavior in a Physical Setting." In Wohlwill, Joachim F. and Daniel H. Carson, eds. *Environment and the Social Sciences: Perspectives and Applications.* Washington, D.C.: American Psychological Association, 22-43.

Raymond, Eric S. (2000). *A Brief History of Hackerdom* (v1.24). Available from: http://www.catb.org/~esr/writings/cathedral-bazaar/hacker-history/.

Roush, Wade (2008). "One Laptop Per Child Foundation No Longer a Disruptive Force, Bender Fears: Q&A on His Plans for 'Sugar' Interface." *Xconomy*, 24 April. Available from: http://www.xconomy.com/2008/04/24/one-laptop-per-child-foundation-no-longer-a-disruptive-force-bender-fears-qa-on-his-plans-for-sugar-interface/.

Talbot, David (2008). "$100 Laptop Program's New President." *Technology Review*, May 2. Available from: http://www.technologyreview.com/Biztech/20711/.

Torvalds, Linus (2001). "What Makes Hackers Tick? A.K.A. Linus's Law." In Himanen, Pekka, ed. *The Hacker Ethic and the Spirit of the Information Age*. New York: Random House, vii-xvii.

Turkle, Sherry (2005). *The Second Self: Computers and the Human Spirit*. Cambridge, MA: MIT Press.

Vygotsky, Lev S. (1978). *Mind In Society: The Development Of Higher Psychological Processes*. Cole, Michael, Vera John-Steiner, Sylvia Scribner, and Ellen Souberman, eds. Cambridge, MA: Harvard University Press.

Wilson, Tim (2008). "Hacking: The New Child's Play?" *DarkReading*, March 5. Available from: http://www.informationweek.com/story/showArticle.jhtml?articleID=211201223.

Wolak, Janis, David Finkelhor, Kimberly Mitchell, and Michele Ybarra (2008). "Online 'Predators' and their Victims: Myths, Realities and Implications for Prevention and Treatment." *American Psychologist* 63: 111-128.

Zuboff, Shoshona (1988). *In the Age of the Smart Machine: The Future of Work and Power*. New York: Basic Books.