THE SOFT CAGE

SURVEILLANCE IN AMERICA

FROM SLAVE PASSES TO THE WAR ON TERROR
THE

SOFT CAGE
ALSO BY CHRISTIAN PARENTI

LOCKDOWN AMERICA:
POLICE AND PRISONS IN THE AGE OF CRISIS
For my aunt Jeanne Mahon
    and
my friends
Everywhere the state acquires more and more direct control over the humblest members of the community and a more exclusive power of governing each of them in his smallest concerns. This gradual weakening of the individual in relation to society at large may be traced to a thousand things.

—Alexis de Tocqueville, 1835
CONTENTS

ACKNOWLEDGMENTS

xi

CHAPTER 1
Life in the Glass Box
1

CHAPTER 2
Antebellum ID: Genealogies of Identification and Registration
13

CHAPTER 3
The Accumulation of Bodies, Part I: Identification and Photography
33

CHAPTER 4
The Accumulation of Bodies, Part II: Early Biometrics
43

CHAPTER 5
Cruel Gam Saan: Surveillance and Chinese Exclusion
61

CHAPTER 6
Of Ones and Zeros: Digital Surveillance Emerges
77
ACKNOWLEDGMENTS

Many thanks to Rachael Rakes and Dave Kracke, who helped research early sections of this book. Thanks also to Steve Hiatt, who helped make the book readable. I appreciate the hard work of many people at Basic Books, some of whom I will probably never even meet. For crucial, just-in-time editorial comments, my appreciation goes out to Christopher D. Cook and Theodore Hamm. My comrade Heather Rogers also took a scalpel to the manuscript when needed and helped me at every stage; without her this project would have long ago bogged down in the thickets of frustration that inevitably plague a seriously dyslexic author.

More generally, thanks to Sheila Tully, John Marshall, Williams Cole, Liza Featherstone, Doug Henwood, Josh Mason, Colin Robinson, Garrett Scott, Peter Plate, Eric Drooker, Jose Palafox, Jeff Derksen, Rose Braz, Scott Fleming, Cindi Katz, Omar Dahbour, David Reid, my mother Susan and my father Michael, and numerous others who gave me sources, ideas, and advice. I could not have written this book without generous support from the Soros Foundation/Open Society Institute’s Center on Crime and Communities. Both the Blue Mountain Center and Mesa Refuge gave me time, space, and clean air to work and play in. Also a very deep thanks to Neil Smith for his friendship and for giving me an intellectual home at the CUNY Graduate School’s Center for Place, Culture, and Politics when I moved to New York. I am very indebted to Adolph Reed Jr., Ron Takaki, and Mike Davis, all of whom have inspired and educated me and who wrote letters on my behalf. Betsy Reed and Katrina vanden Heuvel helped me to work out ideas when portions of this book first appeared as articles in
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 dollars
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 batteries?
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. 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.

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 guns 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. 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.”

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 “dataveilance”—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. 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. Similar tests are becoming common elsewhere.
LIFE IN THE GLASS BOX

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
THE SOFT CAGE

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

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.

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. 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. 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. 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."

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 emer-
ging, 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 reg-
ular non-actors living together in a house that is completely exposed by
cameras; their challenge is to create a life worth watching while on occa-
sion hiding from the audience. These surveillance-as-challenge, "real-
ity"-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 po-
litical 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, lit-
ter, 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 indi-
vidualistic terms: