
JEFF GRUNEWALD

Ubiquitous sensors and massive interlinked databases are propelling us into the post-Orwellian era. Are we ready to know everything about each other?

BY HARRY GOLDSTEIN

WE LIKE TO WATCH

WEBCAMS TODAY CAN TAKE YOU to the intersection of 34th St. and Broadway in New York City, to a checkpoint at the Finnish-Russian border or, for that matter, to the shower stall of a pert college girl making a fast buck from fee-paying voyeurs. But, with the advent of better search tools, more-comprehensive public databases, and pervasive sensors, we're moving beyond monitoring pedestrian activities and indulging prurient cravings. Soon we'll be able to tap into the life of anyone we encounter with a simple query, knowing all the while that our lives are exposed to the same scrutiny.

Technology's inexorable advance has brought the world's democracies to a crucial juncture: will next-generation citizens keep an eye on each other in a golden "age of transparency," as famously imagined by science fiction writer Arthur C. Clarke in his 1988 novel, *2061: Odyssey Three*? Or will the tools of surveillance and data analysis be wielded exclusively and with impunity by governments and corporations?

This much we do know: a combination of political, cultural, and economic factors are transforming our world into a place where people, transactions, and things can be observed, monitored, and recorded almost everywhere, and almost all the time. Within the next several years, we'll be awash in powerful, cheap sensors: radio-frequency ID (RFID) tags that track objects (and the people who happen to be wearing, riding, or chatting into them); biometric sensors that will identify us by our unique irises, fingerprints, voices, walking patterns, or other physical quirks; Global Positioning System receivers, embedded into all manner of things, able to track us to within a meter; and tiny, high-resolution digital still and video cameras, also built into everything, from cellphones to wallpaper.

The resulting torrent of data will cascade into government and corporate data systems, as well as that system of systems, the Internet. Facts and information that are largely incoherent but overwhelming in volume and detail will accumulate in databases too scattered and numerous—and valuable—to be shut off completely from the rest of cyberspace.

Without a doubt, though, we'll try to do just that. In fact, we've already started. Researchers, mostly in academia, are now working on various privacy-enhancing technologies [see "Sensors & Sensibility" elsewhere in this issue]. But champions of a transparent society, where the light of accountability would shine upon all of us, contend that over the longer term these privacy enhancers will be like sandbag walls against that relentlessly rising tide of data. They'll keep little areas "dry" for a while, and give some of us a measure of comfort, but will fail to shield us in any absolute, permanent, or globally

GUARDIAN ANGELS: British police officers in the control room at New Scotland Yard in London watch over monitors showing closed-circuit TV images and newscasts during a state visit by U.S. President George W. Bush in November 2003.

effective way. We must embrace the technologies of surveillance, these advocates contend, and in doing so, ensure that we can point the electronic eye right back at the people and institutions who watch us.

This viewpoint—articulated most comprehensively by science fiction novelist David Brin in his 1998 treatise, *The Transparent Society*—runs contrary to the opinions many of us hold about privacy. At the other end of the privacy spectrum, activist groups such as the American Civil Liberties Union and the Electronic Privacy Information Center seem to see ominous portents in every new sensor advance and federal initiative. Each side is grappling with the continuing evolution in seeing and knowing that has been remaking society for centuries.

Our history since the Renaissance has been an endless quest to extend our ability to see and remember. Beginning with microscopes and moveable type, speeding up with photography and public libraries, and accelerating with television, the personal computer, and perhaps most important of all, the Internet, each advance set off waves of technical innovation, individual productivity, and artistic expression. At the same time, these inventions forced us to reexamine and revamp our economies, political institutions, and ethics in light of our increasing power to acquire, analyze, and act on data about ourselves and the world we were making.

The next step—of distributed sensing and rapid data analysis and dissemination—will certainly up the ante in just about every conceivable way. But it needn't lead inevitably to Big Brother–style repression. Brin and like-minded thinkers, such as those who post their opinions at Universaltransparency.org, argue that so long as we the people own most of the eyes, we will be able to debate privacy issues knowledgeably among ourselves, with the aim of shaping public policy for the collective good. It is a monopoly of vision that we need to fear, say the transparency advocates, not vision itself.

GETTING TO TOMORROW'S FISHBOWL WORLD— where we swim in perpetually refreshed pools of information about ourselves and one another—will take time. Today, every new monitoring or data-gathering initiative launched by governments or corporations prompts dire warnings from activist groups about how we're heading straight toward Orwell's terrifying dystopia.

One of the hottest of hot-button issues, for now at least, is public surveillance cameras. They're popping up all over Singapore, Russia, and Great Britain, which now has an estimated four million police video cameras on public streets, up from fewer than 150 000 just 10 years ago [see photo, "Guardian Angels"]. In comparison, the spread of video cameras aimed at U.S. citizens has been almost inconspicuous because most of the cameras are owned and operated by individuals and companies—banks, stores, building operators, and so on. And unlike their counterparts in Great Britain, U.S. law enforcement officials rely heavily on these privately owned security monitors. The Oklahoma City bomber and the Washington, D.C., snipers were caught partly because of video footage obtained from unofficial sources.

Nevertheless, privacy advocates regularly portray the rise in video surveillance darkly, predicting that it is eliminating our privacy and undermining our values. They're right about the loss of privacy, of course. But balancing that imposition are the ways in which the new technologies can be used to promote our values even as they protect us. For example, it has been 13 years since an amateur videographer taped Los Angeles cops beating the daylights out of motorist Rodney King in 1991. Since then, countless other pieces of video have been used to solve crimes, expose government abuses, and promote democratic revolutions from Russia to the Philippines.

The latest, most dramatic example was the debacle in the Abu Ghraib prison in Iraq. The grisly details of prisoner maltreatment there became a matter of public record, or at least many of them did, just months after most of the abuses occurred.

KIRSTY WIGGLESWORTH

Never before has a program of prisoner abuse been so minutely detailed. The difference this time was the existence of digital cameras and an easy way of distributing their images. Many of the cameras were operated by the soldier-jailers themselves, some of whom could not stop themselves from sharing snapshots of their twisted escapades with friends via e-mail.

The pictures' subsequent exposure on network television and in print—and near-instantaneous global distribution on the Internet—turned the tables on the jailers, and prompted people to start asking tough questions about policy decisions and implementation throughout the U.S. military's chain of command. It was a textbook example of what usually happens when you have scattered sensors and a facile, fast means of spreading their output—enough of the data gets out to start the wheels of justice turning.

PUBLIC VIDEO MONITORING ISN'T ALL that bothers privacy activists. At least as disturbing to them are federal programs aimed at expanding government monitoring and data collection.

In the United States, various agencies have been hard at work writing highly sophisticated programs that sift through databases or sample the flood of e-mail traffic passing through Internet hubs, searching for word patterns and other cues that might help detect threats to national interests. When the media spotlight fell on a few of these agencies, they didn't end their efforts; typically, they became more secretive.

Take the FBI's Omnivore system, which came to light in 2000. Assailed as a giant wiretap on the Internet, it allows the FBI to monitor traffic going to and from Internet service providers. Despite pressure from unlikely allies like then Representative Bob Barr (R-Ga.) and the ACLU, Omnivore continued on, first under the name Carnivore, and now with the Newspeak moniker of the Digital Collection System Network. It allows FBI agents to snoop on Internet communications that are the subject of "a lawful order."

Then there is the case of the Total Information Awareness program. TIA began in January 2002 as a U.S. Department of Defense research program charged with developing cutting-edge information technologies to help detect terrorist activities. The initiatives included 18 data-mining projects, some aimed at developing tools capable of sifting through petabytes (thousands of millions of millions of bytes) of data at a time. Substantial descriptions of these research projects were posted on TIA's Web site. And the more people knew about what was being funded, the louder the calls were for the U.S. Congress to cut TIA funding.

All this public outrage has accomplished two ironic things. First, it has driven many of the TIA undertakings and others like them into darker corners of the U.S. government, further from any kind of oversight. Second, it has caused the loss of funding for two TIA programs that would have created counterbalancing privacy-enhancing software: Genysis Privacy Protection, which was to develop "privacy appliances" to filter out personal information from data flowing into and out of a database, and the privacy portion of the Bio-ALIRT project, which aimed to monitor the symptoms of patients (whose names were to be concealed) at emergency rooms and doctors' offices for signs of a biological attack.

Congress terminated many other TIA projects, but much of the research, including some of the data-mining work, was dispersed to other departments. Similar efforts at another obscure intelligence and counterintelligence skunk works—the Advanced Research and Development Activity, which is overseen by the ultrasecretive National Security Agency—continue to receive tens of millions of dollars.

If we can't keep the government from collecting and analyzing data about us, can we at least force it to keep that information locked up? We can try, but we probably won't succeed—at least, not completely. There's no such thing as a hermetically sealed database, conceived and implemented as these things are by imperfect human beings employed by companies and government entities—which, driven by profit motives or policy directives, will keep developing these technologies with or without our consent.

"Those who think we can protect our anonymity by banning technological development should first try to explain how they hope to succeed at banning anything at all," says Brin. "Elites may let us pass laws to blind ourselves, but they will never allow us to blind them. Banned technologies will—if we insist—be developed in secret." Or as science fiction legend Robert A. Heinlein once put it: "The chief thing accomplished by privacy laws is to make the bugs smaller."

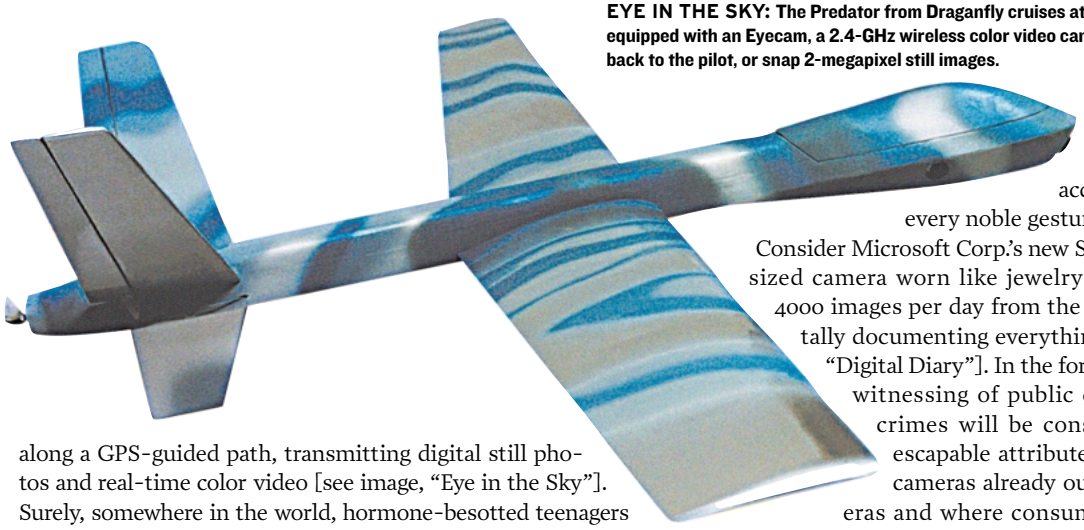
DIGITAL DIARY: Dubbed by one researcher "a black box recorder for the human body," the Microsoft SenseCam's shutter is triggered by changes in motion, light, or temperature detected by sensors embedded in the device.

MICROSOFT

ANOTHER LAW, MOORE'S LAW, ensures that the bugs will get smaller, no matter the political climate. So to fully grasp the implications of the coming sensor revolution, you've got to go beyond the usual sensor suspects—the RFID tags, the biometric sensors, and so on. They're significant, but they're just the first, crude wave of what's coming: sophisticated sensors that could empower citizens at the grass-roots level to keep a wary, high-res eye on governments, corporations, and, of course, each other.

Count on military technologies to keep spinning off commercial versions. It has already happened for night-vision systems and electronic compasses. Next up are devices that warn of chemical or biological dangers. Within five years or so, mass-produced sensors will find their way into our neighborhoods, wetlands, parks, and houses, where everything from appliances to security systems will wirelessly communicate their conditions to you via IEEE 802.15.4, the new ZigBee standard for home automation and control sensors. Neighborhood or activist groups that create sensor networks to monitor, say, groundwater quality will have access to data about pollutants and other toxins rivaling that of local governments.

The same military spinoff effect has already transformed unmanned battlefield reconnaissance drones into inexpensive but powerful civilian toys. For US $750, you can now buy a radio-controlled airplane called the Predator from Draganfly Innovations Inc., in Saskatoon, Sask., Canada. With a wingspan just under 2 meters, the drone can cruise independently for more than an hour



EYE IN THE SKY: The Predator from Draganfly cruises at a speed of 80 km/h and can be equipped with an Eyecam, a 2.4-GHz wireless color video camera able to transmit real-time video back to the pilot, or snap 2-megapixel still images.

along a GPS-guided path, transmitting digital still photos and real-time color video [see image, "Eye in the Sky"]. Surely, somewhere in the world, hormone-besotted teenagers are already using them to find the skimpiest bikinis on a beach. Homeowners will use them to keep tabs on the neighborhood or reconnoiter fast-moving wildfires.

The question is, should we push for yet another unenforceable law to guard our backyards against Peeping Toms and their drone planes? Or, as Brin has suggested, perhaps we'd be better off simply insisting that the companies that make the little robot spies give us the means to trace them back to their nosy pilots. One enabling technology for that kind of reciprocal transparency is being developed at ETH Zurich, Switzerland, by researcher Marc Langheinrich. His personal digital assistant application detects nearby sensors and then lists what kind of information they're collecting.

"If the sensor is mandatory, like a security camera, at least I know I'm being taped," he explains. "If it's an optional service, like a friend finder for instant messaging, then I can turn the software off or on." The commercial version of the device probably won't look like today's PDA, he says, but will be built into a watch or cellphone.

Just as Langheinrich's invention will shrink in size right in step with Moore's Law, so too will the devices his spy tracker tracks. Cameras will become hugely more effective and ubiquitous when they get to be so small that they are hard to see with the unaided eye. Absolutely nothing in the physics of this technology precludes that kind of miniaturization. At the University of California, Berkeley, researchers such as Kristofer Pister and David Culler, as well as companies like Crossbow Technology Inc., in San Jose, Calif., and Dust Networks, Berkeley, Calif., are already developing technology they call smart dust—cubes of silicon the size of ants' heads that each host a sensor, a processor, and wireless-communications hardware. A decade or so from now, these kinds of devices could well spread vision into every nook and cranny of our world.

As the sensors and sources of data proliferate, so too will our options for accessing their output, digested or otherwise. Foremost among these options will be sensor-studded, wearable multimedia devices—such as displays, already commercially available—that clip onto eyewear or pop down from visors. They will be mated to computational and communications capabilities woven into clothing. They'll overlay your view of the world, whenever you wish, with digitally supplied facts, directions, or commentary, snatched out of the ether by tiny but ferociously fast wireless receivers.

For most of us, the incredible convenience and utility of having instant access to entertainment and information wherever and whenever we want it will trump any self-consciousness about funky-looking eyewear or odd little garment accessories. These same wearables will not only let us access information, they'll acquire it, too, documenting our every noble gesture, promise, or transgression. Consider Microsoft Corp.'s new SenseCam, a prototype badge-sized camera worn like jewelry that automatically records 4000 images per day from the wearer's point of view, digitally documenting everything he or she sees [see photo, "Digital Diary"]. In the foreseeable future, surely cyber-witnessing of public events, business deals, and crimes will be considered routine. It's an inescapable attribute of a world where cellphone cameras already outsell all other types of cameras and where consumers' insatiable demand for small, sleek recording devices of all sorts makes it likely that someday everybody you meet will be wearing a "wire."

IT WILL NOT BE EASY to create a truly transparent society. For most of us, being more accountable, and holding others to account, will be a challenge. But the benefits might well outweigh the costs, as in this scenario, circa 2010:

Passing you on the street, I swipe my RFID reader to obtain your name and address. Googling you on a few public databases, including one of new homeowners in the neighborhood, I discover that you're in the market for a used lawn mower. Your bank account is in order, and your credit is fantastic, even after you paid off your ex-wife's debt as part of your recent divorce settlement. You had a quadruple bypass last year and need a riding mower just like the one sitting in my garage. Your spy tracker alerts you to the fact that I'm checking you out, prompting you to launch your own investigation. You learn I suffer from obsessive-compulsive disorder and am taking medication to keep my life together. But you also know that my disorder manifests as a cleaning fetish; it's a good bet that the lawn mower I listed on eBay is in pristine shape. Furthermore, you can infer that I'm so desperate to make my credit card payments this month that I'll sell you that mower for a song.

Ideas and attitudes about personal privacy differ from culture to culture, era to era. Is it such a stretch to believe that the developed world's collective attitude toward privacy is evolving to a point where we're no longer concerned with who's watching us or what they know about us, as long as our lives are safer and more convenient? After all, we live in a time when we automatically remove our shoes so airport screeners can check for explosives; when we are videotaped every time we conduct an ATM transaction or walk into a store or office building; and when we are tracked every time our computer accepts a cookie from a Web site we've visited.

For entertainment, we gather in front of the tube for mass-mediated group therapy sessions called reality shows. Hundreds of millions of us around the globe tune in to watch people who eagerly endure excruciating plastic surgery; stab each other in the back for a chance to work for Donald Trump; or wolf down sea worms, cockroaches, and worse to survive on a desert island. For Generation Y, "Big Brother" is a reality television show, where, for a chance at winning half a million dollars, contestants volunteer to be cooped up in a house with total strangers and have their most private moments broadcast to a hungry audience.

It's not hard to imagine a near future of reciprocal transparency when all of us are watched and can watch right back. We're halfway there. ■

DRAGANFLY INNOVATIONS