LARRY KUEHN

Surveillance 2.0: The "Information Panopticon" and Education

Naomi Klein, in a recent issue of *Rolling Stone*, describes the new surveillance technologies being developed in both the U.S. and China (the world's biggest potential customers, as well as developers) as "Surveillance 2.0" (Klein, 2008).

Klein describes a high-tech surveillance and censorship program being built and tested in China called the "Golden Shield." It includes close-circuit TV (CCTV) cameras — millions of them — in cities across China. The city of Shenzhen, where many of the cameras are built, expects to have 2 million of them in place within three years.

But the expansion of surveillance goes well beyond CCTV — the key is linking data. The move from Surveillance 1.0 to 2.0 takes place with the linking of multiple sources of data from a number of different media. This integration links the cameras to the Internet, phones, facial-recognition software and GPS and more. Identification will be made through a massive, searchable database of names, photos, residency information, work history and biometric data. Can you imagine a database of 1.3 billion photos? The developers in China can.

I might be skeptical about the possibility, except for a seeing what is already happening as shown in a recent movie, *Red*

Road, set in Glasgow, Scotland. The main character in the movie works at the Public Space CCTV monitoring centre run by the city of Glasgow. She is shown at her work as she tracks a person as he moves about the city, getting to know a great deal about his life, seeing who he associates with, and catching poignant, but misunderstood, actions.

You can check out what another Scottish city, Edinburgh, is doing at www.edinburgh.gov.uk. The city says "CCTV makes a significant contribution to addressing antisocial behaviour across the city….extensive investment in public space CCTV across the city has assisted in the identification and prosecution of criminals and provided reassurance to residents."

What if we could use the technology to get inside the head of a student to understand how the student is responding to different information input and actions?

That's the claim. The reality is more problematic. For example, one study of the use of CCTV monitoring showed that "40% of people were targeted for 'no obvious reason', mainly 'on the basis of belonging to a particular or subcultural group. Black people were between one-and-a-half and two-and-a-half times more likely to be surveilled than one would expect from their presence in the population" (Privacy International, 2008).

In British Columbia, the Privacy Commissioner has ruled against police and city authorities who want to blanket high crime areas with TV monitoring. However, the security plans for the Olympics in Vancouver in 2010 include extensive CCTV — and will anyone bother to take them down after the show?

Biometric data is also available already. Every time a Canadian flies across the border to the U.S., the camera you may not notice behind the immigration agent is capturing you. The web site of the Transportation Security Agency says "Biometric identification allows us to verify a person is who they say they are by using their own unique set of identifiers - whether fingerprints, iris scans or a combination of the two (TSA, 2008)." It is easy to imagine the linking of this and data about credit card use, mobile phone calls, email messages, grocery store purchases and the like.

Figuring out Surveillance 2.0 has changed Klein's view of the technology. In an earlier book, *Fences and Windows*, she presents

the Internet as providing the ideal tool for anti-corporate activists in the age of globalization. She asserted then that the Internet is difficult to control. It "responds to corporate concentration with fragmentation, to globalization with its own kind of localization, to power consolidations with radical power dispersal." (Klein, 2002, p. 21)

That was, unfortunately, a hopeful vision of the potential of Web 1.0 written in July 2000, in the days after the successes of the "Battle in Seattle," opposing the WTO negotiations. However, it was also written before September 11, after which surveillance moved to centre stage in applications of technology.

Surveillance 1.0 morphs into Surveillance 2.0

The classic definition of "surveillance capacity" was developed by James Rule in the 1970s. He identified four components that determined capacity: 1) size and scope of files in relation to the subjected population; 2) centralization of those files; 3) speed of information flow; and 4) number of points of contact between the system and its subject population (Lyon, 1994).

Rule was quite optimistic on the limits to surveillance because many of these conditions could not be met when he did the analysis. Three decades have changed the reality, with all four of the components having been ramped up substantially with the rapid development of more and more capacity, not only to gather and hold data, but also to link and retrieve it.

Eliot Spitzer and the future of education

You probably assumed that deposed New York governor Eliot Spitzer was caught in his expenditures on expensive prostitutes through the phone taps that were reported when he was first accused. I did, at least.

It may have been the phone taps that provided the concrete evidence, but not what led to listening to Spitzer's conversations. According to an article in the *Globe and Mail* (Harvey, April 16, 2008), he was caught by anti-money laundering software used to dig through mountains of customer data looking for suspicious activities.

Author Ian Harvey says "The software looks for subtle patterns that indicate odd activity, and when a transaction is flagged, a human evaluates the findings. More often than not, the

anomaly is explained and dismissed….But when investigators do find something — like chunks of money transferred from the account of a state governor into the account of a shell corporation — they flag the information and forward it to the authorities."

Harvey reports that "Powerful computers running various vendors' anti-fraud software analyze almost every transaction processed — as many as 50 million a day. But what tweaked the software in Mr. Spitzer's case was not money moving from point A to point B. In fact it was the former governor's efforts in trying to conceal the transactions that triggered the alert, authorities say."

Although the linking of data about individual students is still limited, one can see all of the pieces coming together that will make it possible to create this totally invasive form of education.

He continues that "The challenge for the software…is to prioritize those transactions that are most suspicious, and at the same time reduce the number of false-positives — transactions that are flagged, but aren't suspicious. In order to do so, the software runs on a set of rules that are always being tweaked. Account holders are also rated by risk factors in order to generate behavioural baselines, so a nurse or mechanic would likely not get the same scrutiny as, say, a public official" (Harvey, 2008).

So what has this to do with the future of education? I probably would have found this story of interest, but not have thought of it as an education story, had I not recently been at a technology workshop at an education conference.

Roy Pea is Professor of Education and Learning Sciences at Stanford University and is one of the gurus of technology in education. He spoke during the 2008 version of the American Education Research Association annual meeting at one of the special interest groups — Technology as an Agent of Change in Teaching and Learning. These are folks worth listening to — whether you are encouraged or frightened by their expectations of the changes in education.

Pea talked about the pervasiveness of technology in our lives, and especially in the lives of the young. Search engines, social networking, cell phones and other participative media have created a new public sphere. Pea quoted a recent Pew survey of

youth that says 64% are creating content using these tools — mostly at home, not in school.

Changes are taking place so rapidly that educators and researchers cannot keep up — academic educational research takes five years from idea to publication — much slower than the development of the new infrastructure of participation.

Suppose you think of education a little differently, as a collection of data points. Pea talked about getting a piece of data entered into the digital environment every five minutes during classes. That would produce a huge amount of data when you aggregate all the classrooms.

I recall reading once that a teacher makes about 200 decisions an hour (no wonder we get stressed) and if you captured just a fraction of those, along with various student interactions, you would have a massive collection of data to be mined.

Pea wasn't talking about stopping every five minutes to do some data entry. Rather, he mentioned using tools like special glasses for the teacher designed to record which student the teacher is watching at any particular point. This mass of data would then be mined, using the kinds of tools that caught Spitzer and produce returns similar to those you get when you do a search on Google.

This conception of education and its techno applications provide the high "number of points of contact between the system and its subject population," the fourth of James Rule's elements required for a high capacity for surveillance.

"Brain waves tell all" — More of a possible future

Mining data in the technosphere deals with information that is outside the individual. Granted, that tells a lot about what an individual does and how they behave. But what if we could use the technology to get inside the head of a student to understand how the student is responding to different information input and actions?

Again, it is business where the tools are being developed that may some day be used in education. The advertising business is using biometric techniques to measure consumer response to ads (Elliott, 2008).

The tools of biometrics include measuring brain waves, galvanic skin response, eye movements, and pulse rates. Of course,

these tools are all benign, according to those who work in the industry. It is the usual "it's just a tool" claim.

The chief analytics officer for one of the companies using these techniques, Elissa Moses, assures the *New York Times* reporter that "The role of neuromarketing is to understand how people feel and react. It in no way sets out to meddle with normal, natural response mechanisms." Oh, sure! And they will never, ever be used to "meddle" (Elliott, 2008)?

The CEO at another biometrics company, NeuroFocus, says "We measure attention, second by second; how emotionally engaged you are with what you're watching, whether it's a commercial, a movie or a TV show; and memory retention."

Imagine the classroom of the future. Every student wears various monitors sending by wireless to a central database, information about brain waves, eye movements and pulse rates. The student working at home on an online educational program is feeding the information to the teacher — or to the replacement for a teacher — an electronic monitor that has a dashboard showing attention and emotional engagement. That data collected from students is mined to determine effective pedagogical practices.

The tools of surveillance currently used in education seem primitive compared to these possibilities. Standardized testing with data in central databases currently provides tools for "steering at a distance," a characterization of the accountability systems as they now exist. The testing allows administrators and politicians to reach into the classroom to put the teacher under the spotlight, but currently a pretty dull spotlight.

However, our current surveillance systems are very limited compared to the invasive approaches of using biometrics and data mining. These would allow for almost instantaneous intervention in the classroom — or wherever the student is engaged in learning. We can imagine the way that applying these already existing tools could change the nature of teaching.

Surveillance in schools today

Maybe it is just my age, and my commitment to democratic participation, that make me more than a little frightened of these applications of technology to education. Will these surveillance tools become a part of the education system? When they are

cheap and ubiquitous and meet all the elements of "surveillance capacity," can you imagine them not being used?

The tools used in education these days are still pretty much Surveillance 1.0 — each operating individually. However, while still relatively primitive, the building blocks are being put in place. What they lack in 2.0 characteristics is the ability to link all of them. However, we can count on that being possible before too long, as military and national security agencies develop more and more user-friendly versions of linking tools and as the necessary computing power substantially increases, while costs continue to decrease.

Although the linking of data about individual students is still limited, one can see all of the pieces coming together that will make it possible to create this totally invasive form of education.

Closed-circuit TV has appeared on some Canadian school sites, although it is not as ubiquitous as at schools in the U.S. or Britain. In Edinburgh, the cameras are already widely in place in schools. Their purpose generally is "to both prevent and detect antisocial behaviour." If you want information on "cameras in schools," the public is told, "contact the Head Teacher" (City of Edinburgh, 2008). In London, a car with a CCTV camera built into a periscope is being used to deter parents from parking in banned areas near school gates (BBC, 2008).

Some UK schools are experimenting with having students wear chips sewed into their uniforms to track them. According to an article in the *Times Education Supplement*: "The chip is embroidered into school jumpers using conductive 'smart threads.' This allows a pupil's identity, photographs and other details, such as whether they misbehaved in their last lesson, to flash up on the nearest teacher's laptop or hand-held computer" (Milne, 2007).

Some pre-schools provide streaming video over the Internet so that parents can look in on what their child is doing at any time during the day. A "Chaperone" service by cell carrier Verizon sets up a "geofence" around an area selected by a parent and sends an automatic text message if the child, carrying their cellphone, moves outside that area (Hakashima, 2007).

Many provinces and states are building centralized databases, aiming to have detailed data on every student. This is to fit government mandates, such as *No Child Left Behind* in the U.S.,

which require extensive testing and tracking of students according to ethnicity. The collection of data, linking of data, and analysis of data is aimed at influencing what the teacher does in the individual classroom — all in the name of accountability and improvement.

Programs such as ParentConnect track a student's attendance, assignments, marks and homework to the parent whenever they want to check in. A *New York Times* article (Hoffman, 2008) describes one parent-child "connection": "When her ninth grader gets home at 6 p.m., there may well be ParentConnect printouts on his bedroom desk with poor grades highlighted in yellow by his mother. She will expect an explanation. He will be braced for a punishment."

A range of positive claims are made for this type of software. One rationale, reflecting the reality of 21st century families, is that divorced parents can both log on and track the child without having to deal with one another.

From another perspective, a search for ParentConnect on Facebook shows two groups one can join: "Rage against ParentConnect" and "Grade-Posting Sites Ruin Lives!!!!"

Surveillance shapes teaching and learning

If the tool shapes the task, how does surveillance affect the teacher, the student and the process of teaching?

The autonomy of the teacher has always rested with closing the classroom door. Whatever government policies or administrative directives were promulgated, the teacher could pay lip service to them, but then proceed to teach in a way that they thought best for their students.

Of course, there were limits, and there was always some check on the teacher. It might come from student reports home to an appalled parent about some teacher comment or classroom activity. It might be from the administrator dropping in, or appearing for an announced evaluation observation. However, these represented only a very limited external observation or surveillance of the teacher.

The greatest shaper of a teacher's actions was likely the socialization they had internalized. This socialization would have come from a variety of sources: their own experience as a student, their teacher education, professional development, conversations with

colleagues, whatever. Direct outside observation into the classroom would have been unlikely as a significant factor.

So what happens when the teacher in the classroom can have every action subject to external view, whether by data collection or visual access through webcasting or closed circuit TV?

So what happens when the teacher in the classroom can have every action subject to external view, whether by data collection or visual access through webcasting or closed circuit TV?

The impact is suggested in a study of students reported in *Surveillance and Society* (yes, it is a field of study sufficient to have its own academic journal). Shane Dawson (2006) describes the effect on online behavior of university students when they believe that their communication is being monitored. In the study, students "browsing behavior, range of topics and writing style is influenced by the various modes of surveillance…. Students enact their own forms of self-regulation as a result of institutional panoptic technologies" (Dawson, 2008, p. 81).

This is the panopticon effect, as theorized by Foucault. By creating the possibility that an individual's behavior is being monitored, the individual performs in ways that assume being watched, whether one is or not.

The effect of information and communication technologies is to increase the potential of observation as digital records are left from nearly every activity, whether online chats, talking on a cell phone, making a bank deposit, to having one's class absence recorded on a database. This has been described as the "information panopticon." Interestingly, according to Dawson's study, *not understanding the technology of surveillance, but knowing it is in place, adds to the disciplining effect*, leading to self-constraint. Not understanding the technology leaves an individual with no sense of what the limits to surveillance might be. Consequently, they act on the assumption that any surveillance is possible.

The stated aims of the introduction of technology to education, often without an intention of surveillance possibilities, are often framed in very positive terms like improved access, accountability and escaping the limits on education of time and space. However, the reality is often, as Dawson points out,

"potential individual and collective disempowerment in cases where populations have high degrees of surveillance" (p. 81).

That high degree of surveillance is increasingly a reality in all aspects of our lives, including at all levels of education. This leaves us with a gigantic challenge — how do we utilize the possibilities of digital communications, but place controls on the use of the surveillance possibilities that come along with them? What might those controls look like?

Let's get started on that conversation.

* * *

Larry Kuehn is Associate Editor of Our Schools/ Our Selves.

References

BBC. (2008). "Dissecting the New Age." Downloaded, May 19, 2008. http://sovereignsentience.blogspot.com/2008/05/cctv-car-patrols-at-school-gates.html

City of Edinburgh. (2008). Downloaded, May 19, 2008. www.edinburgh.gov.uk/internet/City_Living/Community_safety/Crime_and_law_enforcment/CEC_cctv

Dawson, S. (2006). "The impact of institutional surveillance technologies on student behavior." Surveillance and Society, 4(1/2), 69-84. Downloaded May 19, 2008 from www.surveillance-and-society.org

Elliot, Stuart. (March 31, 2008). "Is the ad a success? The brain waves tell all". *New York Times*. http://www.nytimes.com/2008/03/31/business/media/3ladcol.html

Harvey, I. (2008). "Anti-laundering software casts wide net to catch big fish." *Globe and Mail*, April 16, 2008.

Hoffman, J. (2008). "I know what you did last math class." *New York Times*, May 4, 2008.

Klein, N. (2002). *Fences and Windows: Dispatches from the front lines of the globalization debate*. Toronto: Vintage Canada.

Klein, N. (2008). "China's all-seeing eye." Downloaded May, 19, 2008. http://www.rollingstone.com/politics/story/20797485/chinas_allseeing_eye

Lyon, J. (1994). *The electronic eye: the rise of the surveillance society*. University of Minnesota Press.

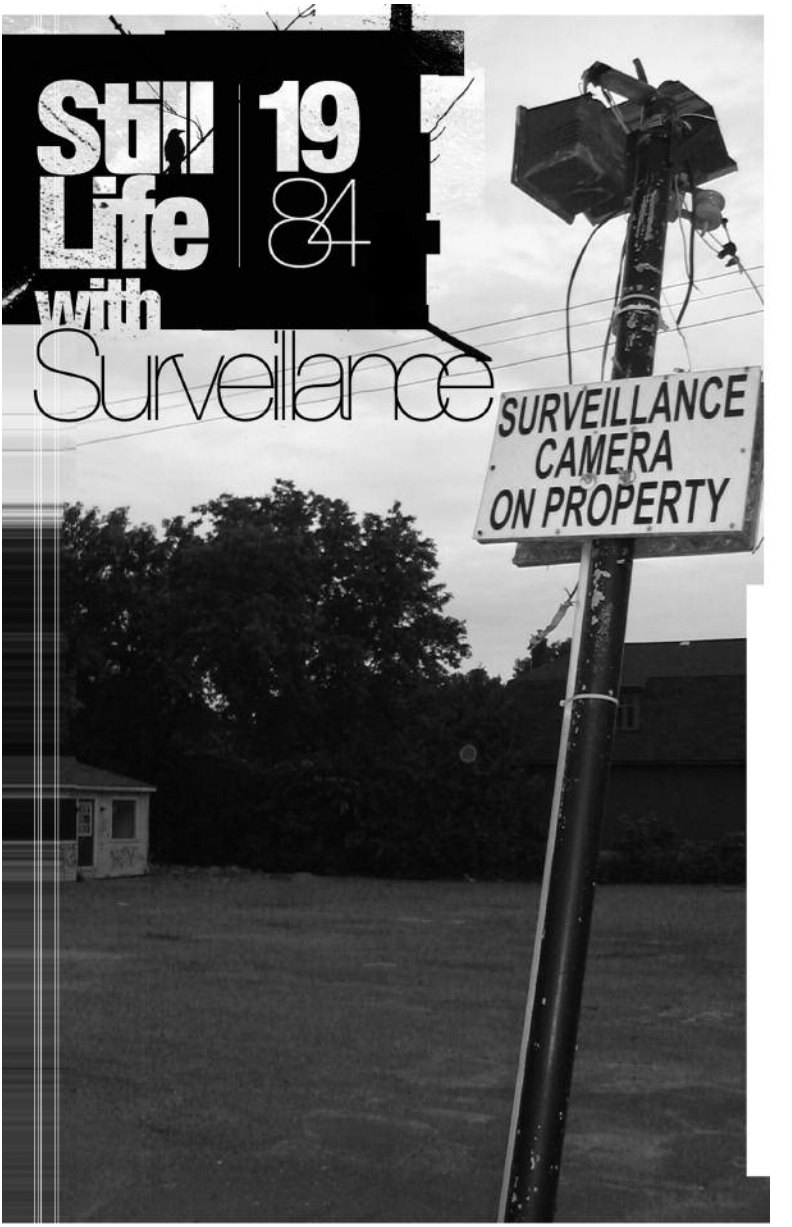
Milne, J. (2007). "Civil liberty groups take a dim view of experiment that could go nationwide." Times Education Supplement, November 23, 2007.

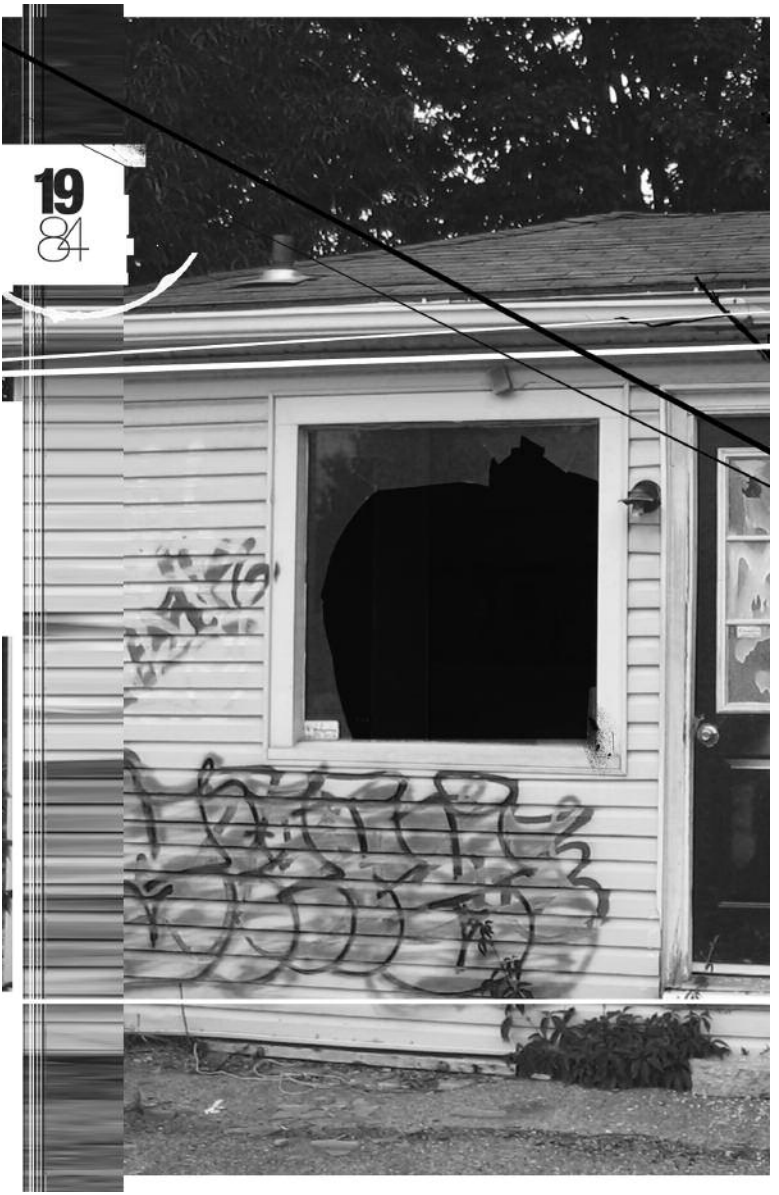
Nakashima, E. (2007). "Cellphone tracking powers on request." Washington Post, November 23, 2007.

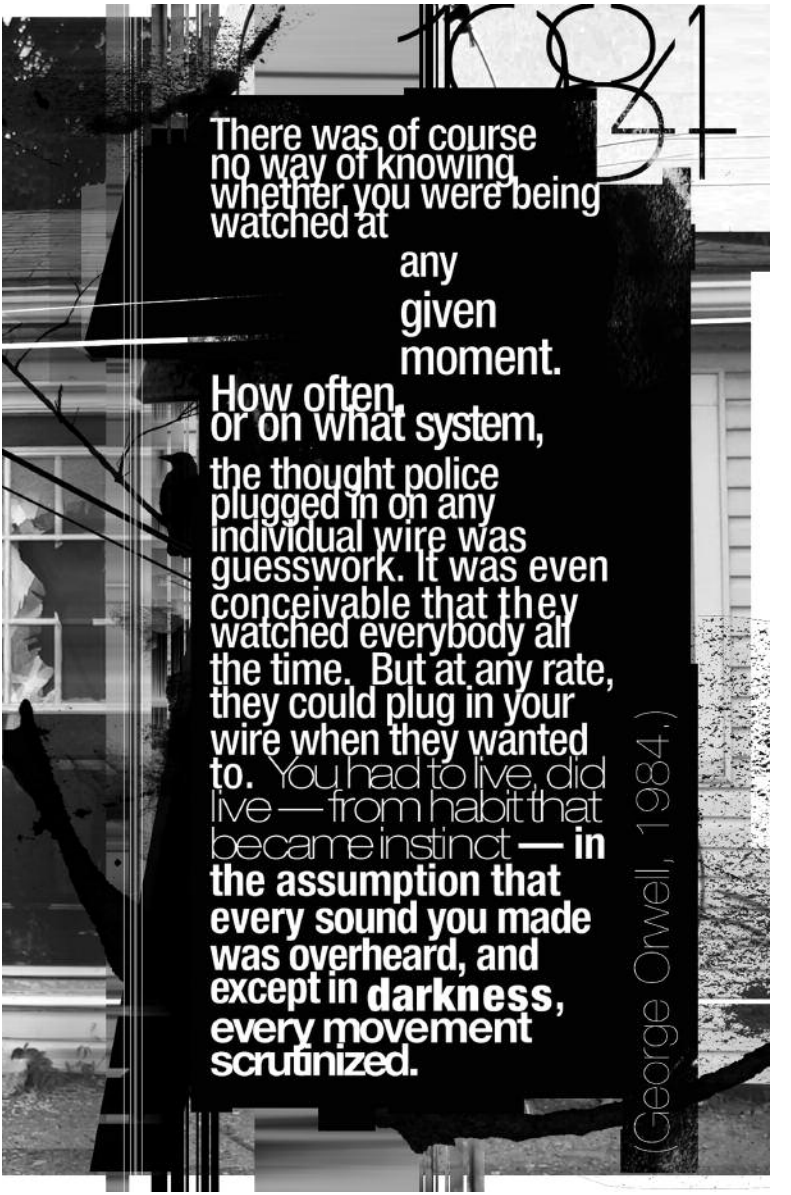
Privacy International. (2008) Downloaded May 19, 2008. http://www.privacyinternational.org/issues/cctv/_index.html

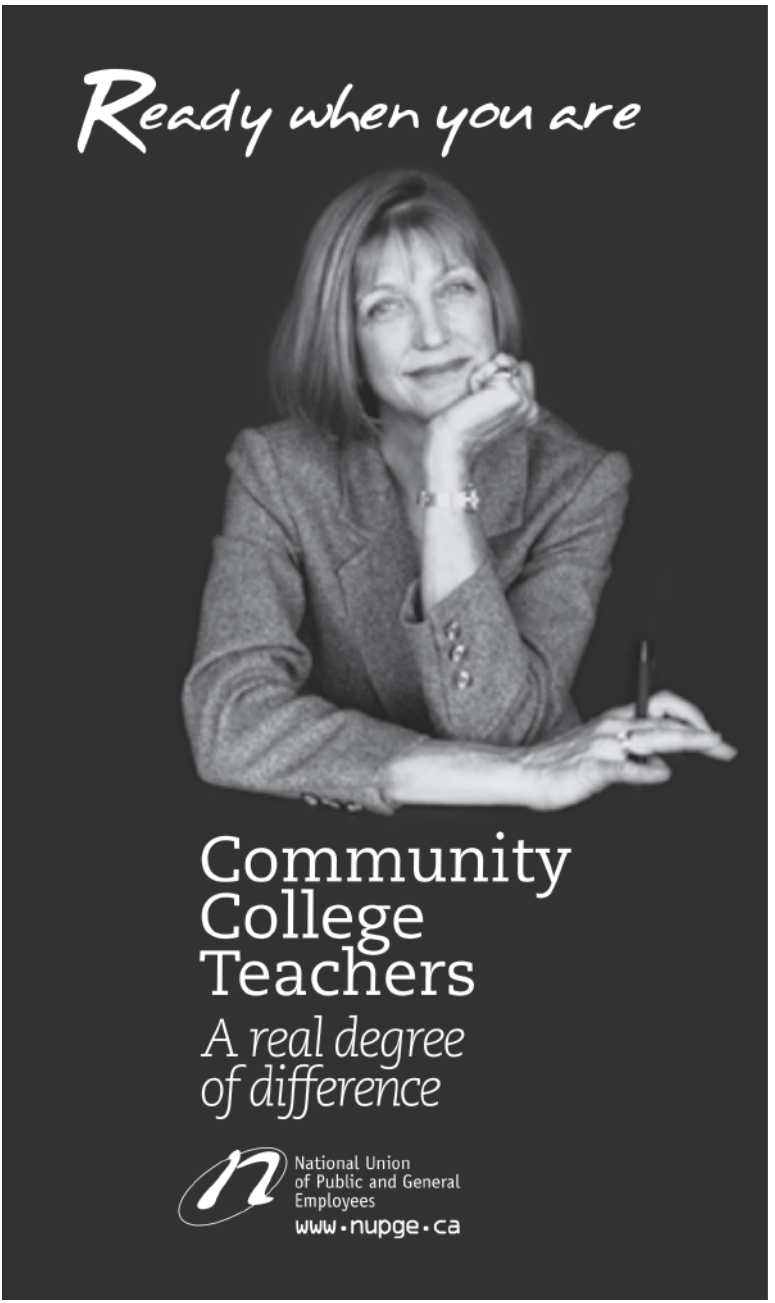
Transportation Security Administration. (2008) Downloaded June 8, 2008. http://www.tsa.gov/approach/tech/biometrics.shtm

PHOTO ESSAY BY CHRYS MOLL

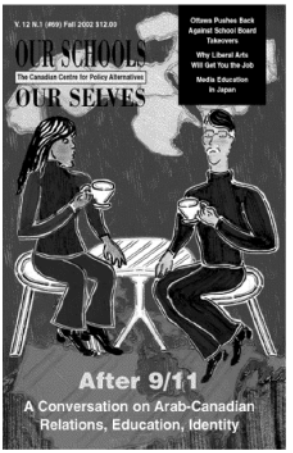



19
84


There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the thought police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate, they could plug in your wire when they wanted to. You had to live, did live — from habit that became instinct — in the assumption that every sound you made was overheard, and except in darkness, every movement scrutinized.
(George Orwell, 1984.)


Ready when you are
Community College Teachers
A real degree of difference
National Union of Public and General Employees
www.nupge.ca

Knowledge is a powerful tool.



OUR SCHOOLS
Canadian Centre for Policy Alternatives
OUR SELVES

"...an excellent general-interest journal... Engagingly written, it bridges the gap between theory and practice."
—The Utne Reader

Our Schools / Our Selves is the Canadian Centre for Policy Alternatives' quarterly education publication. Since 1988 it has been a forum for debates and commentary on issues such as environmental activism; commercialism in schools; young women in trades; labour, education and the arts; schools and social justice, and teaching for democratic citizenship.

Subscriptions (4 issues/year) are $51.36 (including shipping, handling and GST). Make cheque payable to Canadian Centre for Policy Alternatives, 410-75 Albert Street, Ottawa, ON, K1P 5E7. Phone: 613-563-1341. Fax: 613-233-1458. Email: ccpa@policyalternatives.ca. Visit our web site for more information.

http://www.policyalternatives.ca

❍ I'd like to subscribe to **Our Schools/Our Selves**

❍ Please find enclosed my cheque in the amount of $_____

❍ Please charge my ❍ VISA or ❍ MasterCard for the amount of $ _____

Card# _____ Expiry Date:_____

Signature: _____

Name:_____

Address:_____

_____

Phone:_____