

the *Nation*. I borrowed the last lines of the book from an interview on garbage with the eloquent and generous Dick Walker. My old friend Jan Chelminski kindly helped with the illustrations. Finally, hats off to all the librarians who—more than just providing services and information—preserve an alternative social logic: in a cultural landscape marked by venality, price tags, and egotism, librarians steward oases of generosity, free sharing, and collaboration.

LIFE IN THE GLASS BOX

First thing when I wake up and
 Right before I close my eyes at night
 I think, sense, feel man like
 I'm under some kind of microscope
 Satellites over my head, transmitters in my dollas
 Hawkin', watchin', scopin', jockin'
 Scrutinizin' me, checkin' to see what I'm doin'
 Where I be, who I see, how and where and with whom I make my
 money
 What is this?
 Excuse me Miss
 May I have your phone number and your social security?
 Who me? When all I came to do is buy my double or triple A bat-
 teries?
 Please, I decline

— Jill Scott, "Watching Me"

The future is already here. Over the last three decades the prevalence of routine, everyday surveillance has increased to sci-fi proportions. Thanks to the proliferation of computers, databanks, and networks, once distinct

spaces of knowledge—credit records here, medical records there, criminal records elsewhere—now form a single, coherent informational landscape that is easily mapped and controlled by government and business.¹ Everywhere, one leaves a trail of digital information; all daily tasks—working, driving, shopping, tending to health—now create retrievable records.

Consider this: More than 111 million Americans carry mobile phones, each of which creates a rough electronic account of the user's location in time and space. Cell phones communicate with networks of transmission points that monitor and note a phone's location whenever it is on. These records, stored by phone companies, can be subpoenaed when needed or their aggregate patterns can be "data-mined" for commercial uses. And now, in the age of terror and permanent emergency, the federal government has ordered wireless carriers to create systems for tracking mobile phones in real time. As a result, the latest wireless communications devices often contain built-in Global Positioning System (GPS) chips that transmit the gadget's geographic coordinates to twenty-four Pentagon-maintained satellites, tracking users as they move. The resulting records can be archived, aggregated, disaggregated, and correlated with other information to create a broad overview of group behavior or detailed portraits of individual habits. Thus, a convenience, an Information Age accessory, becomes an electronic tag.²

But...who cares?

Why worry that Sprint has buried deep in its guts the coordinates of your exact location? For most people the new surveillance has no immediate material impact. So let's cut to an extreme situation, a dystopic somewhere else, and consider the question again.

POLITICS OF THE MUNDANE

In the occupied territories of the West Bank cell phones have already become critical components in the war between Israelis and Palestinians. During the first year of the *Al Aqsa* Intifada, the Israeli Defense Forces assassinated at least six Palestinian militants with rockets or helicopter gunships by first locating the target's cell phone and then directing fire at the coordinates of the phone. In those days most Palestinian mobile phones

were jacked into Israel's politically suspect Cellcom network, headed by a former Shin Bet commander, Yakov Perry. After the link between phones and fire from the sky became clear, Palestinians started boycotting the Israeli cellular system and set up Jawwal, a Palestinian/Swedish telecom joint venture.³

From this perspective, routine surveillance takes on a new meaning. With a little imagination one can see that no matter how mundane, surveillance is also always tied up with questions of power and political struggle. And not only in the very direct fashion sketched above, but so too at the level of what Raymond Williams called the "structure of feeling"⁴

Routine digital surveillance is now almost ubiquitous and includes the records produced by credit cards, bankcards, Internet accounts, gym memberships, library cards, health insurance records, and workplace identification badges. All these create electronic files and therefore automatically and inadvertently log our movements, schedules, habits, and political beliefs.⁵ In most respects dull, the contents of such electronic dossiers become rich veins of informational ore to be excavated from any number of angles by marketers, insurance firms, or police officials. One recent FBI investigation "seized enough computer data to nearly fill the Library of Congress twice."⁶

Even before the terrorist attacks of 9/11 the routine surveillance of everyday activity was expanding rapidly. But that assault, so galvanizing and palpable for a previously impervious population, has been hijacked by the worst elements of the political class, who seek to steer fear and anger toward the destruction of traditional American liberties, including what Justice Louis Brandeis called "the right to be let alone."

In many ways, 9/11 was only fuel to a fire already raging out of control. The state's drive to tag, monitor, and criminalize, and the media's compulsion to summon fear at every turn, are matched or surpassed only by the aggressive proliferation of commercially based identification, registration, and tracking. This privatized regime of observation and discipline is crystallized in the inexorable slide toward a cashless cybersociety in which every transaction is recorded and correlated to a subject's location in time and space. In Europe, microchip-integrated "smart cards"—the next logical step toward electronic money—are fast replacing all other types of credit and debt cards. Unlike most ATM or

credit cards used in the US, smart cards not only deposit information but also record and store data—that is, they build and hold their own records. In the UK, the Boots Pharmacy “Advantage Card” has more than 10 million users. The Netherlands, Belgium, and France are awash in smart cards, and 70 million Germans carry them for health insurance identification purposes.⁷ And if we are to credit Moore’s Law, which holds that computer processing capacity doubles every eighteenth months, the power of smart cards could grow exponentially.

What does this mean? According to one journalist: “Experts predict that, over the next decade, consumers will carry two or three smart cards: a work card with access to the company’s canteen, computer network and car park; a leisure card with gym club membership and lunch money; a banking card with details about your mortgage payments and social security status.... The small plastic card in your wallet will probably know a lot more about you and your particular habits than you’d tell your best friend, from the last purchase you made to what you got in your final exams.”⁸ Add to this the next generation of wireless telecommunications gear—souped-up cell phones, web-enabled Palm Pilots, onboard navigation and GPS gear for automobiles. Then imagine their interface with the countless rules, dictums, and prohibitions of overbearing state and corporate governance and one begins to see the contours of something rather unpleasant, a world that is nominally free but actually subject to a soft tyranny of omniscient and interlocking regimes of control: work rules overlapping with the criminal law; overlapping with official moralism; overlapping with the concerns of the security-conscious home; overlapping with notions of “correct” political policies; and then all of this overlapping with problematic assumptions about who is dangerous and who deserves privilege.

The new surveillance—which professor David Lyon calls “dataveillance”—often ignores the physical body and instead tracks one’s informational doppelganger, but this does not mean that more traditional forms of surveillance are in decline.⁹ Quite the opposite: visual and biological monitoring complement high-tech computerized observation. For example, Citgo Petroleum Corp. now drug-tests all job applicants at its 14,500 Citgo-brand gas stations, convenience stores, and Quick Lube outlets with a state-of-the-art, instantaneous saliva-based drug test.¹⁰ Similar tests are becoming common elsewhere.

In New Orleans, at Frederick A. Douglass Public High School—named for America’s most famous runaway slave, who forged false identities, lied to authorities, brawled with his enemies, and became one of the nation’s most ardent and eloquent champions of liberty—students are encouraged to “volunteer” for hair-strand drug tests. Although there have been only a handful of dirty results so far, these chemical inspections, funded by an anonymous donor are wildly popular with the local press. Similar tests are standard practice at private Catholic schools throughout New Orleans.¹¹ Educators in one part of northern New Jersey have taken this logic a step further by subjecting all athletes to random, mandatory tests for drugs, alcohol, and nicotine. Kids with dirty samples are dropped from the teams.¹²

Various types of “biometric” surveillance that identify individuals by measuring the body are also becoming less expensive and more prevalent. Banks in all fifty states now require thumbprints from customers (not too surprising, considering that some banks have been requiring them since the early 1920s). The industry’s biggest trade group, the American Bankers Association, defends the practice for obvious reasons: fingerprinting reduces fraud by an average of 60 percent.¹³ The Bank United of Texas skips the prints, having gone one better by installing Sensar Incorporated “iris scanners” at its ATMs. Staff and some frequent flyers at New York’s Kennedy Airport also submit to iris scans, while Chicago’s Department of Aviation makes truck drivers entering O’Hare swipe an ID card and pass their thumbs over a scanner. Public housing projects in Chicago, Baltimore, Wilmington, Delaware, and St. Paul also use “biometric” hand scanners to control the entrance of residents and guests.¹⁴ Some corporations are equipping themselves with desktop computers containing fingerprint scanners to control network access.¹⁵ Even kids in three Pennsylvania school districts are using digital fingerprint identification in “cash-free” lunchroom transactions: no more schoolyard shakedowns, no more chocolate milk binging.¹⁶

Visual surveillance—the quintessential example being closed-circuit television (CCTV)—is also on the rise. In Manhattan, some 2,400 surveillance cameras keep watch over streets, parks, and doorways. That number is growing all the time as police do their best “to keep up with the demand.”¹⁷ In Minneapolis-St. Paul 80 percent of the highways are under constant watch by more than 250 pole-mounted cameras, as are all the key entry and exit points of most major American cities from San Francisco to

New York.¹⁸ Typically, a major airport now deploys up to a thousand hidden and visible closed-circuit television cameras.¹⁹

All this is child's play compared to the total hegemony of CCTV in the UK, where one million cameras nationwide watch train stations, the foyers of buildings, shops, highways, and the public spaces of every major town center. And CCTV everywhere is set to converge with digitalized biometrics. The technology debuted when Tampa hosted the 2001 Super Bowl. From a crowd of approximately 100,000 sports fans the police computer had nineteen "hits" for people wanted on minor warrants. No arrests were made, in part because the freely loaned equipment and software were seemingly deployed to generate press hype for the system's manufacturer. But some European cities, along with various US government office buildings and more than a hundred casinos, use similar biometric programs for scanning their surveillance footage.²⁰

Perhaps the wackiest examples of this paranoid techno-fetishism are the 2.5 million American pets that have been implanted with microchip identification tags. If a lost pet is found, its ID info can be read with a simple handheld scanner that your local pound may or may not have. The same technology—in the form of a microchip bracelet—is already being used to tend Alzheimer's patients and small children.²¹ And, yes, a family in Florida recently had themselves implanted with ID chips containing medical and biographical information. They also bought stock in the chip-making firm just before announcing their stunt to an eager, fear-crazed national press corps.²² The paranoid imagination of yesterday—animals and humans with chips in them—is already passé, or at least kitsch.

Meanwhile, 75,000 Americans live under house arrest, their ankles shackled with high-tech electronic manacles tethering them to distant police computers.²³ The FBI predicts that its wiretapping activities will increase by 300 percent between 2000 and 2010. And the National Security Agency's ECHELON program monitors most international phone calls emanating from the United States, searching them automatically for key words like "semtex" and "president."²⁴

The list could go on and on, spiraling up into the thin altitudes of political psychosis without ever leaving the realm of fact. But what are we to make of all this? And why should we care?

The point is not that any one of these examples taken in isolation is so awful, but rather that they all exist in relation to each other and should be

considered as such. Each new type of surveillance forms part of an emerging, society-wide system. In other words, everyday surveillance is troubling in the same way as advertising: it is not that this or that ad is so oppressive, but a whole landscape and culture of commercialism most certainly is.

IS PRIVACY ENOUGH?

The tides of popular culture bring signs that Americans have embraced their loss of privacy with patriotic vigor and pop-culture nonchalance. Opinion polls show approval ratings of 60 to 80 percent for expanding CCTV in public spaces, while webcam exhibitionism and mass online voyeurism are hugely popular. In New York alone, thousands of vigilant parents have installed "nanny cams" bought from ParentWatch to keep remote tabs on their little darlings.²⁵ Simultaneously, we have new forms of surveillance-based television: the show *Big Brother* casts a group of regular non-actors living together in a house that is completely exposed by cameras; their challenge is to create a life worth watching while on occasion hiding from the audience. These surveillance-as-challenge, "reality"-based shows anesthetize us to the new superintendence and in so doing treat it as another natural element, like heat or cold, with which we must live and against which we test our wits.²⁶ This reification of a political technology is just one barometer of our increasing habituation to the age of surveillance.

Against the cameras, IDs, and swipe cards arises the cry of *privacy*. But too often this is cast as ipso facto valuable. We are rarely told *why* we should care about privacy: its importance is simply asserted. And when its value is explained, privacy is usually cast as an individual "quality of life" issue, as if being spied on is unpleasant in the same way as loud noises, litter, or offensive language. The best example of this logic comes from the eloquent and forward-thinking Louis Brandeis himself.

A life-long progressive and the first Jew to enter the Wasp bastion of the Supreme Court, Brandeis wrote a famous dissenting opinion in the case of *Olmstead v. United States*, which allowed the police to secretly tap telephones. The core of Brandeis's argument is framed in forthrightly individualistic terms:

The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings, and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights, and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.²⁷

One can concur completely with Brandeis and still want something more, an argument that, in conjunction with Brandeis's superb defense of our spiritual nature, feelings, intellect, beliefs, thoughts, emotions and sensations, raises the stakes by making privacy a more social and political issue.

There is a pragmatic political reason for this as well: privacy as a purely individual issue has limited resonance. Many citizens of Tampa welcomed the new CCTV cameras, and most simply didn't care either way. Likewise, very few AOL subscribers protest the company's ready cooperation with law enforcement.²⁸ The logic of such passivity is simple: if you don't have anything to hide, why be concerned? This commonsense argument is rarely engaged because it is, in fact, quite hard to counter at the level of everyday experience.

The rest of this book, through historical narrative and description, seeks to complicate and repoliticize the question of privacy. Here "the right to be let alone" and the value of personal autonomy are not assumed a priori, nor addressed simply at the level of the individual. Instead, I explore the problem of surveillance through its connections to the larger social issues of inequality, violence, state power, and collective political action.

POWER AND KNOWLEDGE

Brandeis's dissent in *Olmstead* was by no means the last word on surveillance. In fact, the whole debate underwent a massive transformation with the intervention of Michel Foucault beginning in the mid-1960s. The curious and

concerned have been examining the pieces from his demolition job ever since. In Foucault's wake we see that routine surveillance is clearly bound up with political repression, but that it *also* has a "generative" function, helping to elicit and construct politically useful forms of knowledge and behavior.

In short, surveillance instills discipline by forcing self-regulation. Constant surveillance brings forth loyal citizens, trained soldiers, obedient patients, productive workers, and docile, useful bodies. External observation recruits us to monitor and police ourselves: we confess, count calories, open our doors to the Census long form, sign our *real* names on hotel registers, pay our taxes, reel off our Social Security numbers and dates of birth. The entire edifice of modern life is built as much upon the primacy of files, record keeping, and everyday surveillance as it is upon nature and labor.²⁹

It is also clear that the knowledge produced by formal observation can justify a wide range of interventions from the intrusive but well-meaning to outright persecution and physical punishment. Once identified and understood, the deviant can be helped, redirected, segregated, imprisoned, or destroyed by doctors, psychiatrists, superintendents, social workers, managers, or police agents.

Foucault's epistemologically relativist argument holds that moral and cultural categories like "madness" or "criminality" are not simply "discovered" and accurately named by science so much as they are *built* by the political and scientific practice and discourses. This is not to say that madness is "unreal," but rather that its reality and cultural meaning are always socially constructed. In other words, whatever biology madness involves, it is also always bound up with, and never appears outside of, the matrix of culture and historically specific forms of knowledge. Hearing voices in one society may be seen as religious insight, while in another it becomes reason for institutionalization. Surveillance thus serves as a "generative" force, one that defines who is an insider and who is an outsider.

FROM THE THEATER OF ATROCITY

For Foucault, the politics of surveillance were bound up with the emergence of modern methods of medicine, psychiatry, and statecraft. He sketched this point most famously by contrasting a quintessential image of

premodern power, the spectacular ritual of public torture in the *ancien régime*, with the cold precision of modern power in the form of a youth reformatory.

It begins in the first pages of *Discipline and Punish* with a harrowing, archival account of the long, slow death of Robert François Damiens, who had attempted to stab Louis XV in 1757. The court's instructions were detailed: "The flesh will be torn from his breasts, arms, thighs and calves with red hot pincers, his right hand. . . burnt with sulphur, and on those places where the flesh will be torn away, poured molten lead, boiling oil, burning resin, wax and sulphur melted together and then his body drawn and quartered by four horses."³⁰ According to Foucault: "Power in this instance was essentially a right of seizure: of things, time, bodies, and ultimately life itself; it culminated in the privilege to seize hold of life in order to surpass it."³¹ This type of public execution may seem like a fairly definitive expression of state force, but Foucault argued that it was also wasteful, and dangerously inefficient. Public torture and execution relied heavily on the role of the crowd for its ceremonial and symbolic impact. Such events were political theater and "the people" were its audience. But to some extent this public ceremony distributed power to the spectators, who in turn might choose to rewrite the intended script in very disruptive ways. The crowds at public executions sometimes rebelled, attacking the scaffold to free or kill the prisoner, and in other ways acted to negate or usurp the power of the king. To avoid such political meltdowns, execution and punishment became increasingly invisible, professionalized, and restrained.

DISCIPLINE AND SURVEILLANCE

Foucault's account of classical brutality—the display of "sovereign power"—contrasts strongly with an example of "disciplinary power" from the late 1830s, less than a century after the brutal public execution of Damiens. From the gallows we cut to the super-regimented daily timetable from the "House of young prisoners in Paris"—a classic reform school. The schedule begins rigorously: "Rising. At the first drum-roll, the prisoner must rise and dress in silence, as the supervisor opens the cell door. At the second drum-roll, they must be dressed and make their beds. At the third,

they must line up and proceed to the chapel for morning prayer. There is a five-minute interval between each drum-roll."³² Here we see power, the ability to control phenomena, appear not as spectacularly vicious theater, but as a meticulously measured regimentation of time, space, and the human body. Furthermore, the operation of power is now hidden within a house of detention rather than displayed for heuristic political effect before an excitable crowd. This progression, away from traditional repression toward "disciplinary power," is about organizing and harnessing the forces of life; thus Foucault writes of "bio-power." And at the center of this type of regulation is routine surveillance. "Discipline produces subjected and practiced, 'docile' bodies. Discipline increases the force of the body (in economic terms of utility) and diminishes these same forces of the body (in political terms of obedience)"³³ People become more useful as they become more obedient.

During this modernization of social control, the ancient art of torture and confession morphed into the modern methods of surveillance, investigation, and interrogation by which judicial, medical, and moral "truth" can be retrieved from the interior workings of the modern subject. From the new practices emerged the modern "soul"—a political object that displaces the body as the central point of power's leverage. Now interior thoughts, emotions, and patterns become "the effect and instrument of a political anatomy: the soul is the prison of the body."³⁴

THE PANOPTICON: SURVEILLANCE AS IDEA TYPE

For Foucault the paradigmatic example of this surveillance-based discipline was the panopticon—an architectural phantasm springing from the twisted imagination of Jeremy Bentham, the utilitarian philosopher whose preserved corpse still sits in a cupboard at the University of London. In Bentham's work, the panopticon is a circular prison in which illuminated cells are watched from a central observation tower. In a panopticon, prisoners know they could be watched at all times and are thus forced to "internalize the gaze" of the overseers and police themselves. For Foucault this became "the diagram of a mechanism of power reduced to its ideal form,"

the perfect cage in which surveillance harnesses the captive to play the role of both ward and warden.

There is one more element in the story. If domination, control, and bureaucratic organization are ubiquitous, then so too are the counterforces of resistance, protest, sabotage, non-cooperation, and liberty. The hidden history of this sort of resistance is perhaps best captured in Peter Linebaugh and Marcus Rediker's *Many-Headed Hydra: Sailors, Slaves, Commoners, and the Hidden History of the Revolutionary Atlantic*.³⁵ They show how the state and modern methods of control are produced in the forge of constant political struggle. Everyday surveillance in American has a similar history, having developed through the dialectical tension between resistance and regulation.

ANTEBELLUM ID: GENEALOGIES OF IDENTIFICATION AND REGISTRATION

It should be remembered that no slave was allowed to be off the plantation after sunset, without a written pass.

—Allen Parker,
Recollections of Slavery Times

On November 21, 1745, a slave owner from the tobacco country of the Chesapeake littoral ran the following ad in the *Virginia Gazette*:

RUN AWAY about the first of *June* last from Subscriber, living on *Chickahominy* River, *James City* County. A Negroe Man, Short and well-set, aged between 30 and 40 Years, but looks younger, having no Beard, is smooth-fac'd and has some Scars on his Temples, being the Marks of his Country; talks pretty good *English*; is a cunning, subtile Fellow, and pretends to be a Doctor. It is Likely he has a great Acquaintance, he may

question. Viewed from this angle the spectre of a totally transparent society in which obedience and self-policing are the ideal is a threat to the basic preconditions of oppositional politics and social progress.

What would it take to wind back the "thousand things" that make up the soft cage? Clearly there must be prohibitions against ever-expanding surveillance, but only popular pressure will cause the state to build new firewalls of privacy. Only sustained protest will compel regulators to tell corporations, police, schools, hospitals, and other institutions that there are limits. As a society, we want to say: Here you may not go. Here you may not record. Here you may not track and identify people. Here you may not trade and analyze information and build dossiers. There are risks in social anonymity, but the risks of omniscient and omnipotent state and corporate power are far worse.

NOTES

CHAPTER 1: LIFE IN THE GLASS BOX

1. One of the latest erosions of privacy came quietly in the summer of 2002 when Bush overturned Clinton administration rules to allow marketers, and therefore anyone with cash, to access medical records *without* patient consent. See Robert Pea, "Bush Rolls Back Rules on Privacy of Medical Data," *New York Times*, August 10, 2002.
2. Amy Cameron, "Homing Device: How Your Cell Phone Tracks Your Movements," *Maclean's*, February 19, 2001; Ephraim Schwartz, "FBI Phone Tapping and Locating Cell Phones Making 911 Calls: Is It Privacy or Paranoia?" *InfoWorld*, January 15, 2001; Marcia Savage and Amanda Stirpe, "Under Surveillance: Location-Based Wireless Technology Raises Privacy Concerns for Solution Providers," *Computer Reseller News*, December 4, 2000; Charlie Schmidt "The Road Ahead," *MIT's Technology Review* 104, no. 6 (July 2001); "Car Use Down, Public Transit Use Up in San Francisco Bay Area," Associated Press, April 17, 2001.
3. Riochard Boureaux, "Palestinians' Phone Boycott Is Call to Arms," *Los Angeles Times*, July 7, 2001.
4. See chapter 9, "Structure of Feeling," in Raymond Williams, *Marxism and Literature* (Oxford: Oxford University Press, 1978).
5. Kathryn Balint, "Looking After You: Technology Takes Surveillance to a New Level," *San Diego Union-Tribune*, November 5, 2000.
6. Statement of Alan Davidson, associate director, Center for Democracy and Technology, "Cybercrime: Protecting Public Safety and Personal Privacy," before

the Subcommittee on Crime of the House Judiciary Committee, congressional testimony by Federal Document Clearing House, June 12, 2001.

7. Ian Pattison, "Smart Cards: Chipping into Greater Customer Loyalty," *Guardian* (London), July 31, 1999; Bryan Brumley, "Europe Fertile Ground for Smart Card Expansion," Associated Press, December 18, 2000.

8. Jennifer O'Connell, "Smart Cards Threat to Privacy," *Sunday Business Post* (London), April 25, 1999.

9. David Lyon, *The Electronic Eye: The Rise of Surveillance Society* (Minneapolis: University of Minnesota Press, 1994).

10. Ronald Rosenberg, "Citgo to Use Avitar Drug Tests; Job Applicants to Undergo New Saliva-Based Exam," *Boston Globe*, October 12, 2000.

11. Brian Thevenot, "School Drug Testing Praised; Principal Applauds Voluntary Program," *New Orleans Times-Picayune*, December 7, 2000.

12. Sue Anne Pressley, "Puff or Play?" *Newark Star-Ledger*, November 26, 2000.

13. "Banks Say Thumbprints Stamp Out Fraud," *Cleveland Plain Dealer*, October 12, 2000.

14. Randy Kennedy, "At Kennedy, Testing a Truism: The Eyes Don't Lie," *New York Times*, November, 2002; David Mack, "Apartment Security System Gives Residents Palm Reading," *Chicago Sun-Times*, October 22, 1995.

15. Athima Chansanchai, "Tell-Tale Hearts?" *Village Voice*, June 1, 1999.

16. Tina Moore, "Fingerprint System Replaces Lunch Money in Pa. Schools," *Washington Post*, February 25, 2001.

17. "Talk of the Nation," National Public Radio, July 27, 1999.

18. See http://news.mpr.org/features/199911/15_newsroom_privacy/thepricerice.html.

19. "Nice Work for the Aviation Industry," *Airports International*, October 1, 2000; Phelim McAleer, "'Fool-Proof' Security Cameras Put the Innocent in the Frame," *Sunday Times* (London), July 18, 1999.

20. "High-Tech Security on Tampa Streets," Associated Press, July 1, 2001; Amy Herdy, "Eye on Ybor: Police Cameras Go Spy-Tech," *St. Petersburg Times*, June 30, 2001. Interestingly, it is the right wing that leads opposition to surveillance; see David McGuire, "Rep. Army Blasts Tampa over Face-Recognition System," *Newsbytes News Network*, July 2, 2001. Visionics, the US firm that outfitted Tampa, first worked its magic back in 1998 on the streets of London's borough of Newham: S.A. Mathieson, "Online: In Sight of the Law," *Guardian* (London), March 1, 2001.

21. Balint, "Looking After You"; Andrea Combers, "Tiny Tracker," *San Francisco Examiner*, December, 13, 2000; or consider this: "A new service, ParkWatch,

can help family members keep tabs on one another. Parents and kids wear wireless wristwatches with individual ID numbers. The watches are rented for \$3 a day and tracked by antennas around the park. Simply drop by a kiosk and have your watch scanned to pinpoint where anyone in your family is," Lisa McLaughlin, "Personal Time/Your Family," *Time*, October 23, 2000.

22. Beatrice Garcia, "Medical Chips Implanted," *Miami Herald*, May 11, 2002; "Applied Digital on the Brink," *Miami Herald*, February 24, 2003; Deborah Circelli, "America Meeting the 'Chipsons,'" *Palm Beach Post*, March 25, 2002.

23. Fred Vogelstein, "Cons, Don't Leave Home Without It" *US News & World Report*, July 21, 1997.

24. Davidson, "Cybercrime."

25. William Schwabe, Lois M. Davis, Brian A. Jackson, MR-1349-OSTP/NIJ, 2001, Rand and International Association of Chiefs of Police; Joe Salkowski, "Child-Care Web Cams Put Focus on Trust," *Chicago Tribune*, July 23, 2001.

26. For an excellent discussion of these issues, see Jeffery Rosen, "Why Internet Privacy Matters," *New York Times Magazine*, April 30, 2000.

27. *Roy Olmstead v. United States of America*, 277 US 438 (1928).

28. "We have a long-standing policy of cooperation with law enforcement," said AOL spokesman Rich D'Amato; Calvin Woodward, "Police on the Internet Trail; Online Data Can Be Used in Probes," *Richmond Times-Dispatch*, May 28, 1999.

29. It is worth noting that much of Foucault's work recapitulates the arguments of Weber, though in different form and with profound and unique additions. For hints of what we might call the "bio-power" of files and record keeping, see Max Weber, "Bureaucracy," in H.H. Gerth and C. Wright Mills, eds., *From Max Weber: Essays in Sociology* (New York: Oxford University Press, 1958).

30. Michel Foucault, *Discipline and Punish: The Birth of the Prison* (New York: Vintage, 1979), pp. 3, 1.

31. Michel Foucault, "Right of Death and Power over Life," from *The History of Sexuality, Vol. 1*, excerpted in Paul Rabinow, ed., *The Foucault Reader* (New York: Pantheon, 1984), p. 259.

32. Foucault, *Discipline and Punish*, p. 6.

33. *Ibid.*, p. 138.

34. *Ibid.*, p. 30.

35. Peter Linebaugh and Marcus Rediker, *The Many-Headed Hydra: Sailors, Slaves, Commoners, and the Hidden History of the Revolutionary Atlantic* (Boston: Beacon, 2000).