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 burglers 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.

*In mid-1998 the British raised the ante once again, testing 140 cameras that scan the faces of pedestrians and compare them to digital images of known felons.
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
demolish it. Only after platoons of clever critics have striven to come up with refuting evidence, forcing changes, do a few hypotheses eventually graduate from mere theories to accepted models of the world.

Another example is capitalism. When it works, under just and impartial rules, the free market rewards agility, hard work, and innovation, just as it punishes the stock prices of companies that make too many mistakes. Likewise, any believer in evolution knows that death is the ultimate form of criticism, a merciless driver, transforming species over time.

Even in our private and professional lives, mature people realize that improvement comes only when we open ourselves to learn from our mistakes, no matter how hard we have to grit our teeth, when others tell us we were wrong. Which brings us to our second observation.

Alas, criticism has always been what human beings, especially leaders, most hate to hear.

This ironic contradiction, which I will later refer to as the “Paradox of the Peacock,” has had profound and tragic effects on human culture for centuries. Accounts left by past ages are filled with woeful events in which societies and peoples suffered largely because openness and free speech were suppressed, leaving the powerful at liberty to make devastating blunders without comment or consent from below.

If neo-Western civilization* has one great trick in its repertoire, a technique more responsible than any other for its success, that trick is accountability. Especially the knack—which no other culture ever mastered—of making accountability apply to the mighty. True, we still don’t manage it perfectly. Gaffes, bungles, and inanities still get covered up. And yet, one can look at any newspaper or television news program and see an eager press corps at work, supplemented by hordes of righteously indignant individuals (and their lawyers), all baying for waste or corruption to be exposed, secrets to be unveiled, and nefarious schemes to be nipped in the bud. Disclosure is a watchword of the age, and politicians have grudgingly responded by passing the Freedom of Information Act (FOIA), truth-in-lending laws, open-meeting rules, and codes to enforce candor in real estate, in the nutritional content of foodstuffs, in the expense accounts of lobbyists, and so on.

Although this process of stripping off veils has been uneven, and continues to be a source of contention, the underlying moral force can clearly be seen pervading our popular culture, in which nearly every modern film or novel seems to preach the same message—suspicion of authority. The

*For a discussion of this term, and many other terms, tangents, and ways to explore this book’s topics, please see the notes beginning on page 336.
phenomenon is not new to our generation. Schoolbooks teach that freedom is guarded by constitutional "checks and balances," but those same legal provisions were copied, early in the nineteenth century, by nearly every new nation of Latin America, and not one of them remained consistently free. In North America, constitutional balances worked only because they were supplemented by a powerful mythic tradition, expounded in story, song, and now virtually every Hollywood film, that any undue accumulation of power should be looked on with concern.

Above all, we are encouraged to distrust government.

The late Karl Popper pointed out the importance of this mythology in the dark days during and after World War II, in The Open Society and Its Enemies. Only by insisting on accountability, he concluded, can we constantly remind public servants that they are servants. It is also how we maintain some confidence that merchants aren’t cheating us, or that factories aren’t poisoning the water. As inefficient and irascibly noisy as it seems at times, this habit of questioning authority ensures freedom far more effectively than any of the older social systems that were based on reverence or trust.

And yet, another paradox rears up every time one interest group tries to hold another accountable in today’s society.

Whenever a conflict arises between privacy and accountability, people demand the former for themselves and the latter for everybody else.

The rule seems to hold in almost every realm of modern life, from special prosecutors investigating the finances of political figures to worried parents demanding that lists of sex offenders be made public. From merchants anxious to see their customers’ credit reports to clients who resent such snooping. From people who “need” caller ID to screen their calls to those worried that their lives might be threatened if they lose telephone anonymity. From activists demanding greater access to computerized government records in order to hunt patterns of corruption or incompetence in office to other citizens who worry about the release of personal information contained in those very same records.

Recent years have witnessed widespread calls to “empower” citizens and corporations with tools of encryption—the creation of ciphers and secret codes—so that the Internet and telephone lines may soon fill with a blinding fog of static and concealed messages, a haze of habitual masks and routine anonymity. Some of society’s best and brightest minds have begun extolling a coming “golden age of privacy,” when no one need ever again fear snooping by bureaucrats, federal agents, or in-laws. The prominent iconoclast John Gilmore, who favors “law ‘n’ chaos over law ‘n’ order,” re-
ently proclaimed that computers are literally extensions of our minds, and that their contents should therefore remain as private as our inner thoughts. Another activist, John Perry Barlow, published a widely discussed “Declaration of Independence for Cyberspace” proclaiming that the mundane jurisdictions of nations and their archaic laws are essentially powerless and irrelevant to the Internet and its denizens (or “netizens”). Among the loose clan of self-proclaimed “cypherpunks,” a central goal is that citizens should be armed with broad new powers to conceal their words, actions, and identities. The alternative, they claim, will be for all our freedoms to succumb to a looming tyranny.

In opposing this modern passion for personal and corporate secrecy, I should first emphasize that I like privacy! Outspoken eccentrics need it, probably as much or more than those who are reserved. I would find it hard to get used to living in either of the cities described in the example at the beginning of this chapter. But a few voices out there have begun pointing out the obvious. Those cameras on every street corner are coming, as surely as the new millennium.

Oh, we may agitate and legislate. But can “privacy laws” really prevent hidden eyes from getting tinier, more mobile, and clever? In software form they will cruise the data highways. “Antivirus” technologies will arise, but the resulting surveillance arms race can hardly favor the “little guy.” The rich, the powerful, police agencies, and a technologically skilled elite will always have an advantage.

In the long run, as author Robert Heinlein prophesied years ago, will the chief effect of privacy laws simply be to “make the bugs smaller”?

The subtitle of this book—Will Technology Force Us to Choose Between Privacy and Freedom?—is intentionally provocative. As we’ll see, I think such a stark choice can be avoided. It may be possible to have both liberty and some shelter from prying eyes.

But suppose the future does present us with an absolute either-or decision, to select just one, at the cost of the other. In that case, there can be no hesitation.

Privacy is a highly desirable product of liberty. If we remain free and sovereign, we may have a little privacy in our bedrooms and sanctuaries. As citizens, we’ll be able to demand some.

But accountability is no side benefit. It is the one fundamental ingredient on which liberty thrives. Without the accountability that derives from openness—enforceable upon even the mightiest individuals and institutions—how can freedom survive?

In the information age to come, cameras and databases will spout like poppies—or weeds—whether we like it or not. Over the long haul, we as a people must decide the following questions:
Can we stand living exposed to scrutiny, our secrets laid open, if in return we get flashlights of our own that we can shine on anyone who might do us harm—even the arrogant and strong?

Or is an illusion of privacy worth any price, even the cost of surrendering our own right to pierce the schemes of the powerful?

There are no easy answers, but asking questions can be a good first step.

THE PRIVACY WE ALREADY HAVE

Much of this chapter up to now appeared earlier as a published article and has since been perused online by interested parties around the globe. Their varied comments opened my eyes to a wide range of opinions about freedom, privacy, and candor. From philosophers to steelworkers, it seems that each person views such things differently. Especially privacy, which, like the fabled elephant fondled by a dozen blind sages, is described uniquely by each beholder.

Even legal scholars cannot agree what the word means. American judicial rulings tend to treat privacy as a highly subjective and contingent commodity, a matter of trade-offs and balanced interests, whereas freedom of speech and freedom of the press are defended with sweeping judgments of broad generality. Some reasons for this difference will be discussed in chapter 3, where privacy is examined from many angles and shown to be the exquisite desideratum that it is. Indeed, without some privacy, we could scarcely function as humans. A chief aim of this book is to explore whether—and how much—privacy can be safeguarded in a coming era of cameras and databases.

Alas, although it seems intuitive to protect privacy by erecting barriers to information flow, there may be good reason to question that assumption. Although I shall put off a more involved discussion until later, let me briefly illustrate with a restaurant analogy.

We all know it is possible to be alone, or hold intimate conversations, in a public place. It bothers people to be stared at, especially while eating, yet we dine in crowded restaurants all the time, fairly secure that most of the eyes surrounding us aren’t looking our way, at least not very often. We don’t achieve this confidence by wearing masks, or because laws require other customers to wear blinkers and blindfolds. Mutual civility and common decency play a role, but not alone.

An added factor that helps deter people from staring is not wanting to be caught in the act. The embarrassment accrued by a voyeur caught observing you is greater than your chagrin at being seen by the voyeur with asparagus in your teeth. Open visibility seems to favor defense over offense.
All right, it’s not perfect, but it works overall.

Now suppose we try to improve things by passing laws and sending forth regulators with clipboards commanding all restaurants to erect a maze of paper shoji screens to keep customers from ogling other patrons. Will this prevent people from staring, or encourage them? Without any plausible likelihood of getting caught, might voyeurs use technology, in this case poking tiny holes, to penetrate the “protective” curtain? No longer deterred, could peepers stare with impunity?

The restaurant analogy is just a thought experiment. But it suggests that there is no dichotomy between accountability and privacy. Rather, you may need one to get the other.

WHAT LIES AHEAD

We must cover important ground before getting to the kernel of the argument over transparency. So chapter 2 begins by comparing the bright new information age with other highly vaunted “eras” that left disappointment in their wake. Cynical observers already predict the same demise for the swaggering epoch of silicon and electrons, yet new cybernetic tools may help bring a time of unprecedented opportunity, assisting hard-pressed humanity with pragmatic solutions to many vexing problems.

Chapters 3 and 4 explore the nature and practical limits of privacy, how it is perceived by the law, and the looming question of whether information is a commodity that can be owned, focusing especially on the role of copyright protection to promote openness and creativity.

Ultimately, the big choices must be made by citizens, who will either defend their freedom or surrender it, as others did in the past. Chapter 5 examines some peculiar traits of neo-Western civilization, a quirky and amorphous global super society that fosters eccentricity and ego the way other cultures have extolled obedience or physical courage. Chapter 6 then considers how lessons of accountability may apply to everyone from cops to social rebels, as we learn to “watch the watchmen.”

Along the way, in secondary interludes following each numbered chapter, we will take a look at several topics of survival in the information age, including the worrisome problems of photographic fakery and computerized extortion, as well as the ongoing question of whether we should concentrate on ideals, or on what works.

(End notes, references, and supplementary material for each chapter can be found in a section at the back of this book.)

Chapter 7 gets into “nitty gritty” issues concerning encryption (secret codes) and anonymity, two prescriptions that are highly touted by some of society’s best and brightest cyberphilosophers. Chapter 8 covers some
pragmatic problems, such as the controversy concerning names, passwords, Social Security numbers, and national ID cards.

Any honest person must consider the possibility that he or she might be mistaken, so chapter 9 is where I do that. Among other things, I discuss whether mathematicians think encryption can really offer security against data spying by the biggest government computers. The chapter also covers a range of possible ways in which “transparency” might turn into a nightmare, especially if my sanguine views of the advantages turn out to be wrong.

Finally, chapters 10 and 11 will expand the context of discussion to encompass the security of global civilization, pondering whether we at last have the tools to avoid the errors that toppled so many societies in the past.

But first, let’s consider the nature of open societies.

THE GHOST OF PERICLES

We live in a time that spills over with contradictions. Extraordinary wealth gushes alongside grinding poverty. Episodes of horrific bloodshed contrast starkly with unprecedented stretches of peace, in which billions of living human beings have never personally experienced war. Within a single life span we’ve seen great burgeonings of freedom—and the worst tyrannies of all time. To find another era with as dramatic a range of highs and lows, you might go back twenty-five centuries, when another “golden age” posed towering hopes against cynicism and despair.

Like the world of today, classical Athens featured profound bursts of creativity in science, culture, and the arts. But above all, the vision we tend to retain is that city’s brief adventure in democracy, a brave experiment that lasted just a little while and would not be tried again in a big way for two millennia.

Even staunch fans of Athenian democracy admit it was imperfect by present-day standards; for instance, women, slaves, and those not born in the city had few rights. Yet its relative egalitarianism was impressive in an age of hereditary chiefdoms and arbitrary potentates. Across centuries of darkness, from that democracy to this one, the lonely voice of Pericles spoke for an open society, where citizens are equal before the law and where influence is apportioned “not as a matter of privilege, but as a reward for merit; and poverty is not a bar. . . .”

The virtues of this notion may seem obvious to modern readers. Today, citizens of many nations—those that I call neo-Western—assume that principles of equality and human rights are fundamental, even axiomatic (though they are often contentious to implement in practice).

So it can be surprising to learn just how rare this attitude was, historically. In fact, Pericles and his allies were roundly derided by contemporary schol-
ars. Countless later generations of intellectuals and oligarchs called democracy an aberration, ranking it among the least important products of the Athenian golden age. Even during the Italian Renaissance, Niccolò Machiavelli had to mask his sympathy for representative government between the lines of *The Prince*, in order to please his aristocratic sponsors. After Athens’s flickering candle blew out during the Peloponnesian War (431–403 B.C.E.), none was more eager to cheer the demise of democracy than Plato, the so-called father of Western philosophy. He wrote:

> The greatest principle of all is that nobody should be without a leader. Nor should the mind of anybody be habituated to do anything at all on his own initiative; neither out of zeal, nor even playfully. . . . In a word, he should teach his soul, by long habit, never to dream of acting independently, and to become utterly incapable of it.

Partly due to the influence of Plato and his followers—and for reasons discussed in chapter 5 of this book—the democratic experiment was not tried again on a large scale until the era of Locke, Jefferson, and Madison.

We all know in our hearts that freedom cannot survive such assaults, unless it is defended by much more than good intentions. For a time, in the middle of the twentieth century, it looked as if the Athenian tragedy might happen again, when constitutional governments seemed about to be overwhelmed by despots and ideologues. Writing under the shadow of Hitler, and later Stalin, Karl Popper began *The Open Society and Its Enemies* by appraising the relentless hatred for empiricism and democracy that Plato passed on through his followers all the way to Hegel—a philosophical heritage of self-serving, tendentious incantations (or “reasoning”) whose hypnotic rhythms were enthusiastically adapted by innumerable rulers, from Hellenistic despots to Marxist-Leninist commissars, many of them using contorted logic to justify their unchecked power over others.

Looking back from the 1990s, when democracy seems strong—though hardly triumphant—we can only imagine how delicate freedom must have seemed to Popper, George Orwell, Aldous Huxley, and others writing in the 1940s and 1950s. Did they feel the ghost of Pericles hovering over their shoulders as they worked? Would the candle blow out yet again?

Scanning history, those writers could see only a few other brief oases of relative liberty—the Icelandic Althing, some Italian city-states, the Iroquois Confederacy, and perhaps a couple of bright moments during the Roman Republic, or the Baghdad Caliphate—surrounded by vast eras when the social pyramid in every land was dominated by conspiracies of privilege. Ruling elites varied widely in their superficial trappings. Some styled themselves
as kings or oligarchs, while others were priests, bureaucrats, merchant
princes, or "servants of the people." But nearly all used similar methods to
justify and secure the accumulation and monopolization of privilege.

One paramount technique was to control the flow of information.
Tyrants were always most vulnerable when those below could see and hear
the details of power and statecraft.

Today, the light appears much stronger than in Popper's day, and new
technologies such as the Internet seem about to enhance the sovereign au-
thority of citizens even further. Yet the problem remains as fundamental
and worrisome as ever: What measures can we take to ensure that freedom,
instead of being a rare exception, will become the normal, natural, and sta-
ble condition for ourselves and our descendants?

In fairness, this same unease motivates many of those who oppose the
notion of a "transparent society." They share the apprehension Orwell con-
voyed so chillingly in Nineteen Eighty-Four: that freedom may vanish un-
less people promptly and vigorously oppose the forces that threaten it. So
from the start, let me say to them that we are not arguing about goals, but
rather the best means to achieve them.

That still leaves room for disagreement, for instance, over whether the
sole peril originates from national governments, or whether dangerous
power centers may arise from any part of the sociopolitical landscape.
Moreover, we differ over which tools will best help stave off tyranny.
Metaphorically speaking, some very bright people suggest that citizens of
the twenty-first century will be best protected by masks and shields, while
I prefer the image of a light saber.

These glib metaphors may cue readers that I won't be presenting an
erudite or academic tome on the same level as Popper's The Open Society
and Its Enemies, and that is certainly true. I shall not claim to prove or de-
molish any broad social rules. Above all, this book does not push an absurd
overgeneralization that candor is always superior to secrecy! Only that
transparency is underrepresented in today's fervid discussions about privacy
and freedom in the information age. My sole aim is to stir some fresh ideas
into the cauldron.

If we have learned anything during the hard centuries since Pericles
and his allies tried to light a flickering beacon in the night, it is that we owe
our hard-won freedom and prosperity to an empirical tradition—in sci-
cence, free markets, and the rough-tumble world of democracy. Only math-
ematicians can "prove" things using pen and paper. The rest of us have to
take our ideas pragmatically into the real world and see what works.

In other words, this is not a book of grand prescriptions (though some
suggestions are offered). I plan chiefly to discuss underutilized tools of
openness and light that have served us well in the past.
STRONG PRIVACY

Before getting to those suggestions, we need to establish some context about today’s public debate over privacy. In keeping with the theme of this book, I rank the players and their arguments according to what effect their proposals would have on the flow of information in society.

Take Megan’s Law, for example. Under a 1994 U.S. federal mandate, all fifty states have begun publishing registers of sexual offenders, which will lead eventually to a nationwide database. California provides this information on a CD-ROM disk that can be viewed at most police headquarters, letting parents, school officials, and other interested parties survey over 65,000 names (and many photos) for “potential molesters” who may live or work in their area. Activists supporting this system portray it as a way to ensure accountability in an area of life where a single mistake can lead to tragedy.

Foes of the measure, including the American Civil Liberties Union (ACLU), claim that the rights of former prisoners are violated by this registry, which can be regarded as a nonjudicial additional penalty slapped onto the sentences of convicts who have already paid their debt to society. Opponents also cite anecdotes in which individuals suffered because they were erroneously listed, showing that innocents can be harmed by hastily and overzealously opening spigots of potentially faulty data.

As far as this book is concerned, the relative merits of Megan’s Law are not at issue. Rather, this struggle simply serves to illustrate two opposing traits that appear in countless other modern privacy disputes.

A. One party believes that another group is inherently dangerous, and that its potential to do harm is exacerbated by secrecy. Therefore, accountability must be forced upon that group through enhanced flow of information.

B. The other party argues that some vital good will be threatened by heightened candor, and hence wants the proposed data flow shut down.

Watch for this pattern as we go along. We shall see that it is almost ubiquitous when people take a stand on knowledge disputes. In chapter 7, for instance, we’ll discuss many and varied “Clipper” proposals that have been floated by the FBI and other federal agencies concerned about the potential of data and voice encryption to conceal criminal or terrorist activities behind a static haze. Officials worry that widespread use of electronic ciphers will thwart traditional surveillance techniques, such as court-ordered wiretaps, enabling dangerous villains to conspire in security and secrecy. They want to retain the level of vision and accountability that they traditionally held in an era of crude analog phone lines.
A coalition of groups, including the Electronic Frontier Foundation (EFF) and the Electronic Privacy Information Center (EPIC), joined numerous journalists and private persons to lambaste the Clipper proposals, depicting them as encroachments by government on freedom and privacy in cyberspace. Often, they couched the threat in dramatic terms, as the opening move in a trend toward a Big Brother dictatorship. In any event, they point out that the FBI seeks a data flow enhancement that would go just one way, to government officials.

In this example, the FBI’s proposal fits pattern A, while their adversaries fill position B. But these roles are often reversed! Take the ongoing struggle faced by anyone seeking documents from a federal agency under the Freedom of Information Act (FOIA). Although many officials are forthcoming and cooperative, others react with hostility against any attempt to enforce accountability. They drag their feet, cite national security, and sometimes use privacy concerns to justify noncompliance.

It can be fascinating to watch the very same players take turns performing roles A and B, without any apparent awareness of irony or inconsistency. Some groups justify this conditional attitude toward information flow by assuming that government will always and automatically be wrong, whether it is trying to open a data spigot or attempting to close one down.

The same pattern can be seen in other areas of modern society. For instance, when a corporation starts spying on its employees, tracking every computer keystroke, timing each phone call, reading everyone’s e-mail, and logging trips to the bathroom, managers justify these actions as essential for efficient conduct of business and to ensure staff accountability. Opponents decry such practices as violating basic human rights, calling for a shutdown of the offensive data flow.

Those same opponents then turn around and file suit to force release of proprietary company documents—for the public good, of course—seeking to widen the particular spigot that they choose.

These issues will all be discussed later. I am not making value judgments at this point, only noting a consistent pattern that will help us explore why we often take one-sided positions, self-righteously demanding far more openness from our opponents than we want applied to ourselves.

Matters of privacy, accountability, and freedom are often judged first and foremost on the basis of whose ox is being gored.

In the following chapters, I use a catch-all phrase, “strong privacy advocates,” to label those who are most outspoken against “transparency.” From the start, let me state that this term oversimplifies a wide range of groups and individuals. For instance, many ACLU members do not share the generalized antipathy toward government that is a common premise of
“cypherpunk” activists like Hal Finney and Tim May. Although liberals and libertarians both see themselves staunchly combating dire threats to freedom, they often find themselves vigilantly facing in opposite directions.

As we’ll see later, the prescriptions proposed by those I put in this camp also cover a wide range. For instance, some groups like the ACLU lobby for new legislation to prevent misuse of private data by corporations and snooping government agencies. This is sometimes called the “European model,” since members of the European Union have been extremely active in setting up rules and regulations to govern who has the right to collect, withhold, or control the use of personal information. At one extreme of this trend are those who demand legal recognition that individuals have a basic right of ownership over any and all data about themselves: no one should be able to use any fact or datum concerning you—not even your name—without your explicit permission.

Supporting a quite different approach are some of the most vivid and original thinkers of the information age. John Gilmore, Esther Dyson, John Perry Barlow, and others on the (roughly) libertarian wing were in the vanguard fighting against both the Clipper proposal and the Communications Decency Act. Seeing little need or value in new laws, they hold that technology will be a key factor in defending liberty during the coming era. Fresh tools of encryption and electronic anonymity will protect individuals against intrusive spying by others, and especially by the state. What they demand, therefore, is that government stand back and not interfere as a myriad anonymous personae and enciphered secrets throng across the dataways.

Taking this attitude to far greater extremes are the “anarcho” libertarians, such as financier Walter Wriston, who take pleasure in predicting a virtual end to all government, opening an age of unbridled and anonymity-shrouded individualism.

Straddling the cypherpunks and lobbyists are some of the newer online privacy groups, for example, EPIC and the Center for Democracy and Technology, which support crypto-technologies while still seeking to influence laws and regulations, a mix that sometimes leaves them seeming to pull in two directions at once. Others, like the Privacy Rights Clearinghouse (PRC), emphasize a strictly pragmatic approach. A book by PRC project director Beth Givens offers copious practical advice about how “little guys” can use today’s legal protections to take some control of their credit ratings, their medical records, or whether their names will proliferate endlessly across countless irritating mailing lists.

This short compilation leaves out many other players, but it is enough to illustrate a single trait shared by all, the belief that modern concerns about freedom and privacy can often be solved by some specific or general reduction in the flow of information, or by making the stream flow in just
one direction. Whether they advocate new laws, technologies, or practical savvy, each would empower people and groups to conceal things. For want of a better term, “strong privacy” will have to do.

In fact, I admire many of these advocates for their intelligence, passion, and concern. We would all be a lot worse off if they weren’t out there, pitching their ideas.

In some cases, they are probably right.
But there is another side to the issue. One that needs to be heard.

**OTHER VOICES**

I am not the only one speaking for transparency, the notion that we may all benefit by carefully increasing two-way information flows. In addition to the names mentioned earlier in this chapter, some others should be noted.

Jack Stack, already a business legend for transforming his manufacturing company from red ink to splendid profitability, hit best-seller lists in the mid-1990s with his book *The Great Game of Business: Unlocking the Power and Profitability of Open-Book Management*, in which he advocates letting all of a company’s employees view the ledgers. By welcoming input and oversight from every level, he claims, managers profit from a much wider pool of criticism and good ideas. This doesn’t mean giving up executive authority, but it does engender in staff at all levels a sense of personal identification with team success—even when the “team” consists of several thousand employees. Stack’s simple argument shrugs aside all theory. He makes no pretensions to ideology. His basis for open-book management is pragmatic. It works in good times, and especially well in hard times. It is a formula for success.

Unfortunately, as we’ll see in chapter 5, it takes maturity and willpower for any kind of authority figure to loosen the reins of control, even when doing so clearly serves the greater good. Despite the popularity of his book, Stack is swimming against powerful currents of human nature.

On the other hand, didn’t I just spend the first half of this chapter implying that transparency is inevitable?

Late in this book, we’ll examine whether any single scenario about tomorrow seems compellingly likely. Personally, I think the jury is still out. But there is one celebrated author who contends that our fate has already been decided. According to cartoonist-humorist Scott Adams, we are destined for a world of universal vision, whether we like it or not. In *The Dilbert Future*, Adams offers a look at the next century that is at once both earnest and biting sardonic. Exploring many of the same themes as this book—for instance, the notion that professional news reporters will be replaced by swarms of amateurs with cameras—Adams takes into account
likely breakthroughs such as ubiquitous video, DNA matching, and cybernetic scent-bloodhounds before reaching the following conclusion:

"In the future, new technology will allow the police to solve 100 percent of all crimes. The bad news is that we'll realize 100 percent of the population are criminals, including the police."

Adams then makes the hilarious extrapolation that every human on the planet will eventually land in jail for minor crimes, except the world's smartest person who, since she was too clever to get caught, must thereafter bear the tax burden of supporting everyone else in prison, forever. Like Mark Twain and other great humorists, Adams uses outrageous exaggeration to raise serious issues—in this case how we may respond when our smallest peccadilloes become public knowledge. Will we become a society of frantic finger-pointers and blamers? Or might we learn to "chill out" when everyone realizes that people who live in glass houses are unwise to cast stones?

At the opposite end of the "seriousness" spectrum from Adams, we find Dartmouth physicist Arthur Kantrowitz and philanthropist-investor George Soros, who have taken up the cause Karl Popper championed a generation ago and are campaigning that an "open society" is healthiest when it lives up to its name. Both men have been vigorous in promoting the notion that free speech and transparency are not only good but absolutely essential for maintaining a free, creative, and vigorous civilization.

Kevin Kelly, executive editor of Wired magazine, expressed the same idea with the gritty clarity of information-age journalism: "The answer to the whole privacy question is more knowledge. More knowledge about who's watching you. More knowledge about the information that flows between us—particularly the meta-information about who knows what and where it's going."

In other words, we may not be able to eliminate the intrusive glare shining on citizens of the next century, but the glare just might be rendered harmless through the application of more light aimed in the other direction. Nor is Kelly alone in this opinion among cyber-era luminaries. Even some of the bright people I labeled earlier as "strong privacy advocates"—Esther Dyson and John Perry Barlow, for instance—have publicly mused that transparency might be preferable, if only it could somehow be made to work. Said Barlow: "I have no secrets myself, and I think that everybody would be a lot happier and safer if they just let everything be known. Then, nobody could use anything against them. But this is not the social norm at the moment."
If transparency is the requisite condition in science, democracy, and free markets, it should come as no surprise that economists—who work at the nexus of all three—find openness appealing. Many economists now lean toward attributing most kinds of injustice, bureaucracy, and societal inefficiency to asymmetric information flows—where one person or group knows something that others don’t. Pick an institution, and these economists will talk about how the structure was chosen in response to some information-related problem. When they examine causes of “market failures” (things that make simple markets handle problems poorly) these experts list uneven knowledge right at the top. Other reasons, such as lack of complete competition, inability to commit, public goods, and externalities, would be relatively easy to fix, via either contracts or politics, if we all had symmetric information.

“In that case,” says Robin Hanson, an economist at the University of California, Berkeley, “we’d each know how much we expect to gain or lose in a change. We could negotiate such changes in ways that made everyone feel better off than before.”

Hanson cites the following familiar problems: war, caused by one side guessing wrong about the other’s power or determination; lack of trade, often due to buyers’ unwillingness to admit how much they want something; going to trial, like war, attributed to misreading what the other side would settle for; law enforcement, costly and overbearing because the police don’t know who did what crimes; status consumerism, buying visible but less valuable goods to show others that we can; the collapse of mutually beneficial negotiations, being afraid that someone else knows something we don’t, and if they agree to a proposal, it must be because it favors them in some way we haven’t realized; monopoly, causing losses because the monopolist can’t discriminate price perfectly and charge each person what it’s worth to them; and rat races, working too hard to convince employers that we really want success. All of these problems arise because of limited or restricted information flows. With improved knowledge on all sides, many governmental and nongovernmental organizations might lose their purpose, lose their constituencies, and possibly fade away.

Caltech professor John O. Ledyard points out that “asymmetric information conveys a monopoly position on the holder of the information that markets cannot easily overcome.”

Although they generally favor transparency, economists warn that information flows should be opened up evenly, lest one side or another gain unfair advantage during the transition—a gradualist approach that is supported throughout this book.

Finally, there are groups and individuals who believe in action, rather than words, and providing the tools of transparency to those who need it
most. For example, the Witness Program donates video equipment and training to human rights groups around the world, from Nigeria, Rwanda, and Bosnia to Guatemala and Haiti. According to Witness cofounder Peter Gabriel, "a camera in the right hands at the right time can be more powerful than tanks or guns. Let truth do the fighting." Other groups concentrate on U.S. inner cities, helping create neighborhood watch programs to combat both crime and unprofessional police practices. Meanwhile, Transparency International fights corruption by promoting open legal and business practices around the world.

All of these efforts are aimed at making things better by increasing, rather than decreasing, the flow of information and forging a path into the future that takes advantage of light, as if the right to see will be as vital tomorrow as the right to bear arms was yesterday. Nevertheless, they would have little chance of success without help from powerful social forces. Chapters 5 and 6 look at some trends in our strange, quirky civilization that lean strongly toward rambunctious openness. If transparency is not "inevitable," at least we are bound for interesting times.

**THE CONCERNS OF NORMAL PEOPLE**

Theory is fine, but in the long run society's course will be determined by regular folks, whose concerns strike close to home. Here are some of the apprehensions expressed by people who have written to me.

Is my boss recovering and reading all my deleted e-mail messages at work? Is my supervisor metering my coffee breaks?

Will my medical records be shared with every insurance company and every employer I submit an application to? Might my neighbors somehow snoop the records of my therapist?

I'm worried about my dossier, kept by some secretive credit bureau. How will reciprocal transparency protect me from the countless databases that already have my name and Social Security number?

Can "openness" ever work both ways—applying equally against the powerful—in a world that's suddenly filled with cameras?

Finally, there is the message I received from one woman reflecting a somewhat different perspective.

I don't care so much about privacy. What have I got to hide that would interest anybody? And even if they did learn everything about me, why should I care? No, what bothers me is the same kinds of things that fret most of the people I know. My family's
safety, with crime all over. Not knowing or having any say in what’s happening each day to my kid in school, if he’s being beaten up or offered drugs. If I’m being robbed by the companies and politicians, or if some maniac is going to swerve around the next corner at ninety and splatter my brains. We live in “gated-community” prisons, afraid of strangers, afraid to let our kids play in the street. Ask me what I’d trade, to have these worries lifted off of me!

All our fancy social speculations won’t matter if we can’t address the concerns of people like this, who feel beleaguered enough to talk about “trading” something for more security, or a little less fear. Later, we’ll talk more about this notion of trade-offs, one of the most insidious, troubling logical fallacies of our day, the widely held idea that danger is a price we all must pay for freedom. For now, let me just say that I won’t exchange my liberty—or anyone else’s—for security. I surely won’t give up essential privacy: of home, hearth, and the intimacy that one shares with just a few.

But that is a far cry from maintaining a so-called right to skulk in shadows and act against others anonymously—a fictitious right that shelters nearly all the predators who make this a wary, suspicious age, fueling both the growth of government and a rising obsession with personal safety.

Suspicions that may snuff out the bright hopes of a coming “infotopia.”

So much for practicing what I preach: letting the reader know what to expect. I’ll close this introductory chapter now with a final thought.

It is hard for recent cave dwellers to transform themselves into smart, honest, and truly independent creatures of light.

For millennia, philosophers have told us we could do it by willing ourselves to behave better, through faith, or by obedience to strict codes of conduct. Those prescriptions never worked well, not all by themselves, and they proved almost useless at thwarting truly malignant men bent on harming others. But now, at last, we seem to have hit on a pragmatic tool more in keeping with our ornery natures.

Accountability.

All right, it still has some kinks to work out. We cave folk are new at this sort of thing—just a few centuries along the road of democracy, and only decades exploring diversity as a paramount virtue.

It’s unclear, as yet, how far this road will take us. Nevertheless, one fact should grow apparent soon.

We’ll all stumble a lot less if we can see where we are going.
THE END OF PHOTOGRAPHY AS PROOF
OF ANYTHING AT ALL

There was once a kingdom where most people could not see. Citizens coped with this cheerfully, for it was a gentle land where familiar chores changed little from day to day.

Furthermore, about one person in a hundred did have eyesight! These specialists took care of jobs like policing, shouting directions, or reporting when something new was going on. The sighted ones weren't superior. They acquired vision by eating a certain type of extremely bitter fruit. Everyone else thanked them for undergoing this sacrifice, and so left the task of seeing to professionals. They went on with their routines, confident in a popular old saying.

"A sighted person never lies."

One of the scariest predictions now circulating is that we are about to leave the era of photographic proof. For generations we relied on cameras to be the fairest of fair witnesses. Images of the Earth from space helped millions become more devoted to its care. Images from Vietnam made countless Americans less gullible and more cynical. Miles of footage taken at Nazi concentration camps confirmed history's greatest crimes. A few seconds of film shot in a Dallas plaza in November 1963 set the boundary conditions for a nation's masochistic habit of scratching a wound that never heals.

Although there have been infamous photographic-fakes—trick pictures that convinced Sir Arthur Conan Doyle there were real "fairies" and Mary
Todd Lincoln that her husband's ghost hovered over her, or the ham-handily doctored images that Soviet leaders used to erase "nonpersons" from official history—for the most part scientists and technicians have been able to expose forgeries by magnifying and revealing the inevitable traces that meddling left behind.

But not anymore, say some experts. We are fast reaching the point where expertly controlled computers can adjust an image, pixel by microscopic pixel, and not leave a clue behind. Much of the impetus comes from Hollywood, where perfect verisimilitude is demanded for on-screen fictions and fabulations like Forrest Gump and Jurassic Park. Yet some thoughtful film wizards worry how these technologies will be used outside the theaters.

"History is kind of a consensual hallucination," said director James Cameron recently. He went on to suggest that people wanting to prove that some event really happened might soon have to track closely the "pedigree" of their photographic evidence, showing they retained possession at all stages, as with blood samples from a crime scene.

---

One day a rumor spread across the kingdom. It suggested that some of the sighted were no longer faithfully telling the complete truth. Shouted directions sometimes sent normal blind people into ditches. Occasional harsh laughter was heard.

Several of the sighted came forward and confessed that things were worse than anyone feared. "Some of us appear to have been lying for quite a while. A few even think it's funny to lead normal blind people astray!"

"This power is a terrible temptation. You will never be able to tell which of us is lying or telling the truth. Even the best of the sighted can no longer be trusted completely."

---

The new technologies of photographic deception have gone commercial. For instance, a new business called Out Takes recently set up shop next to Universal Studios, in Los Angeles, promising to "put you in the movies." For a small fee they will insert your visage in a tête-à-tête with Humphrey Bogart or Marilyn Monroe, exchanging either tense dialogue or a romantic moment. This may seem harmless on the surface, but the long-range possibilities disturb Ken Burns, innovative director of the famed public television series The Civil War. "If everything is possible, then nothing is true. And that, to me, is the abyss we stare into. The only weapon we might have, besides some internal restraint, is skepticism." Skepticism may then further transmute
into cynicism, Burns worries, or else, in the arts, into decadence. To which
NBC reporter Jeff Greenfield added: “Skepticism may itself come with a
very high price. Suppose we can no longer trust the evidence of our own
eyes to know that something momentous, or something horrible, actually
happened?”

There are some technical “fixes” that might help a little—buying special
sealed digital cameras, for instance, that store images with time-stamped
and encrypted watermarks. But as we’ll see in chapter 8, that solution may
be temporary, at best. Nor will it change the basic problem, as photo-
graphy ceases to be our firm anchor in a sea of subjectivity.

This news worried all the blind subjects of the kingdom. Some kept
to their homes. Others banded together in groups, waving sticks
and threatening the sighted, in hopes of ensuring correct informa-
tion. But those who could see just started disguising their voices.

One faction suggested blinding everybody, permanently, in or-
der to be sure of true equality—or else setting fires to shroud the
land in a smoky haze. “No one can bully anybody else, if we’re all
in the dark,” these enthusiasts urged.

As time passed, more people tripped over unexpected objects,
or slipped into gullies, or took a wrong path because some anony-
mous voice shouted “left!” instead of right.

At first, the problem with photography might seem just as devastating to
transparency as to any other social “solution.” If cameras can no longer be
trusted, then what good are they? How can open information flows be used
to enforce accountability on the mighty, if anyone with a computer can
change images at will? A spreading mood of dour pessimism was lately dis-
tilled by Fred Richrten, professor of photography and multimedia at New
York University: “The depth of the problem is so significant that in my opin-
ion it makes, five or ten years down the road, the whole issue of democracy
at question, because how can you have an informed electorate if they don’t
know what to believe and what not to believe?”

Then, one day, a little blind girl had an idea. She called together
everybody in the kingdom and made an announcement.
“I know what to do!” she said.
Sometimes a problem seems vexing, till you realize that you were looking at it the wrong way all along. This is especially true about the "predicament" of doctored photographs and video images. We have fallen into a habit of perceiving pictures as unchanging documents, unique and intrinsically valid in their own right. To have that accustomed validity challenged is unnerving, until you realize that the camera is not a court stenographer, archivist, or notary public. It is an extension of our eyes. Photographs are just another kind of memory.

So cameras can now lie? Photographs can deceive? So what? People have been untrustworthy for a very long time, and we've coped. Not perfectly. But there are ways to deal with liars.

First, remember who fooled you before. Track their credibility, and warn others to beware. "Your basis cannot be looking at the reality of the photograph," says Andrew Lippman, associate director of the Massachusetts Institute of Technology (MIT) Media Lab. "Your basis . . . has to be in the court of trust."

Second, in a world where anyone can bear false witness, try to make damn sure there are lots of witnesses!

. . . .

"Here," said the little girl, pushing bitter fruit under the noses of her parents and friends, who squirmed and made sour faces.

"Eat it," she insisted. "Stop whining about liars and go see for yourselves."

. . . .

In real life, the "bitter fruit" is realizing that we must all share responsibility for keeping an eye on the world. People know that others tell untruths. Even when they sincerely believe their own testimony, it can be twisted by subconscious drives or involuntary misperceptions. Detectives have long grown used to the glaring omissions and bizarre embellishments that often warp eyewitness testimony.

So? Do we shake our heads and announce the end of civilization? Or do we try to cope by bringing in additional testimony? Combing the neighborhood for more and better witnesses.

One shouldn't dismiss or trivialize the severe problems that will arise out of image fakery. Without any doubt there will be deceits, injustices, and terrible slanders. Conspiracy theories will burgeon as never before when fanatics can doctor so-called evidence to support wild claims. Others will fabricate alibis, frame the innocent, or try to cover up crimes. "Every advance in communications has brought with it the danger of misuse," says Jeff Greenfield. "A hundred years ago, publishers brought out books of Abe Lin-
coln’s speeches containing some words he never spoke. Hitler spread hate on the radio. But today’s danger is different."

Greenfield is right. Today is different, because we have the power to make photographic forgery less worrisome.

Because even pathological liars tend not to lie when they face a high probability of getting caught.

Would we be tormenting ourselves over the Kennedy assassination today if fifty cameras had been rolling, instead of just poor Abraham Zaprunder’s? Suppose some passerby had filmed Nazi goons setting fire to the Reichstag in 1933. Might Hitler have been ousted, and thirty million lives saved? Maybe not, but the odds would have been better. In the future, thugs and provocateurs will never know for certain that their sneaking calumny won’t be observed by a bystander or tourist, turning infrared optics toward those scurrying movements in the shadows.

We are all hallucinators to some degree. So now our beloved cameras may also prove faulty and prone to deception? At least they don’t lie except when they are told to. It takes a deliberate act of meddling to alter most images in decisive ways. Cameras don’t have imaginations, though their acuity is improving all the time. In fact, when their fields of view overlap, we can use them to check on each other. Especially if a wide range of people do the viewing and controlling.

As citizens, we shall deal with this problem the way members of an empirical civilization always have, by arguing and comparing notes, giving more credibility to the credible, and relying less on the anonymous or those who were caught lying in the past. Discerning truth, always a messy process, will be made more complex by these new, flawed powers of sight. But our consensual reality does not have to become a nightmare. Not when a majority of people contribute goodwill, openness, and lots of different points of view.

Again, cameras are simply extensions of our eyes.

If you’re worried that some of them are lying, tradition offers an answer: more cameras.

We’ll solve it by giving up the comforting blanket of darkness, opening up these new eyes, and sharing the world with six billion fellow witnesses.