<< Return to article

Surveillance Nation—Part Two

In pursuit of security and service, we are submitting ourselves to a proliferation of monitoring technologies. But a loss of privacy is not inevitable.

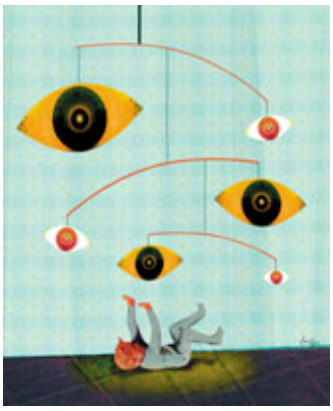


Illustration by Brian Stauffer.

By Dan Farmer and Charles C. Mann
May 2003

“Give me Duquesne minus 7, for a nickel.”

It was February 1965 on a lonely section of Los Angeles’s Sunset Boulevard, and Charles Katz, one of life’s little losers, was placing an illegal sports bet over a public telephone. Unbeknownst to Katz, however, the FBI had placed a microphone atop the telephone booth to record this small-time gambler’s conversations.

Engineers often mock the law for lagging behind technology. In fact, the law is often far ahead of it. This time it was ahead by nearly 200 years, for after Katz’s arrest his lawyers argued that although the framers of the Constitution could not possibly have encountered tape recorders and telephone booths, the Fourth Amendment’s ban on “unreasonable” searches nonetheless covered them. Because the FBI had no search warrant, Katz’s lawyers said, bugging the phone booth was illegal. In a landmark decision, the Supreme Court agreed, affirming for the first time that electronic surveillance was—constitutionally speaking—a search. “No less than an individual in a business office, in a friend’s apartment, or in a taxicab,” the majority declared, “a person in a telephone booth may rely upon the protection of the Fourth Amendment.”

Equally important was Justice John Harlan’s concurring opinion. The government, he argued, could not freely eavesdrop in any place where people have a “reasonable expectation of privacy”—a phrase that even now, four decades later, resonates in the laboratory of Wayne Wolf. An electrical engineer at Princeton University, Wolf leads a research team that is creating a tiny, inexpensive video camera one might glibly describe as a lens glued to a chip. In theory, the camera could be the size of a postage stamp and cost as little as $10, “small and cheap enough to scatter by the dozen,” as Wolf puts it. The laws of optics dictate that tiny lenses make low-resolution images, so the researchers

are developing software that melds video from multiple cameras located in a single area, producing sharp, real-time images of the entire space. "You could stick them up all over a building and know *exactly* what was going on inside," Wolf says. "A lot of people would find a use for that."

These networks of tiny cameras—and the host of other surveillance technologies that are now being unveiled—are both tributes to innovation and, as Wolf acknowledges, potential menaces to personal privacy. Indeed, the new marriage of ever smaller lenses and sensors, ever larger databases, and ever faster computers is making surveillance so cheap and commonplace that it is on the way to creating a state of nearly universal surveillance (see "Surveillance Nation—Part One," TR April 2003).

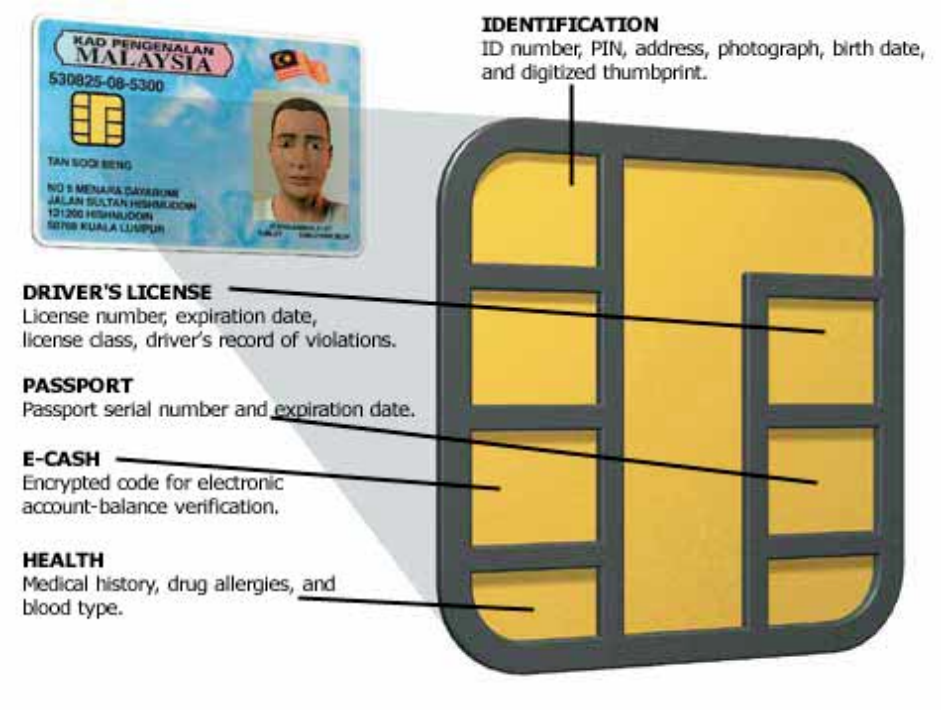
In the past, government agencies and businesses have been blamed for the deployment of surveillance technology—and not without reason. In a single three-week period earlier this year, the Bush administration announced that it was building a system that pools real-time traffic data from Internet service providers and monitors threats to the global information network; inaugurated the Terrorist Threat Integration Center, a vast data bank that will combine domestic and foreign intelligence on U.S. citizens and foreign visitors; and opened up the State Department's database of 50 million visa applications to U.S. police departments. Meanwhile the mayor of London, England, launched a traffic control program that records the license plates of every vehicle entering the city center—and furnishes the information to intelligence agencies.

Such plans have met with scant citizen resistance—understandable, perhaps, given that these same citizens are installing nanny- and pet-watching cameras, flocking to automated highway-toll collection systems (which reduce lines as they record every car that passes through their gates), and scoping out prospective dates, friends, and employees using such Internet search engines as Google. Between 2000 and 2005, according to market research firm Frost and Sullivan, sales of digital video surveillance cameras will increase by a factor of 10. More and more of these cameras are being purchased by private associations, small businesses, and—most startling—consumers. CCS International, a surveillance products company in New Rochelle, NY, estimates that ordinary Americans are buying surveillance devices, many of dubious legality, at a clip of $6 million a *day*. We have met the enemy of our privacy, and it is us.

Although this technology is growing much faster than is generally recognized, its advance is neither inexorable nor uncontrollable. It will be constrained by the structure of the huge databases necessary to store and manipulate surveillance data—and by the cultural and legal environment in which those databases arise. In fact, the way databases are configured may help foster accountability and usage policies that could regulate the deployment of surveillance. Whether these tools are actually used, though, will depend on what citizens want and believe. In the United States, the rise of ubiquitous surveillance will be governed largely by the answer to the question first raised in the long-ago case of Charles Katz: What is a "reasonable expectation of privacy," anyway?

A Smart Way to Protect Privacy

As this conceptual illustration shows, personal data on Malaysia's smart card chips—designed to replace driver's licenses—are stored in isolated files, each accessible only to authorized readers.



AT A BAR
Bartender can check date of birth without seeing patron's name or address.

AT A TRAFFIC STOP
Police can check name and date of birth. If PIN or thumbprint is provided, other data are unlocked.

AT A TICKET COUNTER
Agent can check passport number; during periods of high alert, traveler's thumbprint is required.

Taming the Data Tsunami

One of the claimants to the title of the world's largest database sits on the edge of the Stanford University campus, connected to a three-kilometer-long particle accelerator. Housing records of the millions upon millions of elementary-particle interactions that occur in the accelerator, the BaBar database, as it is known, contains more than 680 terabytes of information—equivalent to a stack of copies of the Bill of Rights some 21,000 kilometers high. (A terabyte is 10^{12} bytes.) From a data-gathering viewpoint, the Stanford experiment is a nightmare. The accelerator smashes electrons and positrons into each other at almost the speed of light, creating an explosion of data in a few trillionths of a second—vastly more input than any computer network can handle. To make sense of these overwhelming infobursts, BaBar engineers have developed a variety of techniques for containing the flow of data. These techniques will almost certainly be used by the enormous surveillance archives of tomorrow, suggesting both how they will function and how—just possibly—they might be regulated for the public good.

Rather than trying to absorb the entire river of readings from the particle collisions, the sensors in the

BaBar particle detector record just a few specific aspects of selected events, discarding millions of data points for every one kept. That small sip of raw data—about a gigabyte every few minutes of running time—is still too much for physicists to study, says Jacek Becla, the lead designer of the database. To further distill the observations, the detector's software intensively "preprocesses" the selected measurements, reducing each to a relative handful of carefully checked, easily manipulable numbers before incorporating them into the database.

Even after preprocessing, a data set can still be too big to examine efficiently in a single central locality. As a result, large databases often divide their work into smaller pieces and distribute the resulting tasks among hundreds or thousands of machines around a network. Many of these techniques were first implemented on a large scale by SETI@Home, a massively distributed system that hunts for alien civilizations. SETI@Home takes in radio telescope readings, breaks the data into chunks, and uses the Internet to dole them out to the home computers of more than four million volunteers. When these computers are otherwise idle, they run a screensaver-like program that probes the data for signs of sentient life.

As the extraordinary measures taken by BaBar and SETI@Home suggest, large databases face inherent problems. Simply running the routine comparisons that are intrinsic to databases takes much longer as data become more complex, says Piotr Indyk, a database researcher at MIT. Worse, he says, the results are often useless: as the data pool swells, the number of chance correlations rises even faster, flooding meaningful answers in a tsunami of logically valid but utterly useless solutions. Without preprocessing and distributed computing, the surveillance databases of tomorrow will drown in their own input.

It is, perhaps, unexpected that both preprocessing and distributed computing also exemplify ways the structure of databases might provide levers to control their use—if people want them. For privacy advocates, surveillance raises two critical issues: lack of accountability and the specter of information collected for a benign purpose being used for another, perhaps sinister, end. "Time and time again, people have misused this kind of data," says Peter G. Neumann, a computer scientist at SRI, a nonprofit research organization in Menlo Park, CA. To discover when users have overstepped or abused their privileges, he says, "accountability as to who is accessing what, altering what data, not updating stuff that should have been corrected, et cetera, is absolutely vital."

Such monitoring is already standard operating procedure in many large databases. SETI@Home, for instance, tracks exactly which of its millions of member computers is examining which datum—not least because the system, according to Berkeley computer scientist David Anderson, its designer, sends dummy data to users during the 10 to 15 percent of the time it is down, and therefore needs to monitor what is real. Nonetheless, Neumann says, most commercial database programs don't securely record the usage data they collect. With off-the-shelf database software from Oracle, IBM, and Microsoft, he says, "there is no way" that such large surveillance databases as the Terrorist Threat Integration Center "could get accountability in any meaningful sense." The software simply allows for too many "trusted users"—people who have full access to the system and can modify audit trails, thus deleting their tracks from the logs. The possibility of meaningful accountability does exist—but people must demand it.

Similar logic applies to the fear that data collected for one purpose will be misused for another. Consider, for example, the program in London, England, that levies a £5 ($8) "congestion charge" on each vehicle crossing into the central city. To enforce collection, the city uses hundreds of digital video cameras and character recognition software to read the license plate of every vehicle crossing into the fee area. Plate numbers are matched against the list of drivers who have paid up; noncompliant vehicle owners

receive summonses in the mail. Just before the program's launch, newspapers revealed that the images would be given to police and military databases, which will use face recognition software to scan for criminals and terrorists—an example of what privacy activists decry as "feature creep." Observes Marc Rotenberg, executive director of the Electronic Privacy Information Center in Washington, DC, "They say they're taking your picture to stop traffic jams. Then all of a sudden they're trying to find out if you're a terrorist."

As all this suggests, repurposing surveillance information is subject to so many pitfalls that "we need to build restrictions on the way data are used," says Lawrence Lessig, a Stanford University law professor who is the author of *Code and Other Laws of Cyberspace*. Ideally, in Lessig's view, "you'd want to have a situation like what goes on with credit reports—we can see them, and know something about who is using them and why, and potentially remove any errors."

The technology to provide such protections is already emerging. The Malaysian government is rolling out a multifunction smart card with 32 kilobytes of memory that can store up to seven types of data, including details about a person's identity, driver's license, bank account, and immigration status. Embedded software encrypts and compartmentalizes the information and keys it to the cardholder's biometric data, ensuring that when an authorized government or business official accesses one type of data, the other types remain off-limits (*see "A Smart Way to Protect Privacy," p. 1*). If introduced into the United States, such cards could be set to tell bartenders that their bearers "are over 21 and can drink alcohol; but that's all," explains Lessig. "And if a police officer stops you, the card should only tell her that you have a valid driver's license"—and not, say, your Social Security number.

The same kinds of access controls should be applied to large, centralized databases, Lessig believes. Users logging onto a sensitive database should have to identify themselves, and their access should be restricted solely to data they are authorized to examine. To further deter misuse, the database should preserve a record of its users and their actions. Such precautions are not only technically feasible but, to Lessig's way of thinking, simply good policy. Still, he sees "next to no chance" that such precautions will be implemented, because terrorist attacks have changed the government's attitude toward privacy and because ordinary people have demonstrated their willingness to embrace the technology without understanding the consequences.

Illustration by Brian Stauffer.

The Golden Rule of Surveillance

Just hours after the first bombs fell on Afghanistan in October 2001, the Arabic television network Al-Jazeera broadcast a grainy videotape that showed Osama bin Laden reveling in the destruction of the World Trade Center. Partly because of the timing of the tape's release, the Internet was quickly filled with speculations that the tape and others that followed were counterfeited by bin Laden's confederates or the U.S. government. After all, video is easy to fake, isn't it?

Nonsense, says Steve Sullivan, R&D director for Industrial Light and Magic, the well-known digital-effects company. Such spoofing, he says, "is simply not possible with any techniques I'm aware of." Even for modest video quality, today's computational power and rendering skills fall far short of what would be required to model a human realistically enough to fool viewers. "You could hire an actor to impersonate [bin Laden], I suppose," Sullivan says. "Basically, though, when you see surveillance video, it's real."

Nonetheless, the impulse toward suspicion is fundamentally correct. Video may not yet

be easily spoofed, but most other forms of digital data—spreadsheets, documents, and records of all types—are easy to alter subtly. "Sheer size and complexity are your enemy," says Bruce Schneier, chief technical officer for Counterpane Internet Security, in Cupertino, CA. "The vast majority of data stored or used by computers are never seen by people. Answers are assumed to be correct, but the integrity of every part of the system is nearly impossible to verify." In other words, even if original surveillance data are correctly observed and entered—far from a foregone conclusion—the deductions made by databases using such information must be treated with care.

Without safeguards, the security problems of large surveillance databases could quickly get out of hand. "It's like Willie Sutton," says Herbert Edelstein, president of Two Crows, a database consulting firm in Potomac, MD. "He said he broke into banks because that's where the money was. Well, identity thieves will try to break into large databases of personal information because that's where the identity data are." For similar reasons, any government database compiled for hunting criminals and terrorists will be irresistibly attractive to its own targets.

Unfortunately, computers are notoriously hard to secure, and this difficulty increases as they grow more numerous, complex, and heavily used. People were sharply reminded of this vulnerability on January 25, when the Slammer worm hit the Internet. (A worm is a malicious computer program that hijacks one computer after another, forcing each compromised machine to send out more identical worms.) Within 10 minutes of its appearance, Slammer had infected some 75,000 computers, many of them critically important to business. Alas, Slammer was not unique: almost every major site—from the *New York Times* to the CIA and FBI—has been cracked at one time or another. On the basis of a General Accounting Office analysis last year, Congressman Stephen Horn (R-CA) issued failing grades to 14 of the 24 major federal agencies on his annual "computer security report card" for Uncle Sam. Given such dismal statistics, operators of government, corporate, and other databases must assume their networks will be periodically compromised, and they should plan accordingly.

Yet this inescapable lack of trustworthiness—perhaps surprisingly—is not all bad. Indeed, the very need to be constantly suspicious of the integrity of large databases is a powerful argument for the accountability measures that would mitigate their impact on privacy.

Stringent monitoring of database usage and public access to those records constitute what might be dubbed the Golden Rule of Surveillance. "If the police can track us as we go about our daily routine, we need to be able to see the police as they go about theirs," says Carl S. Kaplan, a New York City appellate lawyer and former *New York Times* columnist on Internet law. (*Kaplan conducted TR's Point of Impact interview in this issue. See "Curbing Peer-to-Peer Piracy,"*) In his view, surveillance databases will be less prone to misuse if the same rules apply to everyone. "It's a fact of life that some police officers lie," he says. "Equal access would either make it a lot harder for them to lie or make them a lot more careful about what surveillance they use."

The Electronic Panopticon

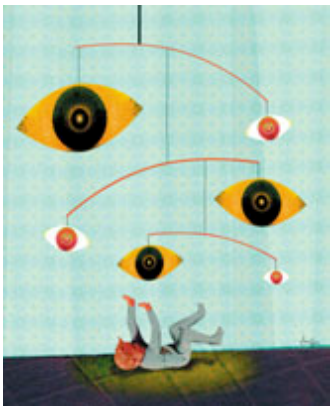


Illustration by Brian Stauffer.

In 1791 the British philosopher Jeremy Bentham envisioned a "panopticon," a domelike prison where guards could observe all the inmates at all times from within a central observation tower. Bentham never managed to convince the Crown to build his prison, but its principles were embraced across the Atlantic, in Philadelphia's Eastern State Penitentiary. Built in 1829, this radical building became a global sensation—the most influential prison ever built, according to Max Page, an architectural historian at the University of Massachusetts, Amherst.

In the Philadelphia panopticon, prisoners lived in solitary confinement in seven cellblocks that radiated like the spokes of a wheel from an observation room. The inmates could see neither the guards watching them nor the other prisoners around them; their only window was a skylight. Living in isolation under the scrutiny of invisible authorities, inmates were supposed to reflect on their sins and become penitent: Eastern State was the world's first "penitentiary."

After Eastern State was unveiled, governments around the world built more than 300 panopticon prisons. But they gradually fell out of use, partly because neither wardens nor inmates could bear playing their roles. According to Dutch architect Rem Koolhaas's study of panopticons, prisoners found ways to avoid surveillance; guards, disheartened by the lack of interaction, left the center. Ultimately, inmates and guards found themselves continuously watching each other, transforming the prison, in Koolhaas's phrase, into "a transparent space" where "no action or inaction remains unnoticed."

Similarly, omnipresent electronic surveillance leads to what Carl Botan, a researcher at Purdue University's Center for Education and Research in Information Assurance and Security, calls panoptic effects—unexpected reactions that counter the purpose of monitoring. According to the American Management Association, nearly 80 percent of major U.S. companies electronically monitor their employees. Common observational methods include logging telephone calls and e-mail to determine which employees are wasting time and periodically recording what is on workers' computer screens to inhibit porn perusing. Such innovations, Botan says, do help employers encourage efficiency and avoid "hostile environment" litigation. But there are other, unintended results. "Employees who know everything is being logged," he says, "are less willing to exchange information with other employees—the horizontal communication that is the problem-solving communication in the workplace. Not wanting to be recorded calling home to monitor how a sick kid is doing, they'll take a sick day instead." If people aren't comfortable with a surveillance regime, Botan argues, they subvert it, exacerbating the problem surveillance was supposed to ameliorate.

Panoptic effects take hold in the larger society as surveillance spreads, says Jeffrey Smith, a lawyer at Arnold and Porter in Washington, DC, who was general counsel to the Central Intelligence Agency. "The notion of what is private and what the limits of privacy are clearly changes to reflect technology," he says. "If what was once thought of as public data can be used to construct what might be an intrusively detailed picture of your life, people will push back. The courts will visit this issue. There will be legislation too."

Much as last year's accounting scandals led Congress to push for corporate reforms, legislatures could demand that organizations that maintain databases of personal information keep detailed publicly available records of their use. But that will not happen without a shift in public opinion. "A lot of law turns on 'reasonable expectation of privacy,'" says Paul Schwartz, a privacy law specialist at Brooklyn Law School. "But as technology becomes cheaper and surveillance spreads everywhere, the danger is that the

reasonable expectation of privacy will change." If Americans grow accustomed to a lack of privacy, in other words, they will get exactly what they expect.

"This technology could do a lot of good and a lot of harm," says Shari Pfleeger, a computer scientist and senior researcher at the RAND think tank in Washington, DC. "But to get the balance right, it needs to be actively talked about." More often than is commonly realized, such public discussion—nudged along by legal action and ongoing public-awareness campaigns—has transformed prevailing notions of acceptable behavior. Examples include the dramatic turnabouts over the past two decades in attitudes toward smoking and drunk driving, both of which were driven in part by grass-roots activism. The rapidity of the advances in surveillance technology, unfortunately, means that society has much less time to confront the trade-offs between security and privacy. The moment for debate and conversation is now, while the technology is still in its adolescence.

Watching What You Do		
TECHNOLOGY	**DESCRIPTION**	**SELECTED PROVIDERS**
AT HOME		
"Nanny cams"	Small, easily hidden wireless digital video cameras for monitoring children and pets.	**Nanny Check**, Plainview, NY **Know Your Nanny**, North Brunswick, NJ
Infrared surveillance	Technology that alerts police to such suspicious thermal activity inside houses as the heat from marijuana-growing equipment.	**Monroe Infrared Technology**, Kennebunk, ME **Sierra Pacific**, Las Vegas, NV
ON THE ROAD		
Traffic cameras	Web cameras mounted at high-traffic points; specialized cameras that read plate numbers for law enforcement.	**Axis Communications**, Lund, Sweden **Computer Recognition Systems**, Cambridge, MA
Automobile transponders	Electronic toll deduction when users pass through tollgates; supported by laser vehicle measurement and axle number detection.	**Mark IV Industries**, Sölvesborg, Sweden **SAMSys Technologies**, Richmond Hill, Ontario
Cell phones	Technology that reports a cell phone user's precise location to authorities during 911 calls.	Mandatory for all U.S. wireless carriers and cell phone manufacturers by 2006
AT WORK		
Internet and e-mail monitoring	Text and data filters that ensure compliance with privacy and harassment laws and corporate confidentiality requirements.	**Tumbleweed Communications**, Redwood City, CA Clearswift, Theale, UK
Keystroke logging, file usage review	Systems that record everything typed into a computer, including e-mail, instant messages, and Web addresses.	**Amecisco**, San Francisco, CA **NetHunter Group**, Tallinn, Estonia

AT SCHOOL		
Web filtering	Software that prevents students from reaching inappropriate Web content.	**N2H2**, Seattle, WA **iTech**, Racine, WI
Locator wristbands	Bracelets that combine GPS and digital cell-phone signals to locate wearer within 30 meters.	**Wherify Wireless**, Redwood Shores, CA **Peace of Mind at Light Speed**, Westport, CT
AT THE STORE		
Smart cards	Microchips embedded in plastic cards that carry e-cash, along with driver's license, age and address information, and medical records.	**Gemplus**, Luxembourg **Oberthur Card Systems**, Paris, France
Supermarket discount cards	Cards—with embedded chips or standard magnetic stripe—that earn member discounts and track shopping habits.	**Catalina Marketing**, St. Petersburg, FL **SchlumbergerSema**, New York, NY

Dan Farmer is a software engineer and computer security expert. Charles C. Mann has written for *Technology Review* about the free software movement (January/February 1999) and the use of genetic engineering in agriculture (July/August 1999).