ACCESS: CONTEMPORARY ISSUES IN EDUCATION
1997, VOL. 16, NO. 1, 36–43

Privacy, surveillance, and classroom communication on the internet

Nicholas C. Burbules

ABSTRACT
As more and more people are involved with the Internet and new technologies of data collection and record-keeping, there has been a growing anxiety expressed about the loss of privacy citizens face in a networked world. In schools and in other networked institutions the activities of those working and communicating on the Internet are continuously subject to surveillance by others. These developments appear to threaten an increased 'invasion of privacy'. This essay critically reviews the notions of 'invasion' and 'privacy' at work here, concluding that the ideal of privacy people are seeking to protect - especially for students in schools - is already to a large extent imaginary. Moreover, when the same state institutions that threaten privacy also undertake to 'protect' is (such as schools), resistance rather than cooperation is an understandable response.

From the recent popular film 'The Net' to countless news features in the media, there is a growing sense of awareness of the vast implications of digital technologies for traditional assumptions about privacy. The volume of information that is instantly recorded whenever one uses a credit card, travels the Internet, visits a hospital or pharmacy, files a tax return, rents a film on video tape, and so on - information that can be accessed by authorized and unauthorized persons alike - has t hanged the speed and ease with which much of one's personal life and activities (including the circumstances of one's body) can be surveyed by others. The central premise of 'The Net', that a young woman's entire life and identity could be erased and replaced with another by altering her digital records, feeds and feeds off of a popular suspicion that the Net we use is also the net in which we are caught.

Real and disturbing as these concerns are, however, they only begin to address the changes that are taking place in what we have considered our 'private' space. Upon further reflection, the very existence of a discrete, autonomous private space seems to have dissipated long ago, and the facility of certain digital means of access has only made more apparent changes that have been at work for more than a century. Furthermore, the idea that this private space is being 'invaded' suggests that we can easily sort out the legitimate from the illegitimate sources of observation and recording that reach into our personal lives. This essay will question the ideas of 'privacy' and 'invasion' at work here.

This topic is of special concern for educators. Children, and especially children in schools, have frequently been among the first to be examined, tested, charted, and evaluated, their performance tracked over time - techniques that, once perfected and legitimated in their use with the very young,

© 1997 Philosophy of Education Society of Australasia

have often found their way into more and more areas of society generally (see Foucault, 1977 for the different senses of 'examination' at work here).

Students usually have very little privacy: from having to announce to the entire class when they need to use the toilet; to being observed through one-way mirrors; to having their desks, lockers, and persons subject to search; to having their property subject to confiscation; to having their correspondence (such as passed notes) subject to seizure and scrutiny by authorities; to having few opportunities aside from the hallways, the toilets, or the playgrounds to engage in conversation with one another. Students in most schools have to accept encroachments upon their personal activities and social interactions that few adults would tolerate without outrage. The fact that these 'invasions of privacy' have usually been justified as well-intended and practiced in the students' best interests must be seen as part of the process by which such practices come to appear innocent, legitimate, normal - even necessary - features of social life.

As classrooms enter the digital age, these two broad trends come into contact with one another: the capacity of computer networks to record and survey personal information, and the long tradition of schools to examine and discipline students 'for their own sake'. One of the main benefits of digital technologies is in promoting new and more rapid forms of communication and information-sharing among users. Where these users are students, however, it is easy to anticipate some of the ways in which their communications and other uses of the Internet will be subject to screening if not outright censorship - as is already becoming apparent. But as we peel through four layers of this problem, we will come to see that 'invading privacy' is not the most disturbing aspect of this process at work. By the end of this essay, the very meaning and value of 'privacy' in schools (and in society generally) will be viewed in an inverted fashion: less as a haven from state surveillance, and more as a confirmation and legitimation of it.

I.

With networked computers in which certain kinds of file sharing have been activated, it is possible to survey everything from the text of users' e-mail correspondence, to the World Wide Web sites they have visited, to the contents of their hard drives. School students are not the only ones subject to such scrutiny: in the United States many states and private businesses have mandated that computers used in work environments cannot be used for games and that hard drives can be searched to find and expunge such software - the same can be done with 'pirated' software that is not registered to the user. Of course, the rationale goes, these are 'illicit' uses of the technology, which justifies such surveillance and intervention.

In the U.S. the recently passed (though now in court-imposed limbo) *Communications Decency Act* seeks to establish broad-ranging powers to limit what some consider 'indecent' materials on the Internet. This l aw is a major initiative by conservative politicians, undertaken, they say, to 'protect the children' (although its effects would restrict everyone's access to certain materials, not only children's). At what might be called the opposite end of the political spectrum, many have called for screening e-mail and Web site content to eliminate sexually harassing material. It is easy to see the rationale for such policies: Do we want children to have free access to pornographic materials? Do we want adults using the Internet to solicit sexual liaisons with underage youth? Do we want to allow threatening, pornographic, or racist e-mail to be sent to individuals for the sole purpose of harassing them?[1]

Such questions seem to be especially pointed when we are dealing with young people who may have fewer resources to protect themselves from unwanted materials and may exercise less experienced judgment in how they use digital technologies. However, these assumptions are far from undebatable, in view of the fact that youth are often much more savvy and discerning in their understanding and use of the Internet than the adults who worry about them. (Indeed, this may be part of the underlying problem: that adults who do not understand these technologies assume the

most insidious uses for them and assume that young people are more vulnerable to offensive materials than they may in fact be. (Katz, 1996))

In the decentralized and anarchic context of the Internet such material cannot be effectively censored or banned at the point of production, so the currently evolving approach seems to be a heightened degree of surveillance and filtering at the point of reception. Several software programs allow users (or their parents or teachers) to block access to different categories of Internet materials. In schools messages sent and received by students can be screened and censored. As noted, however, such interventions must be seen as less an invasion of some privacy that students once had, than a continuation of attitudes and practices that have always governed how young people in schools are treated.

Thus the central questions arising at this stage of the discussion are not, How do we avoid invading students' privacy? but, What kind of privacy have students ever had? What circumscribed notion of 'privacy' are we trying to protect, and is protecting it - that is, maintaining its boundaries from further encroachment - also, ironically, a way of maintaining its boundaries from further *expansion?* By accepting certain tacit institutional practices and circumstances that have become so commonplace that we have stopped questioning them, are we in fact conceding a notion of 'privacy' for students that is already so circumscribed that it is more worthy of critique than of preservation?

II.

Perhaps the most-discussed section of Michel Foucault' s *Discipline and Punish* is his description of Jeremy Bentham's dream (or nightmare) of the panopticon, a system of surveillance originally designed with penal institutions in mind, but which has become a metaphor for the much broader and more subtle intrusion of observation and record-keeping techniques into more and more areas of social life (Foucault, 1977: 200-209; see also Poster, 1990: 69-98). The basic idea of the panopticon is straightforward: a central tower or structure has windows on all sides, and it is in turn surrounded by a ring of cells occupied by the inmates, the open sides facing inward. Observers can look out in any direction, at any time, to see what any inmate might be doing. Furthermore, since the inmates cannot see into the central observation tower, every window or observation point does not, in fact, need to be staffed all the time; the *possibility* of being observed has a deterrent effect even when inmates are not in fact being observed. And, still further, as inmates become accustomed to this environment, and to the routine of assuming that they are being observed at any/every time, it becomes less important for the observation tower to be staffed at all; the structure of the environment is what exerts control, as people internalize changes to their habits and movements without remembering the original circumstances that necessitated them. The panoptic condition becomes part of the identity of an inmate ('a madman, a patient, a condemned man, a worker or a schoolboy' (Foucault, 1977: 200)).

Several deeper conclusions follow from Foucault' s discussion. The first is that such mechanisms of surveillance tend to become more pervasive: for example, few people even notice any longer how frequently they are monitored through partially hidden video cameras (from the bus or subway, to the bank, to the store, to the parking lot, to the elevator). All sorts of activities, and not only illegal activities, are inhibited by such surveillance. Now, everyone knows that such observation is supposed to *protect* people from assault or robbery, and in many communities people are up in arms because they want more protection, not less. But this is one of the central themes of Foucault' s book: that as the mechanisms of surveillance and control become more subtle and 'humane', they become more extensive; they actually become more controlling in their effects, but with less complaint.

For example, in schools, it is a commonplace that sitting in a circle is a more humanistic, egalitarian arrangement of persons in a classroom than the old row-by-row seating design.

Progressive educators have pushed this idea for years. Yet, ironically, from a Foucauldian standpoint, a circular arrangement is in fact a more effective panopticon, since every member of the circle is continuously visible to every other member, all the time. No skulking in the back row to sneak a candy bar into one's mouth! And again, even when one is in fact not being observed, at any moment one might be, and that is all that matters. Furthermore, all members of the circle become conspirators in the panopticon, observers and observed; what the teacher might not see, others will.

The panopticon, then, is not a simple physical structure, machine, or spatial arrangement: it becomes a way of life. As people accept the inevitability of being observed and recorded, their habits change; *they* change. As people become *more* visible, the omnipresent circumstances that observe and record their lives become *less* visible. As the 'private' domain (the space of activity that is in principle unobservable, unrecordable) has become more and more circumscribed, an alarm about its now being 'invaded' seems ironic, for the real issue is with how that domain has become already so compromised; yet these restrictions, because they are often consensual, implemented gradually and with good sensible reasons, are actually more pervasive and insidious and hence harder to resist.

Finally, and at the extent where the panopticon ceases to be a discrete physical structure or mechanism, but simply a feature of ways of living together, what does the distinction of 'public' and 'private' spaces mean any longer? For the ancient Greeks, this distinction actually corresponded to discrete physical locations, the *agora* and the household, two separate realms of activity and human relation. This essay is not the place to engage the larger question of the status of such public and private spaces; but in a panoptic society people carry many of the attitudes and self-imposed restrictions of activity from the surveyed public into their private life - so in what sense is it still 'private'?

What this discussion shows is that restrictions on 'privacy' are often consensual in the sense that people give up certain degrees of freedom for the sake of protections that they believe preserve or enhance other freedoms. What is not seen is that this apparent tradeoff commits society to a basic dynamic that inevitably means a gradual diminishment of freedom and privacy in any sense at all. Spaces of free action are increasingly circumscribed by restrictions on freedom. These paradoxical tendencies come together in the idea of an *architecture* - not merely the physical architecture of buildings (or panopticons), but the social architecture of ways of living. An 'architecture' can be seen as the locus where capabilities of creativity and mechanisms of control come together: architectures both contain and exclude, and the analysis of distinctive architectures (again, not only physical architectures) can reveal important dimensions, and limitations, of human freedom. The Internet is such an architecture; while a medium that is enormously powerful and susceptible of quite varied uses, it includes constraints (as does any medium) on how information is shared, what sorts of information can be shared, and how people can communicate. It both enables and inhibits.

Within educational contexts and others, this paradox is of fundamental importance for thinking about the relation of new technologies to learning and human freedom: the *very same* devices that allow the creation, exploration, and sharing of new knowledge and information, that spark new possibilities of action and interaction, also facilitate a heightened degree of observation and record-keeping about what people actually do. The dynamics of simultaneous production and recording are clearly linked within communications media, especially computers (for example, whenever one visits a Web site, one's own address is automatically recorded by that server). One can avoid using such devices, in order to resist having one's freedoms compromised in one sense - but only at the expense of giving up the other kinds of freedoms and opportunities that those new technologies make available. A life without computers, without credit cards, without a passport - indeed, without schooling - may in one sense be less panoptic, and more 'free'; but this freedom is obtained only at the cost of forgoing a number of other opportunities.

III.

However, the language of 'tradeoffs' suggests that these changes in privacy and freedom are primarily a matter of choice, a choice that could be made otherwise. Often a choice is not possible because the very terms of social participation involve restrictions and encroachments upon personal life; moreover, in many contexts, including school contexts, people are *not* asked if they consent to observation. We are, in many circumstances, *already* surveyed with or without our knowledge. William Bogard's *The Simulation of Surveillance* (1996) provides a detailed, discouraging picture of how this happens. Moving beyond a Foucauldian 'panoptic' thesis to the ideas of Jean Baudrillard's *simulacrum* and Donna Haraway's *cyborg,* Bogard argues that today we already inhabit a world constituted by simulations (through new virtual technologies, through the media, through the representations of advertising, and so forth), so that the spaces ('public' *or* 'private') that we occupy are already constructed as imaginaries; they are to a large extent defined for us by cultural circumstances that we do not choose, that we can hardly see beyond, since they predominantly define the horizons of our understanding. Hence, when we think that we are choosing between different possibilities, the choices from which we choose are themselves *not* chosen.

Moreover, the 'we' who choose are partly defined by such technologies as well: we are, as Haraway says, 'cyborgs', humans with a technologically constituted identity. Bogard offers a perceptive analysis of how this happens: of how technologies of simulation and surveillance come together, of how the very processes for exploring or creating a sense of self inherently contain the conditions of surveillance and control as well. I have already mentioned the extensive data collection that takes place, with or without our knowledge. Still further, the increasing use of focus groups, survey techniques, and sophisticated computer modelling have enabled advertisers, marketing agents, pollsters, and politicians to become increasingly adept at developing audience or consumer profiles and predicting the preferences of persons *be fore they have even considered the choices themselves.* Such highly effective social science and psychological techniques are used for everything from helping police to decide which cars to pull over on some pretext and search as high risks for 'criminal' activities, to helping politicians select the homes and neighborhoods on which to focus their 'get out the vote' efforts (or, as some recent U.S. campaigns have shown, neighborhoods in which to work at *discouraging* voting). Such efforts at profiling and prediction are not new, of course: but through the use of various digital technologies they have become much more sophisticated and effective, and extend through more and more areas of our lives (for example, when marketing researchers can analyze the patterns of our credit card purchases). It is sobering to think that when one enjoys a movie, or television show, or politician, or breakfast cereal, it is often because a demographically correct test audience of people very much like us previewed the product and advised the producers on how to change it so that they (we) would enjoy it even more. The product is a simulation designed to fit the audience's expectations; the audience are already-examined cyborgs whose preferences and reactions have been predicted and shaped in advance. We seem to be making a choice as consumers (or as voters, etc.), but it is a choice that was prepared for us to make - of course, we like it; how could we not? Furthermore, as these choices are prepared for us, our tastes and attitudes are changed by them. These 'public' incursions predict and shape our reactions even in the 'private' sphere (what we read, what we eat for breakfast); they are constitutive of the people we are.

Such dynamics are clearly involved in schools. For example, when teachers identify student 'needs' (in order to classify students into different learning categories), and when this identification takes place in terms of examinations normed on assumptions about students, based on previous representative samplings, as well as assumptions about valuable learning objectives, the loop of self-confirming identities closes in upon itself. When a test is *validated* on the basis of a certain percentage of students not doing well at it (a percentage that happens to comprise disproportionate numbers of certain racial and ethnic groups), then how do we judge the outcome when, in fact, members of those groups do 'fail' that test in large numbers? What Bogard wants us

to see is how such processes - common practices in schools and elsewhere - are simultaneously acts of simulation and surveillance: they create knowledge, they create categories and norms, they create identities, and they constrain and direct human behavior. In terms of this essay, these are privacy issues: privacy, because they survey and constitute the identities that students (and the rest of us) carry with us throughout our lives, and because they represent attempts to shape, through modelling and prediction, the horizons of hope and possibility within which we act. Like the panopticon, but even more pervasively, such interventions make us feel that what we do (or fail to do) has been observed and anticipated in advance.

IV.

As noted previously, it is deceptive to justify such actions because students in schools are a special population, because they are younger, or because the school experience is intended to be 'good for them'. Without denying that in fact the intentions of most educators are benign, it needs to be seen how these processes of surveillance and control operate behind the scenes (indeed, teachers are caught up in them as well[2]). The ethos of the liberal state and its institutions and policies is fraught with good intentions; they are the internal as well as external thread of legitimation that allows its daily practices to continue.

This essay has attempted to show that the 'privacy' one might seek to protect for students in schools has long been compromised. Moreover, the boundary of 'public' versus 'private' spheres that such concerns generally rest upon does not exist: in a panoptic society, students and the rest of us carry with us, in our own identities, the tacit restrictions, the categories, the very sense of being observed (examined, tested, surveyed, polled, modelled, predicted) *before* we act or choose. So what does 'protecting privacy' mean any longer?

Bogard makes an excellent point about this as well. The system of digital record keeping and examination prevalent in schools is merely the extension of a larger mode of operation typical of state institutions generally. Maintenance of precise records and ostensibly benign surveillance are integral parts of the process by which state agencies seek to 'help' their clients: the imperatives of bureaucracy (maintaining detailed files as part of orderly business) and of therapeutic practice (observing and recording information to be used in diagnosis and treatment) coincide, reinforcing and legitimating one another.

Collecting mountains of information itself, as well as having legal access to all sorts of information collected by others, the state *creates* a problem of privacy by its own means of operation. Having collected such information and used it for its purposes, the state then presumes to undertake the responsibility of 'protecting' such information and defining what will constitute legitimate and illegitimate uses of it. Yet the potential for 'misuse' is inherent in the very fact that such information is collected and maintained in the first place. Here the scope of 'privacy', and its protection from 'invasion', is nothing more than the self-defined limits that the state allows in the use of information and surveillance data that it has authorized itself to collect (Bogard, 1996: 125-126, 131-133). The state may seek to protect this information, but in the realm of digital technologies no protection is entirely secure, once the information is gathered and stored on-line. Moreover, in deciding itself what will constitute use and misuse, the state cannot readily recognize when its own (possibly well-intended) conduct may be a species of misuse.

To be sure, states often do adopt laws (Privacy Acts, and so forth) that exert real restrictions on their information-gathering activities, and on who can access certain information, and for what purposes. Such laws are not trivial, and they constitute a major area for political contestation and resistance. These restrictions, though real, are restrictions that the state writes, interprets, and imposes upon itself (including the exceptions it grants itself to those restrictions); hence the actual scope of their application is an outcome of the extent to which citizens allow their own horizons of

freedom to be defined for them. This is one way in which the scope of 'privacy' can be rethought as the *outcome* of a process of contestation and resistance, not as a given to be protected.

In the context of public schools, state policies and procedures of record-keeping and examination are supposedly justified by a concern with the best interests of children, protecting them from indecency, harassment, exploitation, or their own illicit conduct; and as noted before one cannot deny that this motivation is frequently sincere. Activities of testing, examining, and categorizing, on the one hand, and activities designed to protect students through surveying or screening their communications *both* are redefined and facilitated by new digital technologies. In many circumstances, they are indistinguishable. They become more effective, more pervasive, and more difficult to recognize and resist.

The free exercise of communication and information-sharing by students has often been regarded by educators as mildly subversive. This is a domain in which students do contest the sphere of 'privacy' that is defined for them. From passing notes surreptitiously, to whispers, to graffiti in the bathrooms (and now in unregulated uses of the Internet) students have always sought to resist surveillance and to find alternate avenues for communication and interaction. Such resistances seek to create a sphere of *unauthorized privacy* that is explicitly not dependent upon the approval of authorities or state 'protections'. This is a second way in which the scope of 'privacy' can be rethought as the outcome of a process of contestation and resistance.

In communications between teachers and students information is often elicited for the purpose of 'helpful' diagnosis of student problems, for the routine examination of student performance, or for the prevention of 'illicit' conduct. Such activities, however well-intended, need to be seen as manifestations of how the state operates at the ground level, how this interaction exists against a background of unequal power (a power dynamic that bears upon different students and groups to different degrees), and how this process *creates* 'privacy' issues: by collecting information that then must be protected from misuse, by shaping attitudes and constructing identities that students carry with them out of the 'public' school and into their 'private' lives, and, generally, by drawing out from students their thoughts and feelings in an asymmetrical relation where the student ends up exposed, and the teacher does not. One response to such requests for information (for confession, as Foucault might say) is *silence* (Marshall, n.d.). This is a third way in which the scope of 'privacy' can be rethought as the outcome of a process of contestation and resistance.

The erosion of privacy has happened through a series of gradual compromises in which the promise of good intentions, on one side, and the promise of trust, on the other, create the mutually sustaining fiction that one can safely trade off the privacy of one's personal life and activities for the sake of greater protection in an increasingly estranged social world: through the acceptance of surveillance, in the expectation that it will only inhibit illicit conduct; the acceptance of new constraints, with the belief that some freedoms must necessarily be limited so that others might be preserved; and the tacit assumption that these are freely made choices, when the very terms of 'choice' are themselves constituted in ways one does *not* choose. In all of these ways, we have found ways to accustom ourselves to the gradual erosion of privacy, to mistakenly hope that increased state interventions are the only way of preserving the privacy that remains. I hope to have made this contradiction explicit.

What I have tried to sketch here is a tension between 'authorized' and 'unauthorized' senses of privacy, and to suggest that the notion of an authorized sphere of privacy, in which the state, having gathered information about nearly every aspect of one's life that it can, promises to protect it and use it only for legitimate purposes, is an oxymoron. Instead, privacy needs to be thought of not as a sphere, certainly not as a 'protected' sphere (protected by whom?), but as an *outcome* of a process of struggle and resistance. The instance of student communication in schools, including the use of digital technologies, I have suggested, help to reveal three general ways in which this resistance might be manifested: (1) by contestation of the self-defined restrictions that the state does impose upon itself; (2) by the maintenance of a scope of *unauthorized privacy* that circumvents, to the

extent possible, the well-intentioned limits and 'protections' that state authorities seek to impose; and (3) by silence, by withholding trust in certain cases, refusing whenever possible to provide information that can be used for the ordinary business of record-keeping, categorizing, modelling, prediction, profiling, and intervention into the choices and decisions, not only of one's self, but of unwilling others. In this, as in many other respects, students may have something to teach the rest of us.*

Notes

1. An excellent overview of privacy issues and computers can be found at the 'Cyberspace Law' web-site. Its URL is <http://www.counsel.com/cyberspace/privacy.html>.
2. When states pass laws requiring teachers to become agents of surveillance, threatening them with fines or dismissal if they do not report 'illegal immigrants' in their classrooms, or teen pregnancies of which they become aware, it is important to see that teachers thereby become objects of surveillance as well as the students they report. And, of course, teachers are subject to centralised 'examination' and record-keeping as well.

*This essay has benefited from the suggestions of Nicole Bishop, Tom Callister, and Jim Marshall.

References

BOGARD, W. (1996) *The Simulation of Surveillance: Hypercontrol in Telematic Societies.* New York: Cambridge University Press.

FOUCAULT, M. (1977) *Discipline and Punish: The Birth of the Prison,* trans. Alan Sheridan. New York: Vintage Books.

KATZ, J. (1996) 'The Rights of Kids in the Digital Age', *Wired, 4,* 7, 120-123, 166-170.

MARSHALL, J. (n.d.) 'Resistance and Friendship: Foucault and de Beauvoir on Silence'. Unpublished manuscript.

POSTER, M. (1990) *The Mode of Information: Poststructuralism and Social Context.* Cambridge, England: Polity Press.