

The Nation.

[Click here](#) to return to the browser-optimized version of this page.

This article can be found on the web at
<http://www.thenation.com/doc/20010806/parenti>

Big Brother's Corporate Cousin

by CHRISTIAN PARENTI

[from the August 6, 2001 issue]

Winston must log on to the computerized phone system at Charles Schwab brokerage firm no later than seven minutes after 8, or she'll be harassed by a supervisor, called a "team lead." Once her computer is up and running, a message appears announcing yesterday's "productivity scores" in the form of a list ranking the performance of all thirty technicians at Schwab's tech-support call center from best to worst. Arranged in clusters of cubicles, the technicians work beneath a series of huge, elevated computer screens that display each person's name and a minute-by-minute productivity ranking.

"You look up and see who's cleared the most calls, who's done the least, whose phone is 'engaged,' whose is 'idle.' It brings out the worst. You want to win. And everyone just works constantly," says Winston, who prefers not to use her real name.

Such is life on the new shop floor, where surveillance and constant psychological pressure to work harder are increasingly common. According to the American Management Association, 80 percent of US corporations keep their employees under regular surveillance, and that percentage is growing all the time. From the low-tech body and bag searches at retail stores, to computerized ordering pads at restaurants and the silent monitoring of e-mail and phone traffic in offices, the American workplace is becoming ever more transparent to employers and oppressive for employees.

Along with being invasive and increasing the rate of exploitation, on-the-job surveillance makes it easier for supervisors to fire or harass restive workers. Rather than "freeing workers" and "flattening hierarchies"--as the New Economy hype would have it--computers, databases and high-speed networks are pushing social relations on the job toward a new digital Taylorism, where every motion is watched, studied and controlled by and for the boss.

The combination of software and hardware that keeps tabs on Winston is a Customer Relationship Management (CRM) system made by Aspect, the market leader in high-tech "contact servers." With 3 percent of the country's work force employed at call centers, Aspect's market is huge. Along with ranking workers against one another in real time, Aspect's system allows managers to listen in on calls, search for key words and archive all e-mail and voice traffic. This data can then be aggregated or disaggregated in almost any fashion. As one Aspect manager put it, their technology can "drill down" into stored data to retrieve a single, year-old call just as easily as it can search a massive databank for keystroke or call-time patterns that might indicate theft, drug use, pregnancy illness or union organizing.

But most important, Aspect's gear allows Schwab managers to create an intricate and invasive corporate culture based on measuring, ranking and intimidating the line staff. Schwab rituals are liable to send Foucault fans into paroxysms of "I told you so." Take, for example, "Normalization," a three-day, quarterly retreat in which managers collectively evaluate their subordinates and then publish a list of who gets bonuses and who gets discipline. Inevitably, this ritualized "benchmarking" of "best practices" raises the productivity bar ever higher. "A year ago we had three minutes after each call to write up what happened. That was called 'wrap.' Now there's no wrap time, we have to write notes as we handle calls," says Winston.

The regime at Schwab is just one example of the office as panopticon. According to federal law, all communications that occur on employer-owned computers and phone systems are automatically open to employer monitoring. Some states impose mild restrictions on workplace eavesdropping, and many corporations give new employees some, usually obscure, warning about surveillance in the fine print of their contracts.

Nothing has advanced surveillance in the workplace so much as the Internet, which creates both the reasons and the means for surveillance. With an estimated 122 million Americans having some sort of web connection on the job, there's plenty of cyberspace for all sorts of nonwork activities. One recent study by International Data Corporation found that 30-40 percent of all workplace web surfing isn't job-related.

Foremost among the web attractions--surprise, surprise--is pornography. According to the *Boston Herald*, one sex-industry survey discovered that 70 percent of all online pornography traffic takes place between 9 am and 5 pm. Last spring, for example, Victoria's Secret held a live, online, forty-five-minute lingerie show on a Thursday afternoon. According to one estimate, the show cost American firms a total of \$120 million in employees' lost work time. Large corporations routinely fire people for "inappropriate Internet" use such as porn surfing, gambling, online video gaming and chat-room socializing. In 1999 Xerox dropped forty offending employees in one swoop.

In response to such problems, many corporations with vast communications networks are loading up on computer programs that until recently were the sole domain of the Pentagon. Raytheon, for example, is offering a \$65,000 software package called SilentRunner that--instead of simply searching for suspicious keywords--uses complex algorithms to study relationships between people and computers for patterns that might indicate fraud, insider trading or espionage. The patterns, once found, can be displayed in three-dimensional onscreen graphics allowing investigators enhanced analytic powers. An added feature: The program is "passive," meaning it's almost impossible to detect.

Importantly, such technology isn't just for catching laggards and thieves; high-tech surveillance has also been used to break worker organizing. Ex-Intel employee Ken Hamidi, for example, ran an e-mail forum for Intel workers to discuss the grim side of working in silicon-chip plants. Intel tried to block Hamidi's communications; eventually a California court ruled that Hamidi's e-mails, sent to Intel's servers, constituted "unlawful trespass." By a similar logic, Northwest Airlines obtained a subpoena to copy the personal, home-based hard drives of employees who had used e-mail to organize an illegal sickout campaign during contract negotiations (the contract was signed before the subpoena was used).

Along with offices and call centers, the digital gaze is scrutinizing retail stores and even restaurants. Step into Calzone's, a crowded, middlebrow San Francisco eatery specializing in overpriced pasta with reheated sauce. Though trying hard to achieve an aura of sophistication and quality, Calzone's and its four sister restaurants turn a profit thanks in part to rigorously Taylorized operations that rely on the latest in handheld high-tech. Rather than taking orders on paper pads, the wait staff use the Pokky System, a network of mini handheld computers that beam information back to the bar and kitchen via

radio waves. The back-of-the-house staff receive the transmissions from a little printer that spits out paper tickets. This means less walking but it also means less talking, arguing, flirting and complaining among servers, bussers, cooks and bartenders.

"Pokky allowed us to cut our labor costs by at least a third," says Calzone manager Andre Ostabie. His sentiments are echoed by restaurateurs everywhere. One, whose praise is posted on the Pokky website, writes that the device "has literally dropped my labor cost back to the pre-minimum-wage-increase days."

Not all workers enjoy the changes. "You just end up working really, really hard," says Julia, a former waitress at a Pokky-"enabled" restaurant who prefers not to give her real name. "There was never a break. Compared to other restaurants, I handled about twice as many tables." Management counters that more tables equals more tips, but Julia says the tips didn't make up for the hectic ten-plus-hour shifts.

"Trying to organize a union there would be impossible," she adds. "We worked so hard that we hardly knew each other." There was also the issue of workers losing freedom to maneuver within the system, in either innocuous or subversive ways. Pokky's electronic inventory means no free meals or drinks, and no theft; unless, of course, a digital sabot gets stuck in Pokky's wireless gears... "I finally learned how to crash the system," says Julia. "Then we'd switch back to paper and I would steal whole bills: service an \$80 table and just pocket the cash." As for justification, Julia--something of a nihilistic Marxist--explains: "The boss and his wife were filthy rich; they forced us to work fifty-hour weeks. And they'd both blow all their money on cocaine and facelifts. So fuck 'em."

Employers and the security industry may exaggerate the extent of such activities, but it's undeniable that there are many Julias on the frontlines of low-wage America. And on-the-job theft raises the question: Whose actions are worse, the exploitative boss or the broke and pilfering worker? Regardless of one's position on this sort of informal class struggle, retail-level spying cannot simply be dismissed as employer paranoia.

Thus, about 2,000 restaurants nationwide now use some sort of handheld Pokky-style "point of sales" (POS) system. Jamba Juice, with about 300 outlets, has tested a similar device, the Amerauth Technology Systems UltraPad 2700. And many businesses use stationary versions of the same technology. For example, National Wholesale Liquidators just purchased a new point-of-sale system for tracking "data transfer" and "debit/credit processing." They expect to save \$2 million annually by cutting labor costs by 35 percent and reducing theft.

Increasingly, retailers aiming for "loss prevention" are deploying digital video and special software originally developed for casinos. One of the innovators in this realm is Loronix, which combines digital Closed Circuit Television (CCTV) with computerized "point of sales" technology (cash registers) in a unified system that feeds all data into a master computer where every keystroke and movement is archived. This data--both the keystrokes and the images--can be searched automatically for unusual patterns. If, say, a cash register shows more returns than average, that might be a sign of theft. To check it out, just review the video. Likewise, the video can be searched for suspicious visual patterns such as a cashier putting her hands in her pockets or looking over her shoulder.

Retail environments also use low-tech surveillance, like "spotters" or "mystery shoppers." Taco Bell has 150 full-time mystery shoppers who stalk the corporation's 7,100 outlets looking for rude staff, slow service and free refills. These fast-food snitches visit each restaurant at least once a month, using handheld computers from which they upload data to Taco Bell's corporate HQ in Irvine, California. One expert quoted in *Nation's Restaurant News* estimated that 90 percent of American restaurant chains use

mystery shoppers. And at Hudson United Bancorp, the fast-growing "community banking franchise" that fancies itself the McDonald's of finance, mystery shoppers track "sales per banker per day."

High-tech surveillance is even finding its way onto hospital wards. A small but growing number of nurses and orderlies have started wearing computerized "radio-wave" ID badges that transmit their location on the ward to a computerized map that is controlled by the shift supervisor. These systems include new bedside call lights and intercoms that are monitored from a central location. The overall effect is to put medical staff under ever-greater pressure to move from bed to bed.

"It's nonstop work," says exhausted oncology nurse Mary Alice Martinez. "Our patients are very sick. They're in acute condition and need a lot of physical and psychological care." Thanks in part to tracking systems like the radio badges made by Hill Rom, the patient-to-nurse ratio at the Peninsula Medical Center in Burlingame, California, where Martinez works, has increased from around six patients per nurse to eight. Such "efficiency" means that visiting with patients--known as "psychosocial interventions"--is steadily eliminated, as medical work is reduced to its purely physical functions in the interest of cutting costs.

Even working on the road is now subject to high-tech employer surveillance. American trucking firms have equipped tens of thousands of their vehicles with Global Positioning System (GPS) tags. These cell phone-size transmitters automatically beam the coordinates of their location to a series of twenty-four Pentagon-owned and -maintained satellites orbiting the earth. Thanks to GPS, big trucking firms like J.B. Hunt can instantaneously map the exact location of each truck and trailer in their vast fleets at any moment.

Wireless and digital on-the-job surveillance meld with old-fashioned Taylorism most dramatically at United Parcel Service, the country's fourth-largest employer. Known among its workers as "Big Brown," "Uncle Brown" or the "Brown Machine," UPS, which handles 7 percent of US GDP on any given day, has more than 359,000 workers worldwide and has been described by one outside analyst as among "the most technologically sophisticated companies doing any kind of business anywhere."

Always a rigorously ordered firm with a penchant for time-motion studies, UPS began a high-tech makeover in the mid-1980s by purchasing two leading technology companies to develop and test specialized package (and people) tracking equipment. By the early 1990s UPS was busy forging the first nationwide cellular service, a task that involved creating a partnership between four major telecommunications firms and their seventy-five junior partners.

What emerged from all this was a superwired workplace where every detail is watched by a computer. At the heart of the new system is the "Delivery Information Acquisition Device," known as a "DIAD board." Carried by drivers at all times, this computerized clipboard combines the functions of a time clock, GPS tag and two-way text-based pager. At best the DIAD enhances flexibility and efficiency; at worst it is an electronic leash that keeps UPS drivers working at a furious pace.

Simply stated, the DIAD is the Poky system on steroids. Work starts when drivers log on to the DIAD with their personal ID. Using cell-phone technology, the DIAD board logs number, sequence and duration of stops; clocks the speed of each task; notes the driver's location; and communicates all this to a receiver in the truck, which automatically relays all data to the local dispatch center and to a huge UPS database, where information is archived and kept for at least eighteen months in one of the world's largest computers. Similarly, long-haul drivers at UPS are monitored by a device called IVIS, which records and transmits the driver's work patterns and rates of speed, as well as minutiae of engine performance, from temperature to average miles per gallon.

What is all this surveillance for? "It's to grow the business and provide better service," says Pat Canavan, UPS vice president for package project management. When asked about cutting labor costs, company spokesperson Joan Schnorbus explains that "the union has been involved in the process at every step of the way. This is about creating more jobs through growth."

True, but perhaps not the whole story. Some of the more political elements in the Teamsters, like activists in Teamsters for a Democratic Union (TDU), see another dimension to the brave new technologies. "The holy grail, for management, is to scab a UPS strike," said Charles Richardson, a researcher who has analyzed UPS on behalf of the union. Richardson argues that the technological leap forward at UPS is really about "stealing knowledge" and making smart machinery that can be operated by not-so-smart scabs. Currently, work at UPS is too complicated and time-sensitive to use scab labor. Thus, during the 1997 strike the company shut down operations rather than hire replacement workers.

But short of scabbing, UPS technology can already be used to fight union activism. Steve Henderson, a UPS driver in West Virginia, says surveillance was used to harass and target him because he is a TDU member and was active in the strike. Along with scrutinizing every detail from his DIAD reports and subjecting him to managerial ride-alongs, UPS sent spies out to secretly videotape Henderson while out on his route. They finally busted him taking an unauthorized eighteen-minute bathroom break at Hardee's because, Henderson says, he was sick. UPS fired him for "stealing time." Drivers and linemen at Southern New England Telephone reported similar harassment involving the overuse of GPS reports after they won a strike. "They're out to getcha, man," says Henderson, who eventually won his job back with union help. "Only thing to do is watch out and stay organized."