The *Culture of Surveillance* Revisited: "Total Information Awareness" and the New Privacy Landscape

William G. Staples
University of Kansas

It's late November 2002 on a drizzly, cold day in Washington, D.C., a little more than a year after four hijacked planes crashed into the World Trade Center, the Pentagon, and a field in Pennsylvania killing more than 3,000 people. In one of the bewildering number of *Starbucks* off Dupont Circle, Jeff Bezos, iconoclast leader of the mega online e-tailer Amazon.com, and John Poindexter, then director of the Pentagon's Office of Information Awareness, meet. Bezos orders a low-fat latte. Poindexter, ex-Regan national security advisor and a convicted felon charged with lying to Congress and obstruction of justice, takes an Americano (of course). Poindexter gets right to the point.

Poindexter: "Jeff, we have a problem. The world has changed dramatically. During the years I was in the White House it was relatively simple to identify our intelligence collection targets. Today, the most serious asymmetric threat facing the United States is terrorism, a threat characterized by collections of people loosely organized in shadowy networks that are difficult to identify and define and whose goals are the destruction of our way of life. The intelligence collection targets are thousands of people whose identities and whereabouts we do not always know. It is somewhat analogous to the antisubmarine warfare problem of finding submarines in an ocean of noise—we must find the terrorists in a world of noise, to understand what they are planning, and develop options for preventing their attacks. I think the solution is largely associated with information technology. We must become much

more efficient and more clever in the ways we find new sources of data, mine information, and make it available for analysis, convert it to knowledge, and create actionable options."

Bezos, ever the excitable boy, and looking for an opportunity to show off to the elder Poindexter, pipes in.

Bezos: "John, this is way cool! That's what's really got me excited about the Internet and the ability to use technology. In the last five years, we've invested $800 million in technology and we continue to spend $200 million a year."

Poindexter: "I know, Jeff. One of the significant new data sources that needs to be mined to discover and track terrorists is the 'transaction space.' If terrorist organizations are going to plan and execute attacks, their people must engage in transactions and they will leave signatures in this information space. Currently, terrorists are able to move freely throughout the world, to hide when necessary, to find sponsorship and support, to operate in small, independent cells, and to strike infrequently, exploiting weapons of mass effects and media response to influence governments. This low intensity/low density form of warfare has an information signature. We must be able to pick this signal out of the noise. The relevant information extracted from these data must be made available in large scale repositories with enhanced semantic content for easy analysis."

Bezos: "Despite the expense, all this feedback from customers has its rewards. Amazon now has a vast database of customer preferences and buying patterns, tied to their e-mail and postal addresses . . . Ultimately, John, we're an information broker."

Poindexter: "I know, Jeff. That's why I've come to you. I also know that, one year prior to the September 11 attacks—almost to the day—you issued a notice to your customers that you gather information about them every time they search for a product, that you do share information among your extensive list of companies and online partners, and that you consider customer information a 'key asset' that is transferable if you buy or sell associated stores."

Bezos: "In revising our privacy policy, we tried to take into consideration not only our current activities but also those things we could imagine possibly happening in the future."

Poindexter: "Indeed. You were way ahead as usual, Jeff. While our goal is total information awareness, there will always be uncertainty and ambiguity in trying to understand what is being planned. That's why we need to bring people with diverse points of view together in a collaborative environment where there is access to all source data, discovery tools, and model building tools. Collaboration has not been so important in the past when problems were less complex, but now it is essential."

Bezos: "Collaboration. Oh, absolutely. This is long term orientation and a powerful vision which is shared by everybody here at the company. The technology that we've built is very customer centric. Everything that we've done has been around being obsessed over customers. In fact, we've been tracking and profiling their shopping and buying habits for years! Say, have you visited our site lately, John? My favorite product in the kitchen store is the OXO Salad Spinner. Read the customer reviews of that and I guarantee you, even if you don't like salads, you'll buy that spinner."

Poindexter: "Well, that's great, Jeff. I'll tell the wife about it. In the mean time, my IT folks will be in touch."

Now, as you may have guessed, this meeting between Bezos and Poindexter never happened. Yet nearly all of what I have just read has been said by both of these men in published interviews and speeches.[2] Of course, as a sociologist, I am most interested in the larger, structural and cultural context of contemporary forms of surveillance and less in the actions of a few individuals, no matter how powerful they may be. But I use this little parable to signal three things: 1) I expect, as we have already seen in fact, a shift in the scope and quality of social monitoring we can likely expect in the post 9/11 period. I would suggest that the attacks of September 11 have provided an extraordinary opportunity for the state to extend its "governability" (Foucault 1991) of the popula-

tion through a new set of surveillance and control mechanisms; 2) I would argue that the only way that the state is going to implement this kind of large scale, integrated, digitized system of surveillance of the populace is through the cooperation of both corporate capital and, by extension, the populace itself; and 3) I would like to call attention to how a new digital surveillance system will work to constitute our virtual identities as *both* "consumers" and "citizens."

The word surveillance, in the most general sense, refers to the act of keeping a close watch on people, scrutinizing and monitoring their behavior. To many, the term often brings to mind George Orwell's notorious "Big Brother" as depicted in the novel *1984*. Yet, when I began looking at new forms of surveillance and social control in the mid 1990s, "Big Brother" was seemingly nowhere to be found. Sure, there was the legacy of the COINTELL programs of the 1960s and 1970s and no doubt various individuals and groups were being monitored by state agents, but there was little evidence that anything like the tele-screens and oppressive state apparatus depicted in Orwell's novel were routinely affecting the lives of the average citizen. Instead, what I found was a raft of what I called "Tiny Brothers" increasingly present in our workplaces, schools, homes and community institutions. These techniques exist in the shadow of large institutions; they are not ushered in with dramatic displays of state power, nor do they appear as significant challenges to constitutional democracy. These are the more commonplace strategies used by both governmental, but even more likely, private organizations to "keep us in line," monitor our performance, and accumulate evidence. These local, knowledge gathering activities are often enhanced by the use of new information, visual, communication, and medical technologies.

In my book, *The Culture of Surveillance* (Staples 1997) first published in 1997and later in a revised and updated edition entitled *Everyday Surveillance: Vigilance and Visibility in Postmodern Life* (Staples 2000), I identified an array of these tactics from the "soft," seemingly benign and relatively inconspicuous forms of monitoring such as preventive shoplifting systems, marketing

databases, "pagers" and other electronic monitoring instruments to the "harder" more obtrusive and confrontational practices that often begin with the assumption of guilt and are designed to uncover the "truth," to test an individual's character, and, more generally, to make people consciously aware that they are indeed being watched and monitored. These are what I call "surveillance ceremonies." They include random drug and alcohol testing, the use of lie detectors, pre employment integrity tests, "sobriety checkpoints" in the streets, the use of metal detectors and other types of scanning equipment, and electronically monitored "house arrest." Between these soft and hard types of social control lies a vast array of techniques and technologies exercised on and by people both inside and outside the justice system that are designed to watch our bodies, to regulate and monitor our activities, habits, and movements, and, ultimately, to shape or change our behavior. Some of these procedures are often undertaken in the name of law and order, public safety, the protection of private property, or simply "sound business practice"; others are initiated for an individual's "own good" or benefit. But no matter what the stated motivation, the intent of surveillance as social control is to mold, shape, and modify actions and behaviors. These rituals, I argue, are the specific, concrete mechanisms that operate to maintain unbalanced and unequal authority relationships. These relationships exist between specific clusters of individuals (e.g., between managers and workers, police officers and suspects, probation officials and offenders, teachers and students, parents and their children, and the like) and, in a larger sense, between individuals and the public and private organizations where these rituals take place.

Surveillance and social control of this type are not orchestrated by a few individuals; it is not part of a master plan that is simply imposed on us. Rather, in my view, we are all involved and enmeshed within a matrix of highly intentional and purposeful power relations,, arrangements that can be more or less unequal but are never simply one directional. Moreover, *sans* "Big Brother," it's not just a scary group of "Them" who are doing this to us, either. I argue that we live in a voyeuristic and "looking" postmodern culture as we often turn the tracking devices on ourselves.

We offer up ourselves to the digital machines. We willingly wire ourselves in with "cell" phones and the like as we rush to buy the latest products that offer us access to the "net" and the "web" (the jargon of this technology is revealing). We buy the videocams and use them to document our own movements, or we turn them on our friends, neighbors or strangers. We also bring home the machines to listen in on our kids' phone calls, keep an eye on their driving, or test them for drugs.

Now, in this previous work, my focus was primarily on the local situations of everyday life. But the events of September 11th and its aftermath force us to shift our attention to the institutional level and the actions of the state and here we find what figures to be a reconstitution of state power within a complex web of affiliations with civil society.

For a while it was the "war on drugs"; now it is the "war on terrorism." And it seems that labeling a social policy a "war" justifies the involvement of the military in it. In the *Culture of Surveillance*, I suggested that the nation's military industrial complex was morphing into a "security industrial complex," and with it we see a blurring distinction between techniques and technologies designed for "military" operations and those deployed in domestic "security" operations. September 11th, it seems, has accelerated this process. As part of the government's sweeping Homeland Security agenda that includes the USAPATRIOT legislation, the Pentagon is sponsoring a number of new projects purportedly designed to weed out the suspected terrorists among us. Some of these projects are being developed by the Defense Advanced Research Projects Agency, or DARPA, the Pentagon's "think tank" for new technologies. You may have read about some of these in the newspaper over the last couple of years. For example, there is a project called Combat Zones That See, or CTS. Ostensibly being developed to deal with the urban warfare situations US personnel face in Bagdad today, CTS would coordinate a multiplicity of surveillance cameras, gathering their views in a single information storehouse. The goal, according to a recent Pentagon presentation to defense contractors, is to "track everything that moves." CTS will keep watch by equipping each camera with a processor like the

one in your computer. The chips will be programmed with "video understanding algorithms" that can distinguish, say, one car from another, the car's speed, time of arrival, color, size, license plate, and shape, attributes that are all instantly passed on to a central server. By sharing only this refined data—instead of the raw video itself—CTS should keep a vast computer network of cameras from becoming overloaded with hours and hours of meaningless footage. DARPA is also developing what they call a "LifeLog." LifeLog is a high tech diary of sorts, designed to create a multimedia, digital record of everything a person sees, says, and hears, the goal of which is to create a searchable database of human lives to promote artificial intelligence. There are also identification systems designed to recognize a person's face or style of walk, the retina of the eyes, and the like (Shachtman 2003). I could go on here but let me focus on the story of one tool under consideration.

Until August 2003, ex-Admiral John Poindexter was in charge of the Information Awareness Office within DARPA which got considerable attention when its program "Total Information Awareness" came to light in late 2002. TIA was as "Orwellian" sounding as anything we have seen in some time. The office symbol on a sign outside Poindexter's office is a cultish looking all seeing eye atop a pyramid like on the dollar bill, peering at a globe with the accompanying slogan "Scientia est Potentia" ("Knowledge Is Power"). TIA's stated aim was to "connect the dots" of what Poindexter refers to as the "transactions space"; to "mine" huge amounts of information about people and thus help investigative agencies identify potential terrorists and anticipate their activities. All the transactions and activities that most of us engage in on a daily basis such as credit card purchases, ATM activity, toll collection systems, travel and telephone records, internet traffic and the like—billions and billions of pieces of information generated by millions of people—would be culled for pre-identified patterns or actions of say, a few hundred suspected terrorists.

So, for example, the system would supposedly be able to "connect the dots" between two of the hijackers on September 11th who were on a State Department watch list. Phone records indicated that they were calling each other. They bought airline tickets

on the same day. A search of the people they called regularly would have uncovered other young Arab males who also had bought airline tickets for the same day. A more detailed search would have revealed that several had attended flight schools together. A computer program trolling the Internet for these indicators would have popped up a red flag. Moreover, TIA could jack into video feeds from surveillance cameras as well as the emerging biometric databases of those facial and other assorted recognition systems to trace the movements of suspected terrorists.

Of course, DARPA doesn't actually conduct any of its own research. That's "outsourced" to corporations and our colleagues at universities around the country.

For example, the Office of Information Awareness has awarded 13 contracts to Booz Allen & Hamilton amounting to more than $23 million; Lockheed Martin Corporation had 23 contracts worth $27 million; the Schafer Corporation had 9 contracts totaling $15 million. Other prominent contractors involved in the TIA program include SRS Technologies, Adroit Systems, CACI Dynamic Systems, Syntek Technologies, and ASI Systems International. In addition, at least 24 universities received almost $10 million during the last five years to do research on TIA related projects. Some of the largest grants went to Cornell, Columbia, and UC Berkeley (Mayle and Knott 2002).

After it was made public, TIA came under attack from civil libertarians, privacy groups, and lawmakers across the political spectrum. "This could be the perfect storm for civil liberties in America," said Marc Rotenberg, director of the Electronic Privacy Information Center. "The vehicle is the Homeland Security Act, the technology is DARPA, and the agency is the FBI. The outcome is a system of national surveillance of the American Public"(Markoff 2002). In February 2003, Senate and House conferees agreed to impose severe restrictions on TIA. Virtually without dissent, the House conferees accepted a bipartisan Senate provision stipulating that the program cannot be used against American citizens and that it would be shut down in 90 days unless the Pentagon submitted a detailed report on the program's cost, goals, impact on civil liberties and prospects for success against terror-

ists. In response to the firestorm of controversy over TIA, Pentagon officials delivered their report to Congress in May. In it they announced that they were changing the name of the project from "Total Information Awareness" to "*Terrorist* Information Awareness" and declared:

> The Department of Defense . . . has expressed its full commitment to planning, executing, and overseeing the TIA program in a manner that protects privacy and civil liberties. Safeguarding the privacy and the civil liberties of Americans is a bedrock principle. DoD intends to make it a central element in the Department of Defense's management and oversight of the TIA program...

Few critics were appeased by the DoD move and many contended that a prototype is already in place and has been used in tests by military intelligence organizations. In late July, the Senate voted to cut off funding for TIA, prohibiting the Defense Department to spend any portion of its $369 *billion* budget on the Terrorism Information Awareness program and ignoring a request by the Bush administration to keep the program going. Following this debacle, Poindexter found himself in yet another controversy with his plan to set up an online speculative futures trading place called "Policy Analysis Market" that would have rewarded investors who forecast terrorist attacks, assassinations and coups. Declared a "lightning rod" for contestations, the Pentagon asked Poindexter to resign.

So, what do these events portend? First, despite the minor setback in the story of TIA, we are likely to see a shift in the scope and quality of the social monitoring we will experience. In practical terms, the new national security agenda and variants of programs like TIA will surely deepen the "culture of surveillance" that we currently live in. This is hardly stunning news. Given the implications of the USAPATRIOT Act, the creation of a cabinet level Homeland Security agency with a $30 *billion* budget, and a burgeoning state apparatus set out to monitor the populace, there is bound to be more watching going on. It seems to me that September 11th provides an extraordinary opportunity for the state to

extend its "governability" of the population through a new set of surveillance and control mechanisms. This form of bureaucratic power, what Foucault called "governmentality," is centered on techniques to identify, classify, and manage "risk" populations through continuous monitoring. Will this finally be the arrival of "Big Brother?" I doubt it. This process began in the 19th century with public health movements, formal census taking, the inventions of the birth certificate and passport, and the like. These latest moves seem fairly consistent with the evolution of the liberal state apparatus.

Secondly, the current situation also tells us that the only way that the state is going to implement this kind of large scale, integrated, digitized system of surveillance of the populace is through the cooperation of both corporate capital and, by extension, the populace itself. By this I mean a number of things. The state needs the corporations to provide the technical know-how to build and maintain the system. Was it foresight that the Pentagon's DARPA, responsible for the creation of the Internet, will now use it, and the commercial technology designed by the likes of Microsoft and IBM will enhance as a capillary network, connecting computer to computer to data mine the minutiae our daily lives? The digital network, our banks, credit cards, on line purchases that have become so much a part of our daily lives as consumers —including many of the "Tiny Brothers" that I documented in my book— will become the architecture for this giant monitoring network. Moreover, the public will likely resist attempts by the state to watch them if the actions appear to be top-down and hence "Big Brotherish." This was the lesson of the failed "Total Information Awareness" program. As a former high ranking naval officer who served with Poindexter characterized him, "John Poindexter is a brilliant nuclear engineer who is also politically tone deaf" (Markoff 2003). Poindexter et. al. need to learn from the likes of Jeff Bezos that a jack boot on the neck will raise the hackles of the public, but offer them great prices and free shipping and people will gladly hand over their "personal information." Or as neo-liberal Nikolas Rose puts it, "To govern humans is not to crush their capacity to act, but to acknowledge it and use it for one's own objectives." (Rose 1999,

p. 4). Seduced by the market's desires and overwhelming dependence on it, we are willingly feeding our data into the machines. To paraphrase Mark Poster, we become "individuals plugged into the circuits of our own panoptic control" (Poster 1996, p. 184). The Pentagon will act as the broker, drawing, as it has in the past, on the minds of university professors and profit hungry corporations, to bring it all together. So in order to avoid the political ineptitude of John Poindexter and be deployed successfully, this kind of surveillance will need to be designed into the flows of everyday existence, dispersed, and de-centered, operating in the background. Much like shopping online, we'll hardly know that it exists.

Finally, and relatedly, I would like to call attention to how a new digital surveillance system will work to constitute our virtual identities as both "consumers" and "citizens." "Computerized databases are nothing but performative machines," Poster tells us, "engines for producing retrievable identities" (Poster 1996, p. 186). If the new system is built around monitoring our activity in the so called "transaction space," then we will be subjected to judgements—"normalizing judgements," in Foucault's terms—as to what constitutes a proper consumer profile and thereby be declared a "safe citizen" vs. someone "at risk" (whatever that means). In other words, we will need, in part, to act out our role as good consumers in order to prove our worthiness as good citizens thus binding these two identities together. This is a fitting "homeland security" program for a society that, as Henry Giroux puts it, "equates profit making with the essence of democracy and consumption as the ultimate privilege of citizenship" (Giroux 2002, p.12).

Notes

[1] A version of this paper was presented at the Annual meeting of the American Sociological Association in Atlanta in August 2003 in a thematic session entitled, "The Culture of Surveillance, Civil Liberties, and Freedom" and at the opening session of the MIT Conference on Human Rights and Technology in Cambridge in April 2004 entitled, "Threats to Human Rights in the Digital Realm."

[2] For complete texts of Bezos and Poindexter quotes see:

Bayers, Chip."The Inner Bezos." *Wired*. Issue 7.03 March 1999 <http://www.wired.com/wired/archive/7.03/bezos.html> [accessed 4 June 2003].

Business Week On Line. "Chewing the Sashimi with Jeff Bezos." July 15, 2002. <http://www.businessweek.com/bwdaily/dnflash/jul2002/nf20020715_5066.htm> [accessed 9 June 2003].

The Economist. "A river runs through it." May 8th 1997 <http://www.economist.com/displayStory.cfm?Story_id=596297> [accessed 9 June 2003].

Nash, Kim S. "Amazon.com revises privacy policy on use of customer data." September 01, 2000. *Computer World*. <http://www.computerworld.com/industrytopics/retail/story/0,10801,49388,00.html> [accessed 9 June 2003].

Levinson, Meridith. "Yet Another Interview with Jeff Bezos." October 2002. *Darwin Magazine*. <http://www.darwinmag.com/read/100102/bezos.html> [accessed 9 June 2003].

Poindexter, John. "Overview of the Information Awareness Office." Defense Advanced Research Projects Agency, DARPATech 2002 Conference, Anaheim, Calif., August 2, 2002 <http://www.fas.org/irp/agency/dod/poindexter.html>[accessed 12 June 2003].

References

Foucault, Michel. 1991. "On Governmentality." Pp. 87-104 in, *The Foucault Effect: Studies in Governmentality: With Two Lectures by and an Interview With Michel Foucault* edited by Graham Burchell, Colin Gordon, and Peter Mille. Chicago: University of Chicago Press.

Giroux, Henry A. 2002. "Democracy, Freedom, and Justice after September 11th: Rethinking the Role of Educators and the Politics of Schooling." *The Teachers College Record* 104 (6): 1138 1162.

Markoff, John. 2003. "Poindexter's Still a Technocrat, Still a Lightning Rod." *New York Times*, January 20, p.1.

_____. "Threats and Responses: Intelligence; Pentagon Plans a Computer System That Would Peek at Personal Data of Americans." *New York Times*, November 9, p. 12

Mayle, Adam and Alex Knott. 2002. "Outsourcing Big Brother: Office of Total Information Awareness Relies on Private Sector to Track

Americans." The Center for Public Integrity <http://www.publici.org>[accessed 18 June 2003].

Poster, Mark. 1996. "Databases as Discourse; or, Electronic Interpellations." Pp. 175-192 in *Computers, Surveillance, and Privacy* edited by David Lyon and Elia Zureik. Minneapolis: University of Minnesota Press.

Rose, Nikolas. 1999. *Powers of Freedom: Reframing Political Thought.* Cambridge, UK: Cambridge University Press.

Shachtman, Noah. 2003. "Big Brother Gets a Brain." *Village Voice* (New York, NY) July 15.

New York Times, 2003. "Pentagon Explores a New Frontier In the World of Virtual Intelligence." *New York Times* May 30, 2003, p.22.

Staples, William G. 1997. *The Culture of Surveillance: Discipline and Social Control in the United States*. New York: St. Martin's Press.

_____. 2000. *Everyday Surveillance: Vigilance and Visibility in Postmodern Life*. Lanham, MD: Rowman & Littlefield Publishers.