



# The Transparent Society

*Will Technology Force*

*Us to Choose Between*

*Privacy and Freedom?*

David Brin

# THE TRANSPARENT SOCIETY

*Will Technology Force  
Us to Choose Between  
Privacy and Freedom?*

David Brin, Ph.D.

▼▼  
ADDISON-WESLEY  
*Reading, Massachusetts*

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book and Addison-Wesley was aware of a trademark claim, the designations have been printed in initial capital letters (e.g., Kindercam).

Library of Congress Cataloging-in-Publication Data

Brin, David.

The transparent society : will technology force us to choose between privacy and freedom? / David Brin.

p. cm.

Includes bibliographical references and index.

ISBN 0-201-32802-X

1. Freedom of information.
2. Privacy, Right of.
3. Responsibility. I. Title.

JC598.B75 1998

323.44'8—dc21

98-5310

CIP

Copyright © 1998 by David Brin

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher. Printed in the United States of America.

Addison-Wesley is an imprint of Addison Wesley Longman, Inc.

Jacket design by Steven Brower

Text design by Karen Savary

Set in 11 point Electra by Carlisle Communications, Inc.

1 2 3 4 5 6 7 8 9-MA-0201009998

First printing, April 1998

Addison-Wesley books are available at special discounts for bulk purchases. For more information about how to make such purchases in the U.S., please contact the Corporate, Government, and Special Sales Department at Addison Wesley Longman, One Jacob Way, Reading, MA 01867, or call (800) 238-9682.

Find us on the World Wide Web at <http://www.aw.com/gb/>

*To Popper, Pericles, Franklin, and  
countless others who helped fight for  
an open society . . . and to their heirs  
who have enough courage to stand in  
the light and live unmasked.*

*There is not a crime, there is not a dodge,  
there is not a trick, there is not a swindle,  
there is not a vice which does not live by  
secrecy.*

JOSEPH PULITZER

*Sunlight is said to be the best of  
disinfectants.*

JUSTICE LOUIS BRANDEIS

# CONTENTS

## **PART I: A NEW WORLD**

1

### **ONE THE CHALLENGE OF AN OPEN SOCIETY 3**

*The End of Photography as Proof of Anything at All 27*

### **TWO THE AGE OF KNOWLEDGE 32**

*Citizen Truth Squads 52*

### **THREE PRIVACY UNDER SIEGE 54**

*The Accountability Matrix 85*

### **FOUR CAN WE OWN INFORMATION? 89**

*An Open Society's Enemies 108*

## **PART II: MINEFIELDS**

115

### **FIVE HUMAN NATURE AND THE DILEMMA OF OPENNESS 117**

*Essences and Experiments 146*

### **SIX LESSONS IN ACCOUNTABILITY 149**

*All the World Is a (Digital) Marketplace 178*

### **SEVEN THE WAR OVER SECRECY 185**

*The Problem of Extortion 227*

## **PART III: ROAD MAPS**

231

### **EIGHT PRAGMATISM IN AN UNCERTAIN WORLD 233**

*The Plausibility Matrix 271*

vi CONTENTS

**NINE** HUMILITY AND LIMITS 278

*A Withering Away?* 303

**TEN** GLOBAL TRANSPARENCY 309

*A Little Loyalty* 322

**ELEVEN** THE ROAD OF OPENNESS 325

NOTES 336

FOLLOW-UP 369

ACKNOWLEDGMENTS 371

INDEX 372

ABOUT THE AUTHOR 378

# PART I A NEW WORLD

*There's no going back, and there's no  
hiding the information. So let everyone  
have it.*

ANDREW KANTOR





## CHAPTER ONE

# THE CHALLENGE OF AN OPEN SOCIETY

*Sacrificing anonymity may be the next generation's price for keeping precious liberty, as prior generations paid in blood.*

HAL NORBY

*You're wondering why I've called you here. The reason is simple. To answer all your questions. I mean—all. This is the greatest news of our time. As of today, whatever you want to know, provided it's in the data-net, you can know. In other words, there are no more secrets.*

JOHN BRUNNER,

THE SHOCKWAVE RIDER, 1974

This is a tale of two cities. Cities of the near future, say ten or twenty years from now.

Barring something unforeseen, you are apt to be living in one of these two places. Your only choice may be which one.

At first sight, these two municipalities look pretty much alike. Both contain dazzling technological marvels, especially in the realm of electronic media. Both suffer familiar urban quandaries of frustration and decay. If

some progress is being made in solving human problems, it is happening gradually. Perhaps some kids seem better educated. The air may be marginally cleaner. People still worry about overpopulation, the environment, and the next international crisis.

None of these features is of interest to us right now, for we have noticed something about both of these twenty-first-century cities that is radically different. A trait that marks them as distinct from any metropolis of the late 1990s.

Street crime has nearly vanished from both towns. But that is only a symptom, a result.

The real change peers down from every lamppost, every rooftop and street sign.

Tiny cameras, panning left and right, survey traffic and pedestrians, observing everything in open view.

Have we entered an Orwellian nightmare? Have the burghers of both towns banished muggings at the cost of creating a Stalinist dystopia?

Consider city number one. In this place, all the myriad cameras report their urban scenes straight to Police Central, where security officers use sophisticated image processors to scan for infractions against public order—or perhaps against an established way of thought. Citizens walk the streets aware that any word or deed may be noted by agents of some mysterious bureau.

Now let's skip across space and time.

At first sight, things seem quite similar in city number two. Again, ubiquitous cameras perch on every vantage point. Only here we soon find a crucial difference. These devices do *not* report to the secret police. Rather, each and every citizen of this metropolis can use his or her wristwatch television to call up images from any camera in town.

Here a late-evening stroller checks to make sure no one lurks beyond the corner she is about to turn.

Over there a tardy young man dials to see if his dinner date still waits for him by a city fountain.

A block away, an anxious parent scans the area to find which way her child wandered off.

Over by the mall, a teenage shoplifter is taken into custody gingerly, with minute attention to ritual and rights, because the arresting officer knows that the entire process is being scrutinized by untold numbers who watch intently, lest her neutral professionalism lapse.

In city number two, such microcameras are banned from some indoor places . . . but not from police headquarters! There any citizen may tune in on bookings, arraignments, and especially the camera control room itself, making sure that the agents on duty look out for violent crime, and only crime.

Despite their initial similarity, these are very different cities, representing disparate ways of life, completely opposite relationships between citizens and their civic guardians. The reader may find both situations somewhat chilling. Both futures may seem undesirable. But can there be any doubt which city we'd rather live in, if these two make up our only choice?

### TECHNOLOGY'S VERDICT

Alas, they do appear to be our only options. For the cameras *are* on their way, along with data networks that will send a myriad images flashing back and forth, faster than thought.

In fact, the future has already arrived. The trend began in Britain a decade ago, in the town of King's Lynn, where sixty remote-controlled video cameras were installed to scan known "trouble spots," reporting directly to police headquarters. The resulting reduction in street crime exceeded all predictions; in or near zones covered by surveillance, crime dropped to one-seventieth of the former rate. The savings in patrol costs alone paid for the equipment in a few months. Dozens of cities and towns soon followed the example of King's Lynn. Glasgow, Scotland, reported a 68 percent drop in crime citywide, while police in Newcastle fingered over 1,500 perpetrators with taped evidence. (All but seven pleaded guilty, and those seven were later convicted.) In May 1997, Newcastle soccer fans rampaged through downtown streets. Detectives studying video tapes picked out 152 faces and published 80 photographs in local newspapers. In days, all were identified.

Today, over 300,000 cameras are in place throughout the United Kingdom, transmitting round-the-clock images to a hundred constabularies, all of them reporting decreases in public misconduct. Polls report that the cameras are extremely popular with citizens, though British civil libertarian John Wadham and others have bemoaned this proliferation of snoop technology, claiming, "It could be used for any other purpose, and of course it could be abused."

Visitors to Japan, Thailand, and Singapore will see that other countries are rapidly following the British example, using closed circuit television (CCTV) to supervise innumerable public areas.

This trend was slower coming to North America, but it appears to be taking off. After initial experiments garnered widespread public approval, the City of Baltimore put police cameras to work scanning all 106 downtown intersections. In 1997, New York City began its own program to set up twenty-four-hour remote surveillance in Central Park, subway stations, and other public places.

No one denies the obvious and dramatic short-term benefits derived from this early proliferation of surveillance technology. That is not the real issue. In the long run, the sovereign folk of Baltimore and countless other communities will have to make the same choice as the inhabitants of our two mythical cities. *Who will ultimately control the cameras?*

Consider a few more examples.

How many parents have wanted to be a fly on the wall while their child was at day care? This is now possible with a new video monitoring system known as Kindercam, linked to high-speed telephone lines and a central Internet server. Parents can log on, type "www.kindercam.com," enter their password, and access a live view of their child in day care at any time, from anywhere in the world. Kindercam will be installed in two thousand day-care facilities nationwide by the end of 1998. Mothers on business trips, fathers who live out of state, even distant grandparents can all "drop in" on their child daily. Drawbacks? Overprotective parents may check compulsively. And now other parents can observe *your* child misbehaving!

Some of the same parents are less happy about the lensed pickups that are sprouting in their own workplaces, enabling supervisors to tune in on them in the same way they use Kindercam to check up on their kids.

That is, if they notice the cameras at all. At present, engineers can squeeze the electronics for a video unit into a package smaller than a sugar cube. Complete sets half the size of a pack of cigarettes were recently offered for sale by the Spy Shop, a little store in New York City located two blocks from the United Nations. Meanwhile, units with radio transmitters are being disguised in clock radios, telephones, and toasters, as part of the burgeoning "nannycam" trend. So high is demand for these pickups, largely by parents eager to check on their babysitters, that just one firm in Orange County, California, has recently been selling from five hundred to one thousand disguised cameras a month. By the end of 1997, prices had dropped from \$2,500 to \$399.

Cameras aren't the only surveillance devices proliferating in our cities. Starting with Redwood City, near San Francisco, several police departments have begun lacing neighborhoods with sound pickups that transmit directly back to headquarters. Using triangulation techniques, officials can now pinpoint bursts of gunfire and send patrol units swiftly to the scene, without having to wait for vague telephone reports from neighbors. In 1995 the Defense Department awarded a \$1.7 million contract to Alliant Techsystems for its prototype system SECURES, which tests more advanced sound pickup networks in Washington and other cities. The hope is to distinguish not only types of gunfire but also human voices crying for help.

So far, so good. But from there, engineers say it would be simple to upgrade the equipment, enabling bored monitors to eavesdrop through open bedroom windows on cries of passion, or family arguments. "Of course we would never go that far," one official said, reassuringly.

Consider another piece of James Bond apparatus now available to anyone with ready cash. Today, almost any electronics store will sell you night vision goggles using state-of-the-art infrared optics equal to those issued by the military, for less than the price of a video camera. AGEMA Systems, of Syracuse, New York, has sold several police departments imaging devices that can peer into houses from the street, discriminate the heat given off by indoor marijuana cultivators, and sometimes tell if a person inside moves from one room to the next. Military and civilian enhanced vision technologies now move in lockstep, as they have in the computer field for years.

In other words, even darkness no longer guarantees privacy.

Nor does your garden wall. In 1995, Admiral William A. Owens, then vice chairman of the Joint Chiefs of Staff, described a sensor system that he expected to be operational within a few years: a pilotless drone, equipped to provide airborne surveillance for soldiers in the field. While camera robots in the \$1 million range have been flying in the military for some time, the new system will be extraordinarily cheap and simple. Instead of requiring a large support crew, it will be controlled by one semi-skilled soldier and will fit in the palm of a hand. Minuscule and quiet, such remote-piloted vehicles, or RPVs, may flit among trees to survey threats near a rifle platoon. When mass-produced in huge quantities, unit prices will fall.

Can civilian models be far behind? No law or regulation will keep them from our cities for very long. The rich, the powerful, and figures of authority will have them, whether legally or surreptitiously. And the contraptions will become smaller, cheaper, and smarter with each passing year.

So much for the supposed privacy enjoyed by sunbathers in their own backyards.

Moreover, surveillance cameras are the tip of the metaphorical iceberg. Other entrancing and invasive innovations of the vaunted *information age* abound. Will a paper envelope protect the correspondence you send by old-fashioned surface mail when new-style scanners can trace the patterns of ink inside without ever breaking the seal?

Let's say you correspond with others by e-mail and use a computerized encryption program to ensure that your messages are read only by the intended recipient. What good will all the ciphers and codes do, if some adversary has bought a "back door" password to your encoding program? Or if a wasp-sized camera drone flits into your room, sticks to the ceiling

above your desk, inflates a bubble lens, and watches every keystroke that you type? (A number of such unnerving techno-possibilities will be discussed in chapter 8.)

In late 1997 it was revealed that Swiss police had secretly tracked the whereabouts of mobile phone users via a telephone company computer that records billions of movements per year. Swisscom was able to locate its mobile subscribers within a few hundred meters. This aided several police investigations. But civil libertarians expressed heated concern, especially since identical technology is used worldwide.

The same issues arise when we contemplate the proliferation of vast databases containing information about our lives, habits, tastes, and personal histories. As we shall see in chapter 3, the cash register scanners in a million supermarkets, video stores, and pharmacies already pour forth a flood of statistical data about customers and their purchases, ready to be correlated. (Are you stocking up on hemorrhoid cream? Renting a daytime motel room? The database knows.) Corporations claim this information helps them serve us more efficiently. Critics respond that it gives big companies an unfair advantage, enabling them to know vastly more about us than we do about them. Soon, computers will hold all your financial and educational records, legal documents, and medical analyses that parse you all the way down to your genes. Any of this might be examined by strangers without your knowledge, or even against your stated will.

As with those streetlamp cameras, the choices we make regarding future information networks—how they will be controlled and who can access the data—will affect our own lives and those of our children and their descendants.

## A MODERN CONCERN

The issue of threatened privacy has spawned a flood of books, articles, and media exposés—from Janna Malamud Smith's thoughtful *Private Matters*, and Ellen Alderman and Caroline Kennedy's erudite *Right to Privacy* all the way to shrill, paranoid rants by conspiracy fetishists who see Big Brother lurking around every corner. Spanning this spectrum, however, there appears to be one common theme. Often the author has responded with a call to arms, proclaiming that we must become more vigilant to protect traditional privacy against intrusions by faceless (*take your pick*) government bureaucrats, corporations, criminals, or just plain busybodies.

That is the usual conclusion—but not the one taken here.

For in fact, it is already far too late to prevent the invasion of cameras and databases. The *djinn* cannot be crammed back into its bottle. No mat-

ter how many laws are passed, it will prove quite impossible to legislate away the new surveillance tools and databases. They are here to stay.

Light is going to shine into nearly every corner of our lives.

The real issue facing citizens of a new century will be how mature adults choose to live—how they can compete, cooperate, and thrive—in such a world. A transparent society.

Regarding those cameras, for instance—the ones atop every lamppost in both city one and city two—we can see that very different styles of urban life resulted from just one decision, based on how people in each town answered the following question.

*Will average citizens share, along with the mighty, the right to access these universal monitors? Will common folk have, and exercise, a sovereign power to watch the watchers?*

Back in city number one, Joe and Jane Doe may walk through an average day never thinking about those microcameras overhead. They might even believe official statements claiming that all the spy eyes were banished and dismantled a year or two ago, when in fact they were only made smaller, harder to detect. Jane and Joe stroll secure that their neighbors cannot spy on them (except the old-fashioned way, from overlooking windows). In other words, Jane and Joe blissfully believe they have *privacy*.

The inhabitants of city number two know better. They realize that, out of doors at least, complete privacy has always been an illusion. They know anyone can tune in to that camera on the lamppost—and they don't much care. They perceive what really matters: that they live in a town where the police are efficient, respectful, and above all accountable. Homes are sacrosanct, but out on the street any citizen, from the richest to the poorest, can both walk safely and use the godlike power to zoom at will from vantage point to vantage point, viewing all the lively wonders of the vast but easily spanned village their metropolis has become, as if by some magic it had turned into a city not of people but of birds.

Sometimes, citizens of city number two find it tempting to wax nostalgic about the old days, before there were so many cameras, or before television invaded the home, or before the telephone and automobile. But for the most part, city number two's denizens know that those times are gone, never to return. Above all, one thing makes life bearable: the surety that each person knows what is going on, with a say in what will happen next. And has rights equal to those of any billionaire or chief of police.

This little allegory—like all allegories—may be a gross oversimplification. For instance, in our projected city of “open access,” citizens will have ten thousand decisions to make. Here are just a few examples:



- Since one might conceivably use these devices to follow someone home, should convicted felons be forbidden access to the camera networks?
- Might any person order up a search program, using sophisticated pattern-recognition software to scan a throng of passersby and zero in on a specific face? If such “traps” could be laid all over town, a lot of fugitives might be brought to justice. But will individuals ever again be able to seek anonymity in a crowd? Will people respond by wearing masks in public? Or will safety ultimately come when people unleash their own search programs, to alert the watched about their watchers?
- When should these supercameras be allowed indoors? If cameras keep getting smaller and more mobile, like wasp-size drones, what kind of defenses might protect us against Peeping Toms, or police spies, flying such devices through the open windows of our homes?

The list of possible quandaries goes on and on. Such an endless complexity of choices may cause some citizens of city number two to envy the simplicity of life in city number one, where only big business, the state, and certain well-heeled criminals possess these powers. That elite will in turn try to foster a widespread illusion among the populace that the cameras don't exist. Some folk will prefer a fantasy of privacy over the ambiguity and arduous decisions faced by citizens of city number two.

There is nothing new in this. All previous generations faced quandaries the outcomes of which changed history. When Thomas Jefferson prescribed a revolution every few decades, he was speaking not only politically but also about the constant need to remain flexible and adapt to changing circumstances, to innovate as needed, while at the same time staying true to those values we hold unchanging and precious. Our civilization is already a noisy one precisely because we have chosen freedom and mass sovereignty, so that the citizenry itself must constantly argue out the details, instead of leaving them to some committee of sages.

What distinguishes society today is not only the pace of events but also the nature of our tool kit for facing the future. Above all, what has marked our civilization as different is its knack for applying two extremely hard-won lessons from the past.

*In all of history, we have found just one cure for error—a partial antidote against making and repeating grand, foolish mistakes, a remedy against self-deception. That antidote is criticism.*

Scientists have known this for a long time. It is the keystone of their success. A scientific theory gains respect only by surviving repeated attempts to