5: Watching You Work

It was the moment Anna had been dreading. Ever since a coworker logged in to Anna's computer and sent the boss an e-mail saying, "I'm now in the office," she'd known it might come back to bite her. And it did. Here she was, standing in front of him, tears welling, trying to explain that she didn't tell her coworker to lie about what time she arrived. The boss didn't care, and he certainly didn't believe her. After all, his computer system had discovered the "fact" of the erroneous e-mail, and he was pleased with himself for unearthing a contradiction in Anna's record.

Because she typically got to the office at 6:00 a.m., well before any of the managers, Anna was supposed to send the boss an e-mail, and its time stamp would serve as a clock-in time. Her coworker *thought* she was doing her a favor by clocking her in when she was late for work. But the boss was suspicious—and maybe had way too much time on his hands. So he logged in to the electronic system for the building's parking garage, pulled up the time she swiped her parking card, and compared that with the time posted on the e-mail. Discrepancy discovered! The e-mail was sent forty-five minutes before Anna's car entered the garage.

With disbelief and anger mounting inside her, she listened to the gloating manager inform her that she was formally on probation and had better start looking for another job. It didn't matter that she routinely worked overtime without extra pay. It didn't matter that she never took the ten-minute breaks allowed by law. It didn't matter that she never tried to deceive anyone about what time she arrived. The electronic systems of the office and building had been transformed into surveillance systems, and the boss was eager to use them to punish her.

This story is not made up. It happened to one of our friends a few years back. And it's also not exceptional. Workplace surveillance is the norm for just about all jobs. Sometimes surveillance technologies are direct programs of observation clearly designed to monitor and discipline employees, like drug testing or keystroke tracking. Other times, as in Anna's story, the technologies are designed for different purposes (sending e-mail or entering a parking garage), but they lend themselves to surveillance. This second set of uses is what we've referred to in previous chapters as function creep, because the systems creep beyond their original purposes. Whatever you want to call it, the workplace is crawling with surveillance, and a lot of times people don't even realize it.

Taylorism: The Science of Working Faster

Workplaces have always been places of surveillance. In some accounts of early capitalism, one of the main reasons decentralized production systems were first implemented in shops and then in factories was so bosses could keep a closer eye on their workers. Whether people work in shops or offices, factories or fields, techniques of monitoring and control have been interwoven with labor processes for a long time. But workplace monitoring encountered a fundamental shift in the early twentieth century when a new idea was born: use "scientific" techniques to manage workers in factories to achieve optimal efficiency.

Frederick Winslow Taylor, one of the engineers at the heart of this new enterprise, used a stopwatch to time workers and analyzed their movements in an effort to discover the quickest and most efficient ways to perform repetitive tasks.[1] One of the problems he sought to eliminate was "soldiering," where workers would deliberately slow down to make labor less taxing and more tolerable. Taylor's method consisted of breaking down tasks into their components, assigning workers to the tasks they performed best, and disciplining those who did not consistently operate as quickly as possible.[2] This general technique was called scientific management; today it's often referred to as Taylorism.

Taylor was not simply looking to increase productivity and punish workers. He was advocating for the formation of a new managerial class that he thought could bring about social and economic prosperity by applying scientific principles to the workplace. In 1911 he wrote,

All the planning which under the old system was done by the workman, as a result of his personal experience, must of necessity under the new system be done by the management in accordance with the laws of the science. . . . One type of man is needed to plan ahead and an entirely different type to execute the work.[3]

From this quotation we see that Taylor was attempting to use scientific explanations to justify the subordination of workers and the elevation of managers and engineers. Even today we may perceive managers, who oversee our work, as a natural and necessary component of any organization, but it was men like Taylor who created this "necessity."[4]

One serious downside to scientific management is that it's dehumanizing—it treats workers like machine parts that can be manipulated and discarded at will. In 1913 some workers at a military arsenal wrote to their congressman:

We object to the use of the Stop Watch, as it is used [as] a means of speeding men up to a point beyond their normal capacity. It is humiliating and savors too much of the slave driver. . . . [The Stop Watch system] has resulted in accidents, inferior work and numerous abuses such as no American Citizen should be called upon to endure.[5]

In response to opposition by arsenal workers and trade unions, Congress eventually eliminated scientific management programs at all federal installations,[6] but the ideas have continued to shape management practices throughout many organizations.

Ford Had a Better Idea

Taylor wasn't the only one trying to get more out of workers. Drawing inspiration from the Chicago meatpacking industry, Henry Ford is often credited with instituting a version of scientific management in his automobile assembly lines. Ford's assembly lines are among the most famous icons of industrial efficiency—they allowed for important changes in the visibility and accountability of workers, who were now in the open, each performing one specialized task, under specific guidelines for speed and quality. But Ford's surveillance extended beyond the factory walls and into workers' homes. In 1913 Ford created a

Sociological Department (later renamed the Educational Department) to engage in a moral mission of monitoring workers outside the workplace to ensure that they were upright individuals of good character. The investigators of the Sociological Department "visited workers' homes gathering information and giving advice on the intimate details of the family budget, diet, living arrangements, recreation, social outlook, and morality."[7] Workers were put on probation or fired if they "refused to learn English, rejected the advice of the investigator, gambled, [or] drank excessively."[8]

While some of this may sound outrageously paternalistic today, employers still make judgments about employees' character based on how they look, how they talk, their sexual orientation, or whether they use prohibited recreational substances. Though many forms of discrimination are now illegal, that doesn't stop these practices from happening behind the scenes. And in some cases, as with drug testing, employees are still held accountable for what they do when they're not working, regardless of whether it affects their job performance. (More on this later.)

Surveillance in the Modern Workplace

Taylorism is alive and well in the surveillance society. The electronic systems we use at work automatically log almost everything we do, rendering our activities more "manageable" through analysis and comparison. In other words, workplace technologies simultaneously enable us to do our jobs *and* create data so others can evaluate our performance. Communications scholar Mark Andrejevic explains:

> Keystroke monitoring programs, for example, deter employees from using computers for non-work-related activities while they simultaneously provide a detailed record of worker productivity. Bar code scanners in supermarkets serve not only to record prices, making the checkout worker's job faster and easier; they can also keep track of the checker's scan rate to monitor productivity, as can portable, networked, GPS-equipped devices for delivery workers and truckers.[9]

Even the American farmer, a long-standing icon of independence, might be driving a tractor with a GPS-computer interface that uses satellites to guide the plowing and provides full reports and maps on

the day's coverage.[10] We've left the stopwatch in the dust. Taylor would be proud.

Currently about 75 percent of employees at American companies are subjected to *regular* surveillance at the workplace, while employees who use the Internet at work stand a 33 percent chance of being exposed to *constant* surveillance.[11] Even employees who engage in hard, unrewarding manual labor, such as hotel housekeeping, are subject to electronic scrutiny and performance monitoring. During a recent hotel stay, one of us was puzzled that the housekeeping person assigned to his room was visibly upset when he told her she didn't need to clean the room. She knocked on the door once more and asked if she could use the phone. As she picked up the receiver, she explained that she had to enter her code into the room's phone so management would give her credit for making up that room. The telephone surveillance system was gathering metrics about the number of rooms cleaned, how fast they were cleaned, and which worker was doing the cleaning. If guests complained, blame would be easy to assign. Likewise, it's not difficult to imagine that these data were being used to discipline—or "motivate"—workers who cleaned too slowly. Some hotels even track their housekeeping staff's productivity with a cell phone app that measures movement and speed at all times.[12] If workers stand still or sit down for even a few seconds, management knows.

"This Call May Be Monitored"

Of all service-sector jobs, call centers push workplace surveillance to the extreme. These jobs often crush workers together in a honeycomb of cubicles with almost no privacy: bosses and coworkers can hear you amid the din of voices, can see you over the low walls, and can track your minute-by-minute productivity score on LCD monitors.[13] The electronic surveillance extends much further, too. At most call centers, such as the ones operated by Time Warner Cable, expectations are broken down second by second: "2 minutes, 30 seconds—average length of call; 16 seconds—the maximum time a customer can be left on hold; 8 seconds—the time to complete paperwork between calls. Simply finding time to go to the bathroom can be tough."[14] Your phone must be active at almost all times, typically with only five to twenty seconds allowed between calls.[15] In telemarketing call centers, automated systems called "predictive dialing" increase pressure further by automatically

dialing the next call as soon as the last one is terminated, pushing workers to achieve on-phone rates of up to fifty-four minutes each hour.[16] Of course, managers can listen to your conversations in real time to see if you have a friendly tone of voice and are technically competent,[17] but evaluation of your performance can happen retrospectively too, because all calls are recorded and archived; all e-mails and computer keystrokes are saved; just about everything you do, in fact, is instantly converted into "data."[18]

All this is done in the name of efficiency, just as Taylor proposed, but the experience is grueling for workers. Indeed, "e-slave" has entered the urban slang lexicon to describe call-center employees who put up with tremendous stress, work long hours, and have unpredictable schedules.[19] Some workers refer to the call-center performance systems as a "technological whip" that automates the slave driver's task, contributing to a general climate that includes "bullying, impossible sales targets, not receiving wages on time, and hostility to unions."[20] Given this harsh environment, some call centers have an annual turnover rate of over 100 percent.[21]

And managers are constantly on the lookout for ways to increase output, even if it pushes workers to the breaking point.[22] At a tech support call center operated by the Charles Schwab brokerage firm, one worker related: "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."[23] To cope with this labor intensification, employees must shift that time on to customers; one worker at a different call center explains:

> What you end up doing is keeping the client on the phone while you enter your notes, which makes an already annoyed customer become even more annoyed. And doing that is just a charade—you're wasting the customer's time just so you can avoid getting a "hit" [being disciplined] for refusing an inbound ring.[24]

"Your Call Is Important to Us"

Have you ever felt that your call wasn't taken in the order received? Well, you were right. "Customer relationship management" (CRM) systems triage calls in order of importance based on how valuable you are as a customer. If you fit the right demographic, are calling from the right area code, buy a lot, or

seldom complain—all of that is logged in your profile, and you might be given preferential treatment because of it. Or if you're not in a valued category, you could be stuck forever in the purgatory of phone-tree mazes and on-hold music. CRMs are social sorting systems par excellence: they're automated, invisible, and discriminatory. Now government offices also use them to manage their customers/citizens.[25]

Performance Monitoring

Performance monitoring can be found just about everywhere these days, with the use of wireless order-entry systems to monitor servers in restaurants, GPS devices to track truck drivers, or databases to evaluate the productivity of professors. What does performance monitoring mean to the people involved? From management's perspective, it's a mechanism for achieving efficiency, accountability, and quality. It also implies the ability to make decisions, especially disciplinary decisions, based on the results gathered. As the Institute for Management Excellence puts it, "It is a fact of life that employee performance monitoring, discipline and dealing with employee issues is part of a manager's job—it actually defines what a manager is: someone who has the authority to hire, fire and discipline."[26]

From the perspective of nonmanagement employees, performance monitoring means that workers are subject to varying degrees of surveillance and must strive to prove their worth. It's a fancy way of saying they must work harder and compete for scarce resources to have any chance at job security, raises, or promotions. It implies a state of insecurity for most employees and a lack of trust by managers. At its worst, performance monitoring can create a hostile workplace; at its best, it can allow for structured feedback and improved performance. Either way, like other forms of surveillance, it's always an expression of power.

Performance-monitoring systems shape human behavior and action. As we noted in the first chapter, technologies guide what is considered possible and desirable. With a critical lens, we can "read" technologies to see what values they possess and what types of relationships they produce: Competition or cooperation? Suspicion or trust? Hierarchy or equality? At a very basic level, of course, performance-monitoring regimes are antithetical to the value of human autonomy—the under-

lying premise of such surveillance is that humans can't be counted on to self-regulate and work productively without close bureaucratic supervision. In this way, performance monitoring normalizes hierarchical relationships between managers and workers. It makes it *seem* natural that management should constantly monitor and evaluate employees or that managers should have power over others in the workplace. That these statements probably sound obvious shows how persuasive this particular management paradigm has been. In comparison, the idea of a more democratic workplace, whether through collective bargaining with labor unions or simply through a more egalitarian structure, may sound idealistic or inefficient, especially to American readers, even though plenty of workplaces thrive under such models.[27]

Performance monitoring also feeds the illusion that the criteria used to evaluate employees are objective and unbiased, even when there are many standards for evaluating work (e.g., quantity, quality, creativity, effectiveness, customer satisfaction, teamwork, safety, employee happiness). One unfortunate effect of widespread performance monitoring is that it allows the criteria of competition, speed, and efficiency to outweigh others that might be just as good or even better, such as cooperation, trust, meaningful participation, or care. This subordination of alternative criteria is bad enough for most jobs, because it can diminish workers' satisfaction and investment.[28] And in professions intended to help others, such as teaching or nursing, performance monitoring and other forms of Tayloristic surveillance may have even more harmful effects. Let's take a closer look.

A Day with Nurse Betty: Hospital Tracking Systems

Nurse Betty has a problem. She cares deeply about her patients and wants to give them the attention they need to get better and not feel frightened or lonely. But hospitals don't make money by giving this kind of care; they make money by keeping all their beds full, running procedures, assigning patients the bare minimum of nurse support, and quickly discharging them once the profitable tests are done and it's safe for them to leave—and sometimes before it's safe. By speeding up "throughput" in this way, like factories, and by running a lot of tests, hospitals can maximize the billing potential for each patient.[29]

Nurses at Betty's hospital, and at many others, had creatively resisted management's drive for increased patient throughput. One way they

did this was to pretend patients were still in the hospital even after they'd been discharged. That way new patients wouldn't be loaded in quite so quickly. Fewer patients to take care of meant more time could be spent with each patient. Being responsible for fewer patients also meant nurses didn't feel quite so frenzied, stressed, and burned-out. This coping mechanism was possible because Betty and her colleagues had to enter data into a computer system when a patient was discharged so the room could be cleaned and made ready for the next patient. If nurses delayed entering these data, it would effectively slow down admissions and reduce the number of patients under their care.[30]

But hospital administrators have installed new surveillance systems to make sure Betty and others cooperate with the assembly line. One is a bed management system that relies on radio-frequency identification (RFID) tags for patients. Embedded in a patient's wristband, the small RFID chip is automatically scanned when it passes detectors at the hospital exits. As soon as the wristband leaves the hospital, presumably on a patient, the bed management system is triggered to update that patient's room status to "empty" and send an alert so housekeeping staff can clean the room. Thus new patients are admitted quickly, and nurses are forced to adapt. In a constant battle over control of the workplace, some nurses have responded by removing patients' wristbands and leaving them in the rooms. The danger is that this maneuver more clearly constitutes intentional circumventing of the system rather than simply "forgetting" to update the room status in the system.[31] Thus nurses who do this are more easily disciplined.

Meanwhile, on another floor, hospital emergency departments worry about admitting *too many* patients or admitting patients who aren't sick enough. Because only so many beds are available, it's better for them to be occupied by the sickest patients so that care can go to the neediest and hospitals can generate the most revenue. It's a tough balance: if hospitals have empty beds they make less money, but if all their beds are full, they may have to divert needy patients to other hospitals (or have them waiting on stretchers in hallways), which is not good. So physicians in emergency departments are subjected to routine performance monitoring and pressure to admit fewer patients. One hospital administrator explained:

We monitor all the activity of all our docs. We give them reports every month on their acuity, their time to disposition, the number of tests per

doctor per diagnosis, their efficiency in terms of what we pay through the department, and that's all recorded. And your abilities, your bonuses, all that information is used as a 360[-degree] view of you as an emergency physician in the department. But if you're admitting twenty-two percent or twenty-three percent, twenty-four percent, then . . . you should be more tight with your admissions because you're actually losing [the hospital] money. . . . The chairman would say, "You know, the last couple months you've been admitting a lot more percentiles. Just try to bring it down a little bit."[32]

Perhaps because of their high professional status, physicians are probably more often given incentives to admit fewer patients rather than punished for admitting too many. Still, performance monitoring can serve as public shaming, because monthly reports typically include names alongside performance scores.

Another hospital surveillance system relies on RFID tags worn by the staff. Under the Tayloristic name "workflow management," administrators use these tags to track the movements and locations of staff in real time. The ostensible goal is to reduce redundant movements, minimize inventory, and "rationalize" hospitals so they are as efficient as possible.[33] While all that sounds smart and practical, surveillance is always about control, so the people under its gaze seldom see it in such a positive light.

What ends up happening is that hospital administrators can't help but discipline workers whose locations are being tracked. In one case a hospital was just piloting a workflow management system and asked staff to wear RFID-embedded badges. An administrator saw that two orderlies, people who transport patients, were hanging out at a loading dock, so he called them on their walkie-talkies and asked where they were. When they both lied about their locations, the administrator stormed down to the loading dock and fired them on the spot.[34] The intended purpose of the system was to improve efficiency, and workers were never told they'd be spied on, but once the system was in place it was automatically transformed into a disciplinary surveillance technology.

Although various tracking and performance-monitoring systems in hospitals may improve some measures of productivity, they may also produce unintended consequences that burden workers and their patients. If their primary goals are to increase throughput and save (or make) money, then the health care mission of these organizations may

suffer. Then again, many people and communities may suffer if hospitals go out of business, so the problems are much deeper and more complex than simply saying no to workplace surveillance and yes to care and compassion. Nonetheless, many hospital staff find tracking systems unreasonably invasive and feel they diminish autonomy and trust in the workplace.[35] Some nurses even intentionally smash RFID tags and sabotage the systems.[36] It stands to reason that authentically involving workers in decision making and organizing workplaces to provide incentives instead of punishments would boost morale and combat arbitrary abuses of power.

Cheers!

Bartending may look like fun, but every drink bartenders pour can be scrutinized by RFID-enabled pour spouts and wireless surveillance systems. Want to give someone a bigger shot for a better tip? Don't try it with these systems in place. They send information about what drink was poured, by whom, at what time, how many ounces were poured and how many ounces should have been poured. There are even systems for regulating the pouring of draft beers. According to one bar owner: "My staff know their every move is being watched. If they are doing their jobs well, I will see it. If they need a tune up I will see it. Even if I see things days later I can go back to the archives and get all the detail I need."[37] As if dealing with a bunch of drunken people weren't hard enough.

The "Eyes in the Sky" at Casinos

One of our students was a blackjack dealer at a casino. She described the elaborate rituals she had to perform for the invisible security staff watching her through cameras mounted above her table. She had to ensure that her hand of cards was never lifted more than forty-five degrees off the table; she had to position the deck at a precise angle to the edge of the table; she couldn't touch her cards or the deck unnecessarily, because it might be construed as a signal to a player; when she accepted tips, she had to tap the chips against the table and immediately place them in her tip container; and when she left the table, she had to clap her hands together and turn them palm up for the cameras to see. Any deviation from protocol would automatically trigger an inspection from security that could result in disciplinary action.

Casinos are test beds for cutting-edge, integrated surveillance systems. Because of the tens of billions of dollars in profits they make each year,[38] they're supercharged with systems many government agencies only dream about. It's not just the dealers who are being watched—it's everyone. As one director of surveillance puts it, "There's nowhere on the casino floor that you can hide."[39] When people walk into a casino, the video cameras quickly process images of them through a facial recognition system that determines whether they are in a database of restricted customers.[40] If they are, staff in the security room will radio down to security personnel on the floor to escort them off the premises. Even smaller casinos tend to have over a thousand cameras, some that remain stationary over tables and many that can pan, tilt, and zoom to follow people.[41]

In addition to elaborate camera systems and facial recognition technologies, casinos now have a way to track chips by embedding radio-frequency identification tags in every one of them. These "smart chips" can then be used on "intelligent tables" to track the exact bets of every player, determine the players' value so they can be "comped" for drinks or shows if they're high rollers, and deter the theft or counterfeiting of chips.[42] Security staff can automatically count and audit chips to make it harder for cashiers to steal. There are already prototypes in the works for RFID-embedded cards, but until they're adopted there are other ways to monitor gamblers' hands: "A new technology from MindPlay reads invisible codes on cards as they're dealt from the shoe. The system knows, in real time, what players are holding and betting. Casinos can snare card counters by comparing their play with known counting strategies."[43] The goal is total transparency. And because casino employees are involved in an estimated 34 percent of all instances of theft or cheating, they're watched very closely.[44]

Of course, surveillance doesn't rely entirely on technologies. The technologies are complemented by nested systems of people watching people: inspectors watch dealers; pit bosses watch inspectors; floor managers watch pit bosses; security staff watch everyone from another room; and they are watched by other security staff at remote locations.[45] Besides deterring theft, some of the control functions are designed to make workers more accommodating to clientele. For instance, dealers are expected to have "outgoing personalities," put up with flirtation, and encourage players to make higher bets.[46] Similarly, waitresses in casinos are monitored to make sure they act as "objects of desire" by

dressing suggestively and flattering gamblers; if waitresses don't cooperate, bartenders slow down their drink orders so they receive worse tips.[47] It shouldn't be unexpected that the "eyes in the sky" at casinos would support voyeurism, objectification, and control of others—that's exactly what they're designed to do.

Corporate Espionage

Jerry Treppel thought someone was going through his trash at night, but he wasn't sure, so he hired a private investigator. The PI hid behind a fence all night and, sure enough, saw two men take Treppel's trash away and put decoy replacement trash back in the cans. As the men drove off in a gray minivan, the detective discreetly followed them and then tracked down their identities. The trash stealers were private investigators too! They were hired by the Biovail Corporation, a Canadian pharmaceutical company that Treppel was suing for allegedly damaging his career.[48] (Treppel was a securities analyst at an investment firm. When he advised investors to sell Biovail stock, that company insisted he be reprimanded. Soon after, he was fired.[49]) Hiring PIs is just one of the many surveillance tactics corporations use to spy on individuals, other companies, and governments. Welcome to the world of corporate espionage.

In another telling case a few years ago, the technology company Hewlett-Packard (HP) got into a lot of trouble for hiring private investigators who had little respect for the law. Patricia Dunn, then chair of HP's board of directors, had a problem with board members' leaking secrets to the media. To find the culprits, she hired a firm of private investigators that supposedly hired another company to engage in the seedy practice of "pretexting." Pretexting is an identity theft technique of calling a company, such as a bank or public utility, and pretending to be someone else so you can get access to private information. In this instance PIs got the Social Security numbers and phone records for more than twenty-four people, including HP board members, other employees, and nine reporters.[50] One PI changed a reporter's cell phone password so he could listen to her messages and scrutinize her call log without her interrupting.[51] Patricia Dunn and others involved were fired and charged with four felony counts. A California judge, who was evidently soft on (corporate) crime, dismissed the charges.[52]

What's probably most remarkable is that these examples were made

public at all. Companies engage in corporate espionage all the time. They want to discover trade secrets. They want to know who's leaking sensitive information. They want to know what their competitors are doing. They want to figure out who's counterfeiting their products.[53] They want to know a lot, and they're sometimes willing to transgress ethical and legal boundaries. Employees may thus be the unwitting targets of surveillance by other companies or by their own.

Because corporate espionage is commonplace, private investigators are busier than ever. Close to sixty thousand PIs are licensed in the United States, and who knows how many more are unlicensed.[54] Some of the corporate spies are even current, active-duty CIA agents who are granted permission by the agency to "moonlight" at private companies.[55] And the spying isn't just on behalf of high-powered technology and pharmaceutical companies. The entertainment industry, the insurance industry, the chemical industry—they all do it. Even the circus industry has been involved with hiring PIs to infiltrate People for the Ethical Treatment of Animals and other animal rights groups.[56] Espionage is now a key risk management technique used by many companies.

For most employees, this just adds one more layer of (potential) surveillance to their lives. In addition to companies' running background checks before hiring people, monitoring their electronic communications, and subjecting them to performance monitoring, employers and their competitors may be digging through workers' trash or accessing their phone records. It may be next to impossible for individuals to protect themselves. According to one private investigator, "If someone is willing to break the law to get your personal info, there's almost nothing you can do to prevent them."[57] In the summer of 2011, the world discovered just how true this was when we learned that major newspapers were hiring private investigators to tap into the voice-mail systems of celebrities, killed British soldiers, high-profile crime victims, and members of the royal family.[58]

The New Ford: Drug Testing and Moral Management

Early in this chapter, we saw that Henry Ford had a special department monitoring the home lives of his employees to ensure that they were living up to his moral standards. He believed that the ideal workers didn't just get the job done; they lived their personal lives as the Ford Motor Company preferred. These days this sort of corporate paternal-

ism is frowned on as overreaching—most of us expect that if we do a good job while we're on the clock, the rest of our lives belong to us.

But do they? We've given several examples of the ways contemporary surveillance is used by businesses in their attempt to reduce risk and successfully manage their workforce. Credit checks see if potential employees are good with their money. Background checks search not only for arrests or convictions, but also for past use of workers' compensation or lawsuits. In many workplaces, regulations prohibit hiring smokers, while "wellness programs" give special encouragements to those who work out in the company gym or pursue other healthful lifestyle choices. It may not be enough that you're a whiz at programming—you may need to be a healthy, nonsmoking, exercising, debt-free programmer with a clean legal history and no record of using workers' compensation.

One now commonplace example of this invasive management is the drug-testing frenzy that emerged back in the 1980s. Testing job applicants, employees, welfare clients, and even students typically can be done with relatively low-cost kits that analyze a urine sample to detect evidence of drug use. These tests measure certain residues left in the body *long after* drug use. Because of this quirk in the technology, drug-testing programs provide no evidence regarding current intoxication or impairment. Instead, they implement a 24/7/365 monitoring program on what employees take into their bodies—a far more encompassing version of Henry Ford's inspections of his employees' homes.

If it weren't for all the human pain, wasted money, and nasty politics, the saga of workplace drug testing might be a comedy rather than the tragedy it is. The movement began with a passion during the Reagan administration's War on Drugs of the 1980s. The push to test the urine of America's blue-collar workers was ready-made for the politics of the era. As part of the War on Drugs, workplace drug testing deputized America's employers as quasi-government enforcers of drug control laws. It included overblown claims that America's workers were stoned; it put labor unions in the position of seeming to defend workers' right to be stoned; and it offered a dramatic expansion of employers' power over employees as the moralist commands followed workers home for the weekend and on their vacations. Finally, it meant a huge new stream of revenue for America's pharmaceutical industry, a perennial heavyweight in campaign contributions.[59]

Drug-testing technology was first developed in prisons and the mili-

tary. The next wave of the rollout was in safety-sensitive positions like pilots, train crews, law enforcement, and power plant personnel. Job applicants were brought into the game when prices dropped on low-quality screening tests, and then in some areas those who applied for public assistance were required to demonstrate their abstinence. Along the way, high school students got in on the fun as some districts began testing athletes and anyone else who participated in school-sponsored activities.[60]

Yet this sort of testing for illegal drug use just doesn't make a lot of sense. The most damaging drug in the American workforce is alcohol, which is almost never tested for and was never part of the American debate over drugs in the workplace. Another puzzle is that most drug tests are best at detecting signs of marijuana, which can stay in the body for weeks after use, while evidence of more serious drugs disappears more quickly. So employee drug testing basically skipped the serious stuff to give corporations the power to examine the marijuana smoking habits of their off-duty employees. Add in that drug tests don't even measure current impairment—only past use—and we've got some pretty major disconnects in the safety-testing rationale. The almost silly, unnecessary intrusion of these surveillance policies drives home a point we see in several parts of this book: surveillance doesn't always make sense from a technical, rational, problem-solving perspective. Sometimes it seems to be about power for power's sake or inspired by other motives that wouldn't stand the scrutiny of public discussion.

Checking You Out

Chances are good that if you apply for a job, your prospective employers will try to dig up some dirt on you. They may call your references, request credit reports, or—as we've mentioned—run criminal background checks. They'll probably Google you too. Additionally, 75 percent of US companies now conduct formal searches of applicants' online activity, and 70 percent admit rejecting candidates based on the information they've found.[61]

Some entrepreneurial companies have sprung up to help employers run online background checks. Social Intelligence is one of the big ones, and it claims to do "deep" web searches on individuals, tapping into social networking sites, blogs, Tumblr, Craigslist, Yahoo! groups, and many, many more sites.[62] They've even received the blessing of the Federal Trade Commission to archive *all* social networking posts for

seven years.[63] So cleaning up your Facebook page a few months before applying for a job won't help because seven years of posts may already be on file, ready to be mined for any compromising tidbits.

Some of the things they say they look for are sexually explicit photos or videos, racist remarks, or evidence of illegal activity. But there's also a gray area of subjective indicators they may use to weed out candidates: things like making inappropriate comments, holding marginal political views, or having a questionable lifestyle.[64] The chief executive of Social Intelligence says, for instance, that a red flag was raised by a photo of someone next to some large marijuana plants in a greenhouse.[65] While we can easily see that this is not evidence of "illegal activity," it was suggestive enough to eliminate that person as a candidate. Another person belonged to a Facebook group supporting the exclusive use of the English language in the United States.[66] While we may not agree with this position, it isn't evidence that the person would treat non-English-speaking people differently—indeed, belonging to a "group" isn't even proof that a person believes in that position. Discrimination against prospective employees can take many forms, however, and some are perfectly legal. Currently, for example, employers shouldn't ask (or search for information) about your race, age, religion, marital status, or disabilities, but federal employment law doesn't prohibit them from asking about your sexual orientation.[67]

Finally, don't think employers will stop watching your online activity once you're hired. Social Intelligence also offers ongoing monitoring of all employee posts, photos, videos, and groups and serves up "near real-time notifications and alerts" to supervisors.[68] So if someone tagged you in a questionable photo over the weekend, you might be fired for it on Monday morning. Think of it as Workplace Surveillance 2.0.

Back Talk

Now a high-priced man does just what he's told to do, and no back talk. Do you understand that? —FREDERICK WINSLOW TAYLOR[69]

It is a degradation of human beings, Damn You.
—An American worker, commenting on urine-based drug testing[70]

Despite Taylor's hope, back talk has been a big part of the story of workplace surveillance. A lot of resistance these days occurs on the Internet on blogs, websites, and other "rant" forums, which is one reason com-

panies are monitoring these media. In an era where corporations try desperately to control their public image, companies see online venting by workers as a real threat that may damage profitability and perhaps even put them out of business. And there are an overwhelming number of "workplace sucks" sites: WalmartSucks, RadioShackSucks, HomeDepotSucks, and thousands more.[71] It's not clear whether such sites have been effective at reducing workplace surveillance, and they may have increased it (as companies monitor the sites and try to shut them down), but they do offer a public venue for griping, outing unsavory corporate practices, or whistle-blowing. They also provide a medium for isolated workers to join together and collectively push for policy changes.[72]

In a more traditional vein, labor unions have been at the forefront of political struggles over such things as employee drug-testing programs, new means of tracking employees' locations, call and keystroke monitoring, and test-based assessments of teacher performance. In our discussions of ID cards and schools, we looked at the quiet, everyday resistance to surveillance that individuals practice in their lives. But here we're going to note that the politics of surveillance also include some prominent public battles that end up in courts and legislatures.

It's no surprise that workers fight back against surveillance—so do corporations when they oppose regulatory inspection and government agencies when they fight "sunshine" laws. Surveillance is an expression of power that reduces autonomy and expands the visibility of our actions—people and organizations typically have a strong interest in opposing intensified scrutiny. In much of the surveillance covered in this book, the people targeted are not well positioned to fight back. Consumers, for example, are not typically shopping as an organized group, so they lack the information and collective clout to do much about anything. Students, criminal suspects, drivers, job applicants, and others typically find themselves in the same lonely and powerless boat.

But unionized workers have been a particularly strong source of opposition to increasing surveillance. By pressuring legislators, filing lawsuits, and working with regulatory agencies, unions have been able to at least publicize and modify, if not fully prevent, increases in the surveillance of their workers. Working with more specialized groups—like the American Civil Liberties Union, the Electronic Privacy Information Center, and Privacy International—unions try to play the role

that privacy regulators and agencies tend to neglect, especially in the United States. With US labor unions declining in membership and political influence, one of the most effective forms of political opposition to surveillance may be disappearing. It remains to be seen whether online tools and social media can pick up the slack and slow—or roll back—the seemingly inexorable push of workplace surveillance.

Conclusion

Like schools, the typical workplace is defined by the struggle to manage large numbers of people. In each environment, one group attempts to exert power over others. And in each environment, too, the new arsenal of the surveillance society is redefining our daily lives. With performance monitoring, cubicle farms, keystroke tracking, background checks, drug testing, and all the other facets of surveillance in the modern workplace, the trends most famously linked to Frederick Winslow Taylor have become a way of life. Older means of surveillance such as audits, double-entry bookkeeping, time clocks, and simply concentrating workers in single, observable locations now seem like quaint throwbacks to a simpler era.