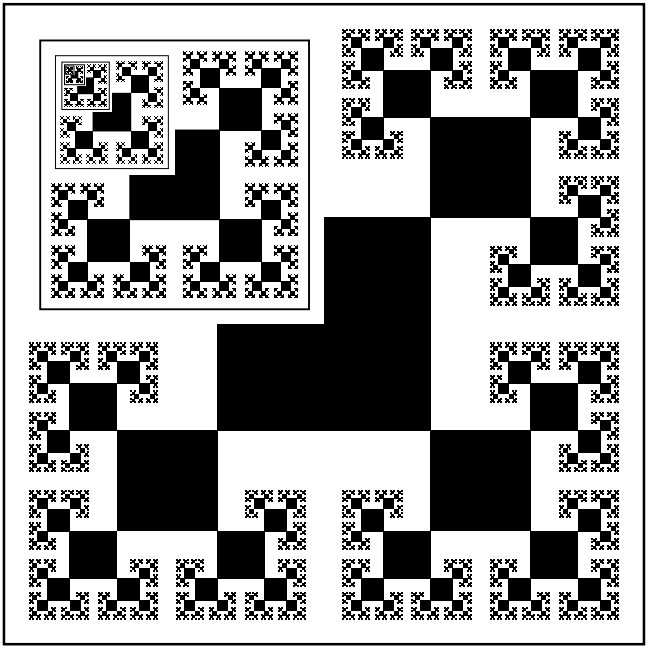
MAKING CRIME IMPOSSIBLE

+

WALDEN 3.0



Also by Neal R. Wagner

WWW: The End of Time
(fiction)

The Laws of Cryptography
(non-fiction)

MAKING CRIME IMPOSSIBLE

Non-Fiction

+

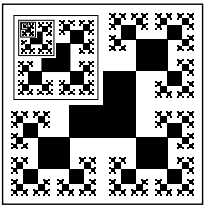
WALDEN 3.0

Fiction

By

NEAL R. WAGNER

Anomie Hollow Press



Making Crime Impossible
Attached novella: Walden 3.0

Published by:
Anomie[1] Hollow Press
(a division of: Telemeister Strategic Services, LLC)
2640 Tam O'Shanter Dr.
El Dorado Hills. CA 95762

Visit us on the Web: `telemeister.com`

Written and designed by:
Neal R. Wagner: `neal.wagner@gmail.com`

Version 0. Date: July 12, 2022. Time: 20:02.
ISBN: 978-0000000000
Library of Congress Control Number: 0000000000
Printed in the United States of America

[1] **anomie** *also* **anomy** *n.* [French *anomie*, from Middle French, from Greek *anomia* ($\alpha\nu o\mu\acute{\iota}\alpha$) lawlessness] a condition[2] in which society provides little moral guidance to individuals; social instability resulting from a breakdown of standards and values; a breakdown of social bonds between an individual and the community; *also* : personal unrest, alienation, and uncertainty that comes from a lack of purpose or ideals.

[2] Popularized by the French sociologist Émile Durkheim[3] in his influential book *Suicide* (1897).

[3] Durkheim maintained that crime is a normal part of any society, necessary and even inevitable.

To my parents:

ALBERTA RUTH HETZER
18 December 1908 – 20 August 1997

RALPH RICHARD WAGNER
12 July 1907 – 23 June 1967

A Golden Age, whether of art or music or science or peace or plenty, is out of reach of our economic and governmental techniques. Something may be done by accident, as it has from time to time in the past, but not by deliberate intent. At this very moment enormous numbers of intelligent men and women of good will are trying to build a better world. But problems are born faster than they can be solved. Our civilization is running away like a frightened horse, her flanks flashing with sweat, her nostrils breathing a frothy mist; and as she runs, her speed and her panic increase together. As for your politicians, your professors, your writers—let them wave their arms and shout as wildly as they will. They can't bring the frantic beast under control.

—B. F. Skinner, *Walden Two,* Macmillan, 1948, Chapter 11.

If you wish to build a society in which individuals cooperate generously and unselfishly towards a common good, you will get little help from genes and evolution. Let us teach *them generosity and altruism, for we cannot expect it to be part of their biological nature.* [Reworded.]

—R. Dawkins, *The Selfish Gene,* Oxford, 1976, 2006, 30th Ann. Ed., pp. ix, 3, 139.

Combined Contents[1]

Making Crime Impossible
(Non-fiction)

Walden 3.0
(Fiction)

[1] Chapters with the same number have similar topics.

Preface

[Based on twelve global environmental problems from Chapter 1.] *Our world society is on a non-sustainable course, and any one of these problems . . . would suffice to limit our lifestyle within the next several decades. They are like time bombs with fuses of less than 50 years. . . . [they]* will *get resolved, in one way or another, within the lifetimes of [the young] alive today. The only question is whether they will become resolved in pleasant ways of our own choice, or in unpleasant ways not of our choice, such as warfare, genocide, starvation, disease epidemics, and collapses of societies.*

—J. Diamond, *Collapse: How Societies Choose to Fail or Succeed*, Penguin, 2006, 2011, p. 498.

. . . it is not difficult to demonstrate a connection between the unlimited right of an individual to pursue happiness and the catastrophes threatened by unchecked breeding, the unrestrained affluence which exhausts resources and pollutes the environment, and the imminence of nuclear war.

—B. F. Skinner, *Beyond Freedom and Dignity,* Knopf, 1971, p. 213.

During a computer ethics course that my friend Myles McNally and I were teaching, he mentioned the phrase "What if crime were impossible?" It struck me as profound—these were magic words, words of power. I imagined societies that didn't have to worry about crime. In this book I propose to use technology, especially computer technology, to eliminate crime in some cases and reduce it in others.

This same computer technology can provide other benefits, too: open access to information in public and privacy of information in

our own private space. Hand-in-hand with this openness is the gathering and logging of information about public activities, for one must possess the information in order to provide it.

I picture privacy of communications between individuals who desire such privacy and privacy of their private stored data. They should also have personal privacy in their own private space, as well as *empowered* free speech, making it easy to contact any individual or group desiring such contact, easy to start a discussion group, easy to let others know about important events. In exchange, I expect much more direct and indirect control, limiting individuals' freedom.

At the outset one must realize that it's not possible to eliminate all crime. We are always going to have the mentally ill or challenged, the angry, greedy, immature, or impulsive. As one example, young boys often have a fascination with starting fires. It is also unrealistic to imagine that we will eliminate all the difficulties and inequities that lead to crime. But this situation is interesting here because the sociologist Émile Durkheim put forward theories maintaining that crime must be present in every society and actually is essential, even beneficial. Think about Thoreau's civil disobedience, or the "crime" of mixed-race marriages. Durkheim was talking about deviations from the morals of a given society, not about crimes for profit, crimes of greed, of violence. Durkheim popularized the use of the word "anomie" to describe a society that no longer helps and guides its citizens.[1] These issues are beyond the scope of this book, but are of interest, as societal anxieties are greatly enhanced in today's more stressful world.

Utopian Communities.

The word "utopia" is used for a society that is much better than others, perhaps even perfect. Imagined utopias have been in literature and philosophy for all of history, starting at least with Plato's *Republic*. Such fictional utopias have given rise to small experimental societies, often trying to improve some aspects of their citizens' lives.

In the first part of this book I focus on computer technology that

[1] Our press name uses this word—see the copyright page for a definition.

could be the basis for a version of a utopia. The second, fictional part of this book presents such an imagined utopia.

Walden, by H. D. Thoreau.

Henry David Thoreau's work *Walden* is a major piece of American literature and philosophy. In 1845 he moved into a remote cabin he had built himself on the shore of Walden Pond, beginning a nearly two-year experiment in living a simpler life. Over the course of the next decade he wrote of his experiences from a journal he had kept.

Though he lived alone, he was not a hermit and often walked into the nearby town of Concord, often had visitors. Instead he proved that it was possible for a man to live by himself with great simplicity. In addition to representing individualism and simplicity of life, Thoreau is known for his use of civil disobedience in opposing slavery before the Civil War.

Thoreau's masterpiece is of special interest here because of the next item below.

Walden Two, by B. F. Skinner.

In 1948 a young Harvard professor wrote a novel about a fictional utopian society based on "behavioral engineering," using psychological conditioning to make people happy and productive. In the early 1960s the book became very popular, especially at universities, although it was vilified by many academics. By 1970, over 2 million copies had sold. Skinner's book is still in print but not nearly as popular now as it was. He named the book after *Walden* because he felt he was providing for a whole group of people the benefits that Thoreau had enjoyed by himself.

Skinner was a skillful writer who painted an elegant picture of his utopia, with few problems and no dissent. In fact, Skinner's utopia had a single leader who created the society and set the controls for it in place. Problems of leadership and control were hardly addressed.

Later, several actual experimental communities were partly modeled after his fictional one, with modest success—two have survived long-term. However, many of Skinner's ideas were not practical and

his methods over-simplified. The imagined success of his society was too optimistic because these ideas and methods did not easily translate to success in an actual community. In particular, the problem of leadership proved difficult, as many people wanted to be the leader.

B. F. Skinner had a long career as the leading behaviorist psychologist of his time. He has been called "a pioneer of modern behaviorism," and "the most influential psychologist of the 20th century." He taught us to think before using terms like "free will" or "freedom" and to realize how much of our nature and behavior is determined by our environment.

His best-known book, written late in his career, is *Beyond Freedom and Dignity*, in which he maintained that in order for humanity to survive as a species, it must give up its freedom, which for him was always just an illusion anyway. Notice that the date of the quotation from Skinner at the start of this preface is almost fifty years before the present book's copyright date, while his concerns are far more pressing today than when he wrote.

Walden 3.0, the second (fictional) part of this book.

This tells of a fictional community of my own devising, using many techniques from the first (non-fiction) part of this book. Each chapter partly covers topics from the chapter with the same number in the non-fiction part. (The Table of Contents emphasizes this correspondence.)

I am not suggesting that techniques from the earlier part of this book would solve all problems in my imagined society. This society needs and uses many other methods that human beings have developed to handle problems, to get along with one another, such as those from religion, philosophy, medicine, education, management, and many other fields.

I am trying to present this approach to a community as a reasonable one, but still I have characters making pointed criticisms of the ideas. Skinner's book also has fictional critics, but they are mostly straw men.

This Book's Emphasis.

At first glance, this book would seem to emphasize those technologies and techniques which would enable the creation of a special kind of utopia, one illustrated by the small town in the second fictional part of the book. Such technologies would indeed be very useful in the organization of such a town. But the same technologies should scale up to an arbitrarily large city, to a country, and to the whole world. For me it is much more important to imagine the technologies used to deal with a number of unprecedented challenges we face in the twenty-first century. I suggest exerting a greater degree of control over the entire global population, as I think we can no longer afford to let people behave just as they please.

Following Skinner's quote at the beginning of this preface, if our civilization is to survive, it must devise ways to control the issues he mentions as well as many others. The notion of unrestrained individual freedom of action is a poison that is ruining our world.

This individual freedom is partly driven by a global capitalism that itself is increasingly less restricted, now more than ever emphasizing profits to shareholders and avoiding any other responsibilities. Capitalism provides a savagely efficient exploitation of resources, both natural and human, and all at a time of global crisis due in part to such unrestrained exploitation. Globalization is causing ever-increasing harm, as with successful goods being those produced most cheaply, and often produced without regard to any ethical standard, whether for the workers or for the environment or for anything else not related to profit.

Anti-Utopias and Control.

Modern fiction is filled with dystopias (anti-utopias), which are perfectly bad instead of perfect. By far the most important are the classic books *Brave New World*, written by Aldous Huxley in 1932, and *Nineteen Eighty-Four*, by George Orwell in 1949. In both books the stability of civilization was a goal (the "primal and ultimate need" in the case of Brave New World) and both also envisioned absolute control of the population. These books are like bookends on a row

of ways to control a society. At one end is Huxley making everyone happy using psychological conditioning and drugs, so no one wanted to rebel, while at the other end is Orwell using constant surveilance and even control of thoughts with an artificial simple language:

> Don't you see that the whole aim of Newspeak is to narrow the range of thought? In the end we shall make thoughtcrime literally impossible, because there will be no words in which to express it.

I am proposing much more control, but what to control and how to do the controlling is the great challenge for our civilization, a challenge that mankind has not met.

The Coronovirus Pandemic.

Society is now recovering from a terrible pandemic, the effects of which will be around indefinitely. This has been a tremendous challenge for the whole world, causing so much catastrophic harm to so many people and institutions that I won't bother with a list here. I don't want to discount all these recent horrific difficulties, but our response has been remarkedly poor and flawed, especially in the United States where I am writing.

I see this pandemic as a type of dress rehearsal for a host of other problems, some current and others on the horizon. The pandemic's challenges and society's responses illustrate how ill-prepared the world is for inevitable future problems. Such problems could include another pandemic, or some other crisis based on the many vulnerabilities discussed in the first chapter of this book.

Across the world, the demand by many individuals for their individual freedoms, as they preceive them, has greatly exacerbated the past and continuing damage caused by the pandemic. Thus it amounts to a clear demonstration of the many future difficulties we will inevitably face.

Limits of Optimism and of Pessimism.

The quotations at the start of this Preface, along with the recent pandemic, set a clear pessimistic tone that is continued elsewhere in this

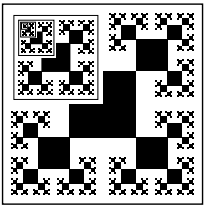
book. Nevertheless, pessimism alone can lead to a defeatist attitude that is not helpful. No matter how problematic and challenging we humans perceive our future, we still need to engineer the best outcome we can during difficult and often deteriorating circumstances. Such pessimism can and ought to be a strong motivator as we work to improve our long-term outcome as a species.

On the other hand, what I consider unfounded optimism is common across the world. Many people believe that our science and engineering skills will bail us out as they often have in the past. This only makes sense if there are specific actions and tools that could mitigate our problems. In this book I am trying to do just that: recommend posible actions and suggest a way forward. Today's optimists usually have no basis for expecting reasonable solutions to our manifold problems. Some optimists are handycaped by ignorance even of the basic science involved. They may feel that it is our destiny to prevail, or that a higher power will intervene on our behalf. These attitudes are one more reason for pessimism. There are also optimists who believe in a far-fetched scientific rescue, such as space colonization or massive geo-engineering projects. Others believe in efficiency improvements in all our activities, and while efficiencies are welcome, by themselves they will at most stave off the reckoning that foolish past and continuing actions are leading us toward.

San Antonio, 2021

MAKING CRIME IMPOSSIBLE

Non-Fiction



Contents[1]

Making Crime Impossible
(Non-fiction)

[1] Topics in the non-fiction chapters correspond to those with the same chapter number in the fiction. The page number of each corresponding fiction chapter is given in parentheses at the right above.

1. Introduction
A Vulnerable Civilization

Our culture has produced the science and technology it needs to save itself. It has the wealth needed for effective action. It has a concern for its own future. But if it continues to take freedom and dignity, rather than its own survival, as its principal value then some other culture may make a greater contribution to the future.

—B. F. Skinner, *Beyond Freedom and Dignity,* Knopf, 1971, p. 181.

Here are four conclusions about the world of climate change:

- *This thing is coming at us a whole lot faster than publicly acknowledged.*
- *All the stuff about changing the light bulbs and driving less is practically irrelevant to the outcome of this crisis.*
- *It is unrealistic to believe that we are going to make [all the various] deadlines. It's too late now.*
- *For every degree that average global temperature rises, so do the mass movements of population, the number of failed and failing states, and very probably the incidence of internal and international wars.*

—Gwynne Dyer, *Climate Wars: The Fight for Survival as the World Overheats,* Oneworld, 2010, pp. xiii–xiv.

Our civilization has a number of disturbing vulnerabilities. In time these will likely produce worldwide population and economic collapses—much worse than the recent pandemic. The outcome is potentially existential, up to our survival as a species. This level of danger has never before been present in our history. Ironically,

some of the problems are caused by incredible advances in science and technology, just where I hope we may find partial solutions.

Vulnerabilities.

First is my list of *causes* of vulnerabilities. These are all negatives. Many positives also exist, highlighted in this book. In particular, of the human nature negatives given below, many might be thought of as male traits, though they are not limited to males. Human nature also includes a large collection of positive traits.

Causes of our Vulnerabilities

- ✪ Capitalism and globalization, extreme exploitation of resources.
- ✪ Growth economics, requiring steady growth and consumption.
- ✪ Absence of limits to population growth, since this absence is in effect essential for economic growth.
- • Advances in science and technology, enabling the exploitation and consumption.
- • An initial world with abundant and exploitable natural resources, but in fact a finite world with finite resources.
- ✪ Waste of non-renewable resources, unwilling to recycle fully.
- ✪ Unequal distribution of economic wealth.
- ✪ Unequal education, particularly of women and the poor.
- ✪ Vulnerable, unnecessary, overlarge construction: buildings, homes, dams, landfills, vehicles, highways, airports, satellites.
- • Natural disasters: earthquakes, meteor strikes, solar flares, vulcanic eruptions, pandemics.
- • Dependence on technology: computers, bioengineering.
- ✪ Negative human traits related to human biological nature:
  - drive to conquer and dominate, aggressiveness,
  - drive to reproduce, with a focus on welfare of offspring,
  - drive to accumulate, own and display, hoard,
  - capacity for self-deception and self-delusion,
  - anti-intellectual and anti-scientific attitudes,
  - tribal nature, distrust of strangers outside the tribe,
  - selfishness, lack of concern for others, jealousy of others,
  - willingness to follow a leader, desire to be the leader, and
  - focus on the immediate and short-term.

Each of the items above that are marked with a star (✪) should be

remediated and eventually somehow eliminated. This is not a realistic short-term goal, but it is a serious one. If we could exchange capitalism for a more species-oriented government, like for example some form of socialism, we might be able at least to mitigate all the other starred items at the same time. It is discouraging that the terrible experience of the coronavirus pandemic only brought forth a desire to get the old capitalist economy working again.

Next I give a list of twelve environmental threats partly caused by the above items. This is an edited version of the list given by Jared Diamond in his 2006 book *Collapse*. The first quotation in the Preface referred to this list. Mitigating the earlier causes would help lessen the threats below.

Global Environmental Threats

Destruction or loses of natural resources, especially:

(1) habitat destruction (forests, wetlands, reefs, oceans),
(2) overfishing, overhunting, and overmining (rare earths and many others, effects of ordinary mining),
(3) biodiversity loses (including animals, plants, bacteria), and
(4) soil problems (erosion, salinization, soil fertility losses).

Shortages of many things, but especially:

(5) energy shortages (including uses of non-renewable resources and of the earth's finite photosynthetic capacity),
(6) water shortages and management (aquifer depletion), and
(7) shortages of almost every resource (minerals, chemicals, fuels, building materials, food, fertilizer).

Harmful things introduced—very many items, but especially:

(8) undesirables (chemicals, plastics, radioactive waste),
(9) non-native or new species (plants, animals, new and evolved diseases, epidemics and pandemics), and
(10) greenhouse gases (causing climate change, other harm).

Human population issues:

(11) human population growth, and
(12) increased per-capita impact of humans.

The problems are intertwined and linked, so that energy and water have major effects on one another; pollution and overpopulation affect everything and are major causes of climate change. Fossil fuels

for energy produce greenhouse gases. Climate change will continue to worsen all the other problems, and in fact directly or indirectly each problem is bad for all the others.

While some local progress is taking place, on average every one of the above problems (and others not on this list) are getting worse; in most cases the problematic levels (whether an excess or a shortfall) are getting worse exponentially. Collectively and individually, the societies of the world will not undertake to implement even proposed approaches to these problems. In particular, it is becoming ever more clear that the many problems related to climate change have no "solution," but only means for coping with them.

Finally, here are several terrible consequences from the problems listed above, but many others could be given. All these items are getting worse right now and will almost surely continue to worsen inexorably:

Consequences of the Problems

- *Diamond's consequences (quote in Preface):* warfare, genocide, starvation, disease epidemics, and collapses of societies.
- *Environmental:* rising oceans, extreme weather (droughts, floods, storms, heat), melting glaciers, thawing permafrost, release of greenhouse gases and other toxic materials.
- *Plagues:* Epidemics of life forms in addition to diseases.
- *Lack of access to essential resources:* clean water, energy, building materials, protection from weather, housing, food.
- *Increases in other common problems:* crime, refugees, slaves and slave labor, despotic and corrupt governments, gangs.
- *Health problems:* harmful drugs, no medical care, medicines not effective, physical and mental stunting, exposure to poisons.
- *Mental health problems:* depression, anxiety, suicide, insanity, mass hysteria, mass suicide.
- *Losses of . . . :* knowledge, art, culture, skills, traditions, a beautiful and bountiful earth.

In addition, the five natural disaster vulnerabilities given earlier (earthquakes, meteors, flares, vulcanos, pandemics) could have significant consequences. Of course we are in the midst of the Coronavirus pandemic and may suffer indefinitely from its lingering effects.

Of the five disasters listed, a pandemic was by far the most likely to cause a planet-wide disturbance in the near future, as this one has done. And yet another pandemic is still the most likely next large disaster. Each of the five would have worse consequences because of our vulnerabilites and threats, especially overpopulation.

Earthquakes and pandemics are interesting because they each could partly have humans to blame for their occurence: some earthquakes caused by fraking or dams, and the recent pandemic perhaps caused by working with (and consuming) bats in China. Earthquakes and meteor strikes can cause ocean tsunamis, and destruction from these is partly limited by early warning detectors. Astronomers now monitor for possible future meteor stikes, with the chance of an intervention. Solar flares have been bothersome, but by far the largest recorded one came in 1859, causing many telegraph systems to fail. This was before other electrical systems were in place. A similar storm today could cause catastrophic problems with the electric grid and satellites, and it might destroy many computer chips. As an act of war, a high-altitude nuclear explosion could also destroy vulnerable chips, making cars and many other devices unusable until their electronic components were replaced. This is a case where the presence of technology could make a natural disaster much worse.

Many people experience food shortages today, although this problem is made much worse by poor food distribution, spoilage, and insistence on food with a high environmental impact. For example, given an amount of feed for beef stock, the weight of edible beef produced is as little as four percent of the total weight of the feed.

The computer revolution itself has introduced many new problems, and this trend is also accelerating. The current favorite technology is artificial intelligence (AI), which is producing astonishing software to improve our lives, yet is likely to be equally important in warfare.

The techniques in this book mostly amount to local coping strategies for these problems, but sometimes there are solutions. These same techniques will enable the greater control that will have to be in place sooner or later.

Out of Control.

In 1995, Kevin Kelly wrote a book titled: *Out of Control*. One brief statement by a reviewer was: "The main premise of the book is the idea of intelligent beings, in this case humans, giving up control of their creations, which are machines, and letting them 'adapt on their own, evolve in their own direction, and grow without human oversight.'" Kelly's book is full of worthwhile and interesting ideas, especially about biological systems, but he was not talking about the complete absence of control. Instead, he was referring to implicit or evolved control, particularly control from below.

A most horrifying science fiction scenario is for mankind to create so-called *lethal autonomous weapons* (LAWs) and let them evolve on their own. What could go wrong with that?

I want to use the reviewer's quote as a metaphor for the terrible processes going on in our world. Everywhere I see harmful events taking place with no reasonable oversight or control. A list of such events partly mirrors the list of problems and consequences in the previous section: an amazing waste of global resources, frantic depletion of these same resources, lack of population control and often the encouragement of its growth, the overpricing of goods such as pharmaceuticals, environmental destruction for profit. Again an endless list. At the extreme end mankind is creating new biological organisms and new AI machines.

As one specific example, consider the oil and gas industry in Texas. Before the coronavirus pandemic, companies used fracking to extract oil from the ground in uprecedented amounts, at a time when our society ought to leave all remaining oil where it is. Natural gas comes out along with the oil, and laws in Texas require that the gas be captured and saved as another energy source. Companies are allowed to request exceptions to the law when no pipelines are available to transport this gas. State regulators have routinely given tens of thousands of such exceptions, and no exception has ever been denied. Every day, billions of cubic feet of the gas are flared (burned). Worse, the flaring is not a clean burn, but generates pollluting nitrogen compounds. Even when pipelines are available, companies

successfully ask for an exception because capturing the gas will cut back on profits. Also the wells routinely and illegally leak into the air large amounts of natural gas, which is mostly methane, the most potent of the greenhouse gases. An oil company needs sand and water for fracking, and the procurement of these, along with the wells themselves, leaves an environmental mess behind that the company is not required to clean up. The companies often skirt legality in operations or are actively fraudulant, cheating investors and the public. The oil-producing lands go through difficult "boon and bust" cycles, with local roads ruined by heavy equipment. I emphasize that this is just an incomplete description of one of many examples.

Climate change becomes the most important example of all, mired as it already is in the midst of many positive feedback loops and completely out of control.

In summary, I propose to monitor for undesireable activities that are out of control and to deter them, preferably to control them, perhaps to eliminate them. The idea of "first monitor, then control" is a prototype for my approach to problems. Chapter 2 elaborates on this issue.

Crimes.

In this book, I use the word "crime" in the widest sense, not just for unlawful actions, but for all manner of undesirable activities. For convenience I include events that have nothing to do with mankind, such as natural disasters. For these last "crimes" the "perpetrator" could be random chance or "Mother Nature." I also want to classify crimes according to their *scale*: how large the crime is, how many people or entities are affected.

Small-scale Crimes. The perpetrators are individuals or entities, or small groups of these. Also single companies or other entities, or groups of these. But the scale is not large. I divide these crimes into seven categories, according to the outcome. Arranged in a rough order increasingly bad for the criminal and good for society, my categories are:

(1) *Crime undetected:* No one knows the crime occurred.
(2) *Perpetrator undetected:* Only the perpetrator knows who did it.
(3) *No punishment:* The perpetrator is known, but no one is willing or able to do anything about it.
(4) *Punishment:* One punishes the perpetrator after the fact.
(5) *Deterrence:* One deters the perpetrator, perhaps by fear of punishment.
(6) *Physically impossible:* One arranges things physically so that the crime is impossible.
(7) *Behaviorally impossible:* One uses upbringing, education, conditioning, and other methods, so that a would-be perpetrator does not want to commit crimes or does not think about them.

This book's title calls for category 6, with category 7 as a long-term goal, though many of the proposals are in category 5—using fear of detection to deter. Current society is mostly stuck in categories 2 through 5. Category 1 is also common, engendering efforts by society to detect these crimes. Much depends on the implementation of categories 6 and 7. Certain forms of physical impossibility might lead an individual to forget the activity, achieving category 7 after a fashion, but other forms could lead to increasing frustration and an eventual blowup. Surely moral education, conditioning or some other direct method to reach category 7 would be preferable, but such behavioral modification interferes with the "freedom" that people prize. Notice that for dangerous individuals, society already uses the costly and inefficient method of imprisonment to try to achieve category 6, and it is often ineffective. Society can and must do far better, and computer technology can help.

Large-scale Crimes Against the Planet. The difference here is that the scale affects a large portion of the planet. The earlier list of challenges includes many crimes of this type. A criminal element might deliberately cause or exacerbate one of those problems on a large scale, as for example causing widespread environmental problems, widespread shortages, and many other possibilities. The largest and most prominent crime in this category is human-caused

climate change, caused directly or indirectly by most of the population. Climate change itself is the result of many other crimes against the planet.

Large-scale Crimes Against Humanity. Historically these have been the worst crimes. Governments commit crimes against their citizens and against others. Criminal elements force people to become refugees or slaves, start wars, or kill on a large scale. In order to increase profits companies deliberately produce substandard or defective items for use or consumption. Throughout history, there have been horrible examples of genocide and destruction of culture, but even removing or denying the right of privacy is such a crime. The largest, most prominent crime in this category is the unchecked breeding by humans that causes overpopulation.

Technology gives society possibilities not previously imagined for eliminating many of the above crimes. The small-scale crimes are clearly much easier to attack, but widely disseminated similar small-scale crimes look like uncoordinated large-scale crimes. There is no clear dividing line.

Many large crimes come from furthering the goals of capitalism.

Preventing Crimes.

Even if the goal is to make crime impossible, society must often be content with reducing or deterring crime, rather than eliminating it. A list of general methods for dealing with crimes partly parallels the list in the previous section.

Detect the crime before or during its commission. It may be possible to stop the crime before it is even started or before it is completed, so in some cases there might be no crime. For example, it's important to identify the "crime" of an oil leak, even one unrelated to human activity.

Detect the crime after its commission, without identifying the criminal. This level is important in many cases: If an illegal logging operation cuts trees, nothing will be done unless society learns about the felled trees. This example illustrates this book's emphasis

on open access to information, since knowing about a crime is the first step, and often the crucial step, toward preventing it.

Detect the crime after the fact and identify the criminal. In this way society can prevent a repetition of the crime by the same individual or entity. As a bonus, the existence of such detection mechanisms may deter criminals.

Create "crime-proof" objects. Change objects that might be used for crimes or might be the target of a crime so that the objects will not function in committing the crime. For example, a variety of techniques could restrict the use of a gun to its owner, and prevent its use in certain circumstances or locations. A number of technologies will ensure that a stolen object no longer functions after its theft.

Remove or eliminate objects used to commit crimes. Thus society would keep guns from muggers and spray paint cans from graffiti vandals. Society uses various limited versions of this strategy, but much more is possible.

Remove the motive for the crime. There are many complex and subtle approaches. Society could in theory use education, the instillation of morals, or other means to raise individuals who do not think about crime or do not want to commit crimes. With the desperate poor who commit crimes to survive, society could again in theory improve the lives of these poor. As above, one could remove the motive for theft by constructing objects that no longer function when stolen.

Make the crime non-existent or meaningless. Certain changes to society would eliminate the context for a former crime. For example, counterfeiters are fond of printing ever better fake U.S. $100 bills, so society must keep adding security features. But a better approach would eliminate paper money, so that there is no crime of physical counterfeiting.

The Issue of Control.

For most of the small-scale crimes, and some large-scale ones like pollution, control itself is not an important issue. The criminal entity can be charged with a formal crime and control of the situation maintained. In contrast, for many large-scale crimes, control is the main issue. These include: run-away population growth, organized crime,

riots, crimes by multi-national corporations or by nation states, unrestrained affluence, large terrorist organizations, actions by one state against another, and so forth. As before, the list is endless, but it has climate change as its most important entry. Mostly the world has not been able to gain even partial control over these issues and similar ones, yet without control the global society faces a terrifying future. This book discusses tools that should help with control. Unfortunately it is often difficult to imagine effective control at present.

It is a cruel reality, but most large-scale issues will not be controlled until a worldwide economic collapse later in this century. There seems to be no way to get action or agreement. Even partial progress would help.

Freedom Versus Control.

One way to define "freedom" is "to do what one wants." With this view of freedom, it is opposed to control. People imagine they want freedom in order to be happy. But happiness by itself is not a desirable goal, nor even a worthy one, with a key issue being the phrase "by itself."

Consider a child or a dog raised with total freedom. allowed to do anything they want, with no control. This is not what one should want and will not lead to happiness. Instead the child or dog wants discipline, which is self-control. They want a sense of purpose, of accomplishment. They want the control and limitations that are necessary for happiness. Instead of total freedom, one needs the limitation of choices. All this is accomplished by rewarding the desired behavior, and by providing and suggesting good choices. And who decides what is good and desired? Again with children or dogs, it is the teacher or parents, or else for dogs the trainer who decides. In the case of adults, society should decide.

It is possible to develop ideologies of worthiness and higher goals, including most especially the survival of humans as a species. This final goal absolutely conficts with the idea of doing just what one wants.

Public Versus Private Space.

Individuals on both sides of the privacy debate see society's options as a *choice* between developing technologies for surveillance and developing those for privacy. Society should employ *both* technologies, with wide and open surveillance in public space and absolute privacy in private space.

For this reason, everyone needs a clearly-defined, inviolate private space, both physical and electronic. The electronic version might be distributed, but it should be just as secure as if it were in the person's private physical space. Everything outside private space is in public space.

Chapter 5 gives more complete definitions of private and public space, but briefly, private space includes the contents of ordinary and electronic mail, as well as one's own home and the activities inside. Public space includes any activities where strangers are permitted, along with any actions involving hazardous materials, the identity of anyone taking public transportation, and the fact that mail was sent (when, from whom, and to whom).

Many people immediately dislike plans for extensive surveillance in public space. They might envision a camera in every public toilet, checking for those who do not flush after each use, so they can be fined or jailed. In fact, there should be cameras and microphones in public toilets, to protect against robberies, assaults, and vandalism. Right now most societies have no fine for "failure to flush," but a decision about such fines is independent of decisions about surveillance. A person facing an assault in a public toilet will not be worrying about fines. Of course in this book I want to make failure to flush into a non-crime, using the now-common sensor on toilets that will detect that a user has departed and flush automatically.

The U.S. is moving toward small, private communities that use guards and gates to restrict access. This version of security and privacy for the wealthy is obscene, the opposite of what society ought to do, a perversion of attempts to head toward a safe and open environment. In this vision of the future, the poor are stuck with wretched lives of degradation and crime, while the wealthy buy what security

they can—an illusion of security that fails when they leave their protected communities, and even fails inside, as they try to keep crime out and try to hire honest guards.

There is a tradeoff between security and privacy. This book suggests trading most privacy in the public arena, outside one's own personal space, for additional safety and security, using advanced computer technology. At the same time the technology will enhance not only personal privacy, but also add to the knowledge of public activities carried out by other individuals and groups. Finally, the technology will support free speech, planning, education, and other important human activities.

Outline of Approaches.

Here is a breakdown of the uses of computer technology that I advocate in this book into four categories, plus a fifth "misuses" category.

Identification (Chapter 3) of individuals and objects and even of data. The goal is to distinguish one object from another and to identify owners of objects. Then if an object is stolen or misused, authorities can determine its status and trace it back to its original owner. This will not usually make the theft or misuse impossible, but will catch perpetrators after the fact, acting as a deterrent. Included is also the important *Identity Verification.*

Tracking (Chapters 2, 4, and 5), of individuals, of vehicles, and of many other objects, including dangerous objects and abstractions like telephone calls or electronic money. Surveillance in public will identify and track individuals and objects, with the resulting data logged into computer systems. In the event of a crime and with a court order, the proper authorities can retrieve logged data about specific people or objects to help solve the crime. Computers will exchange and coordinate data about similar but geographically distributed crimes. Here again, instead making crime impossible, these uses more often make it impossible to get away with the crime or to continue with similar crimes.

Privacy (Chapter 6), of communications and of stored data. Here potent cryptographic techniques help equalize the discrepancy of

power between an individual and corporations or governments, making it harder for either one to commit crimes against a person.

Applications support (Chapters 7, 8, 10, and 11) is a catch-all category giving additional techniques, including support for open access to information, and for education, health-care, and planning. Such open access is the key capability, but of course it also only makes crime more difficult, and not impossible. One promising area is the crime-proof hardware mentioned earlier: objects that will not work when stolen, or that cannot be stolen or misused, directly making crime impossible in these cases.

Misuse (Chapter 9) of technology is a final giant category causing problems on an ever-increasing scale. I devote an entire chapter to this discouraging subject.

Summary.

This is not a book about technological fixes supplied by computers. Instead the book explores the use of computers to improve old-fashioned solutions to problems. As mentioned in the Preface, the ideas rest on three foundations:

- open access to information about public activities,
- empowered free speech, and
- privacy of private activities.

In exchange for these advantages, individuals and other entities should expect:

- no privacy in public space,
- surveillance in all public areas, and
- increased control of permitted actions.

Openness and free speech are powerful weapons against all crimes, but especially the worst crimes, the crimes against humanity. If everyone learns about public activities, then the large crimes, by businesses and governments, and even by individuals, become more difficult. Free speech promotes this openness and so is an integral part of it. Thus openness and free speech complement one another,

but they can be at odds with privacy. The information one person openly obtains or openly distributes may be personal and private to another individual. This is the reason for such a careful line between public and private space. There must be guaranteed privacy inside private space, while there has never been true privacy inside public space—only *de facto* privacy, except for those with the resources to monitor the public space. On the other hand, confidence in the privacy of communications promotes openness and free speech at least for the communicating parties.

All these changes will not take place automatically, but will require planning, especially long-term planning. The technology of planning has improved greatly, since computers can keep track of everything quantifiable and can simulate the effects of choices. The computers are now essential because of the complexity of the modern world. These proposals only make sense in a world that uses computer-supported planning.

Consider also the problem of control. I do not believe in true autonomous individuals. Everyone is partly controlled by heredity and environment. And I have no desire for "control" in the crass sense, though I would certainly like for people to feel the old-fashioned controls of etiquette and conscience—a desire to behave well. Nevertheless, society should not tell people what to do and what not to do, but should just keep track of what they are doing in public, making this information available, sometimes only available under court order. Then it should limit the gathering of such information by any but the proper agencies. Instead of direct control, one should arrange the world so that people cannot commit various destructive acts. And one should arrange education so that people do not want to carry out these destructive activities.

There are limits to these proposals. The direct use of computer technology to make crime impossible falls short—is no ultimate solution—for several reasons. This is gadgetry used to prevent crimes that people would still like to commit; preventing the crime is not a worthy final goal. This prevention is a matter of getting a handle on crime, to control societies increasingly out of control. And the expanded use of computer technology must itself be tightly controlled

to prevent abuses of the same technology.

In addition, the law is flawed, so that each country's definition of crime is also flawed. "Preventing crime" can actually involve enforcing unjust or undesirable laws—even supporting dictatorships. Thus illegal acts are not the same as immoral or unethical ones; the present book is also concerned with preventing the latter actions.

One can also ask about people who feel that laws can be routinely broken if they can get away with it. What if they were forced (somehow) to obey every law strictly? Many societies, including especially the U.S., have a tradition of selectively obeying the law. People with such an attitude would be particularly nervous about societal changes to make crime actually impossible. Arbitrary or unreasonable laws should be changed or revoked, rather than broken.

Many techniques in this book only detect a crime during its commission or afterward, to identify the criminal and act as a deterrent. But if society does not have the will to rehabilitate or failing that to punish the criminals, they are not likely to stop their activities. Detecting environmental pollution does not help if no one will stop the polluter. And consider impulsive crimes or crimes of passion; these are hard to deter, though they can often be anticipated, as with an individual who is only violent when drunk. Other hidden crimes like child abuse or neglect are difficult to reduce using methods described here.

The methods in this book are not as effective against mass crimes: strikes, revolts, revolutions, insurrections, mass hysteria, and all the other actions by large numbers of people. However, techniques described here would keep track of perpetrators to hold them accountable later.

A last concern is with the emergence of bureaucracies in support of the book's technologies, such as those for surveillance, tracking, and identification. The bloated education bureaucracy in the U.S. illustrates how matters can get out of hand. As with similar issues in this book, society must plan from the beginning to limit the size of the supporting bureaucracies. Related issues involve the cost and technical challenge of getting the hardware and especially the software to work.

What mankind really must do is create a society with citizens who do not need to or even want to commit crimes. This goal is daunting, but open access to information will engender the formation of open societies, ones with free speech and with privacy, that can address these larger issues. Education will play an essential role here as mankind progresses to new forms of organization and to global communities that those in the present cannot imagine.

2. Monitor
followed by Control

> *Technological optimism means in practice the ability to recognize bad surprises early enough to do something about them. And that demands constant monitoring of the globe, for everything from changes in mean temperatures and particulates to traffic in bacteria and viruses. It also requires a second level of vigilance at increasingly porous national borders against the world exchange of problems. But vigilance does not end there. It is everywhere.*
>
> —Edward Tenner, *Why Things Bite Back: Technology and the Revenge of Unintended Consequences,* Knopf, 1996, p. 277.

> *Pedestrians with 5G-enabled smartphones could be able to walk safely into the street without checking for cars, because 5G-enabled cars would be routed automatically around the person or come to a full stop. In 20 years, most fatalities on the road should be a thing of the past.*
>
> —Gerhard Fettweis, quoted in "Developing 5G and Beyond," *The Institute, IEEE,* March 2017.

Blah, blah.

Example: Pollution.

I want to use the "crime" of pollution as an example of this book's approach to problems. As mentioned before, there are instances of pollution that are part of the natural world, independent of mankind. For example, huge amounts of oil can leak into the ocean due a natural process (say, an earthquake). This is undesirable, so I want to handle it along with human-caused pollution.

I follow the "first monitor, then control" approach, detailed in Chapter 2. There are many ways to monitor pollution, depending on the pollutant. Best is to have the monitoring devices in place before any pollution occurs, rather than belatedly discovering the pollution. Chapter 4 on fingerprinting presents ways to identify the source and time of any pollution, so it can be clear who should bear the blame. These techniques would even allow for multiple sources of the same pollutants, assigning the proper percentage of blame to each agency causing the problem. More specifically, gasoline storage tanks in gas stations are required to have monitors that will give an alert for the initial start of a leak.

Example: Birth Control.

Consider a critical issue such as overpopulation and birth control

Next I want to consider the much more difficult example of birth control.

Consider a critical issue such as birth control. The technology is available to achieve such control, and the cost of control is usually far less than the cost of no control. But there is not even agreement on its need, and the use of birth control falls short for many reasons.

3. Identification
and Identity Verification

"We'd like to get a sample of your brain tissue."

— *Ghostbusters* movie, 1984, near the end.

"Shut up," the big one said, and kidney-punched Bill. "I'm Litvok, and this is my bunch. You part of my bunch now, newcomer, and your name is Golph 28169-minus."

"No, I'm not; my name is Bill, and it's easier to say—" He was slugged again.

"Shaddup! Bill's a hard name because it's a new name, and I never remember no new names. I always got a Golph 28169-minus in my bunch. What's your name?"

"Bill—OUCH! *I mean Golph!"*

"That's better—but don't forget you got a last name too … "

—Harry Harrision, *Bill, the Galactic Hero,*
Avon, 1965, Book Two , Chapter IV.

Please place your right eye against the red aperture, leaving the eye open and relaxed. There is nothing to fear—we are just doing a laser scan of your retina for identification. There has been no evidence of any long-term vision impairment or other morbidity associated with this procedure."

It sounds like a passage from a horror novel, everybody's nightmare of intrusive identification. In fact, individuals are wary of identification schemes, and not just ones that promise to shine a laser into their eye. Even a request for a fingerprint makes people wonder about storage and reuse of the print. However, reliable identification of individuals is the basis for accountability schemes; to hold someone

responsible requires accurate identification of the person. Without such identification, there is no point in passing a law requiring that an individual identify himself when carrying out certain activities, such as buying a gun. I myself want perfect identification to keep someone from passing himself off as me, doing something in my name.

Each human activity can be explicitly attributed or kept anonymous, and attribution requires identification. For example, society sees false attribution in poison pen letters, those harmful letters falsely claiming a particular author. Identification plays a role even in anonymous activities, because it is often desirable to verify that several activities have been carried out by the *same* anonymous individual.

Many public activities should be attributed; society would be better off with much anonymity removed. The attribution should be verified with reliable identification techniques. For example, articles in newspapers and magazines usually profit from attribution, though anonymity also plays a role in the freedom of information of the press to correct wrongs, as with the U.S. Watergate scandal. Similarly, discourteous acts committed in public or while driving would be toned down if there were no anonymity. Certain activities, such as whistleblowing, the use of a suggestion box, voting, or a health-care inquiry, benefit from anonymity. Chapter 7 explores these and other issues related to anonymity.

The concepts of identification and verification are central to a discussion of the identity of individuals. To *verify* an individual's identity means to check that a person is who he claims he is, using stored data about that particular individual. To *identify* an unknown individual is much harder—one must discover the person's identity using data describing a large pool of individuals. With fingerprints, for example, verification will check that a single fingerprint is what it should be, while identification may have to search through vast files of fingerprints. The possible mistakes for verification are to verify the identity of an impostor, or to reject a correct individual as if he were an impostor. Identification can make the additional mistake of deciding on the wrong identity.

A system that monitors the transfer of prisoners in San Antonio

gives a real-life example in current U.S. society where perfect identity verification is a requirement. This system uses fingerprints, automatic fingerprint recognition by software, and ID bands with photographs. Officials need to know during a transfer of prisoners by bus that the right person is getting on the bus and that the same person gets off the bus. It seems that an easy way to effect an escape is to "talk" someone in prison on a lesser charge into trading identities, even when there is no close match in appearance. The "talking into" is not hard to do with a few well-placed threats to a prisoner and his relatives.

Verification.

Identity verification techniques continue to present problems in a practical setting. Simultaneously, one wants a low error rate, an easy and inexpensive implementation, and convenience for users. Private industry and government are carrying out a vast amount of research in this area, with a number of mature systems in use. Most facilities still use one of the two classic methods: either a password or PIN (Personal Identification Number, like the 4-digit numbers used in bank teller machines) that the user has memorized, or an identification card with a picture that the user carries. Notice that merchants accepting a credit card often do no identity verification at all.

Both these methods have flaws. Users are bad at remembering passwords, especially computer-generated passwords or multiple passwords. (One expert on identity verification said he has trouble with more than a couple of 4-digit PIN's.) Users respond to these difficulties by choosing a simple password if that is an option—a password that is easy to guess. Otherwise users record the password where it might be seen. For example, a stolen wallet with both bank teller card and driver's license will allow the thief to guess the birth date as a likely PIN. (In fact, I have been using my own birthday as my PIN; I had better change it now.) As for the other classic method of identity cards, they are often forged, stolen, altered, or not checked carefully enough. Most checks are done by hand, although a careful check causes delays and requires extra manpower.

As a result of these problems, providers of identification services have introduced a variety of hardware schemes. Identity cards can

include data in a magnetic strip for machines to read, or computer chips, or even a self-contained computer on the card—as a so-called "smart" card that can respond adaptively. Other approaches rely on personal features, also known as biometrics. These terms refer to physical characteristics of individuals that people or machines can measure.

Here is a list of categories for identity verification methods. The first four categories are those now commonly considered for implementation.

1. *Prearranged information*, such as passwords or PIN's. These have the disadvantages mentioned above of being hard to remember and easy to guess or steal, but passwords are so convenient to implement and easy to use that they are the dominant system. Current high-security installations recommend a password of eight random letters that is changed every three months—a burden for hapless users to memorize. Promising are methods that, while forcing random computer-generated passwords on users, attempt to make the password easier to remember, either by the choice of syllable parts strung together, or by the use of pass phrases made up of common words. It also helps to give the user a selection of these computer-generated passwords. The prearranged information might even be an agreement to behave in a certain way. For example, one can use a code phrase in an innocent-sounding context, as some embassy personnel are trained to do. As another example, an organization may require that security guards recognize top-level management on sight; use of the ID card is then interpreted as a sign of coercion.

2. *Piece of hardware*, such as an ordinary metal key, a card with a picture or data or even computer components on it. Cards require a machine to create, whether a camera or a computer; except for pictures, hardware is needed to read the card; and cards can be lost or stolen. In spite of these problems, cards are the second most common system, after passwords. Cryptographic techniques allow the design of cards that cannot be created except by an authorized agency. For greater security, the hardware can be hard to remove, as with the ID bands mentioned earlier.

3. *Personal feature*, such as a picture, a fingerprint, retinal pat-

tern, iris pattern, body dimension, hand geometry, voice characteristic, facial thermogram, or even more sophisticated medical or biochemical property. The emphasis is on features that distinguish one user from another, such as the pictures or fingerprints that have long been in use. If pictures are used, the system stores and processes the picture, unlike a picture on a card in the previous category.

Personal feature systems have disadvantages. They are expensive, usually requiring hardware that is easily damaged, either by accident or maliciously. They are intrusive, requiring users to submit to an initial recording session and to repeated measurement sessions. Finally, until recently they have not been very reliable. Many systems still have a high error rate from errors of rejecting a legitimate user, though the error rate of accepting an impostor is now often very low. (Imagine a voice-activated money-dispensing machine that refuses a user money because his voice is hoarse from an infection.) There is a trade-off between the two kinds of errors, so that setting the tolerance to accept almost all legitimate users makes it easier for an impostor to succeed, but both errors are now being pushed below one percent.

There is promising work going on right now (and hardware/software systems for sale) in the areas of fingerprint recognition, retinal scans, iris scans, hand geometry readers, and voice and facial recognition, with claimed error rates far below one percent. Users may object to their fingerprints or other personal data on file, and many users will object to a retinal scan. Of course a blind or mute person would not be able to use the respective system. And one might make an impression of a fingerprint to fool a fingerprint-recognizing system, while a recent lurid science fiction movie (*Demolition Man*) showed what could be done in real life: either dragging an unwilling user to a scanner, or presenting a severed body part to it.

With voice recognition, in addition to forcing a user to answer, one could record the proper responses for playback at the machine. To foil such recordings, the system can give the user a sequence of pre-recorded words to say, different words for each session. Voice recognition will also work remotely and can even adapt to changes in a voice over time.

4. *Real-time skills and capabilities*, such as signature dynam-

ics, typing style and ability, reading speed, or facility in the use of a mouse. The term "signature dynamics" refers not to the final appearance of a signature, but to the particular way it is carried out—the speed of executing the various elements. In theory, such a system would make forging a signature harder, since a forger only sees the final signature and not how it is executed. Systems based on signature dynamics have been under development for years and are just now being released. Typing style gives an interesting way to monitor identity continuously, and though it is particularly error-prone, it could be used along with other methods. One proposal uses facility with a mouse as a way to detect substance abuse problems. Some people are much better than others with a mouse, so a mouse-based detection system would measure ability compared to one's baseline ability, when not impaired.

The final three categories are speculative ones that I am personally interested in. The next section discusses them in detail.

5. *Customary ways of doing things (non-real-time)*, such as usage patterns, that is, the particular activities carried out and the way they are pursued.

6. *Skills and knowledge (non-real-time)*, due to past education, training, history, upbringing, culture, or hobbies.

7. *Psychological characteristics*, including items often measured by psychological tests.

There are hybrid combinations of the above categories: an intelligent card with a picture, or a hand geometry encrypted with a public-key signature scheme (see Chapter 6) and stored on a identity card. In this latter example, the system measures the shape of the hand and stores this shape information on the card in a form that cannot be forged. A local site can verify that the stored information matches the actual shape of the hand, while even the local site itself cannot create a card for someone else. Another hybrid might have the user draw a picture with a mouse, say, a picture of a favorite "doodle" or quick drawing. As with signature dynamics, the system would analyze not just what is drawn, but how it is drawn.

Speculative Verification.

I discuss here the last three speculative categories of the previous section. They are of interest to me, but research and development of practical identity verification systems remain focused on techniques outside this section.

These methods, based on habits, skills, and psychology, have the advantage of requiring only software—there is no special hardware, and a simple phone line would suffice for the connection between the user and the system. Also, these systems require no user memorization, since they already store any needed special information, and they use facts the user knows without memorizing. The methods mimic the way a person would verify the identity of a friend if the two could only type questions and answers to one another.

There are also disadvantages. Constant monitoring of computer usage would seem like Big Brother watching over users. Many of these methods require responses which users may find irritating and obtrusive. There may be software training sessions, and users could object to them as a waste of time and an invasion of privacy. As with all identification systems, there are problems with error rates and tolerance settings. Users might worry that psychological information could be misused. Finally, the system will require extra resources, and implementation will be complex.

The list of disadvantages may seem long, but systems like these are appropriate for applications in facilities with the highest security requirements. Such facilities would also employ conventional verification techniques.

Dorothy Denning introduced the study of computer usage patterns with a real-time Intrusion Detection Expert System (IDES). This approach gives *continuous* monitoring of user identity, in a way similar to typing style. The IDES checks what a user is currently doing on the computer—which programs he uses, what types of files he accesses, and the relative amounts of time spent on the different activities. The IDES then compares his current usage with his usage in the past. (Under such a system, a user starting a new project may have to submit to a special identification check.) The IDES also compares us-

age with activities an intruder might carry out, so the system checks for security violations by legitimate users. One could use a similar approach with an Identity Verification Expert System (IVES) analogous to Denning's IDES. These two expert systems would function as a single unit, with the IVES implementing techniques described in this section. There would be questions and answers, as well as a search for unusual patterns of usage. The questioning part (IVES) would be invoked at random times, at initial login time, and in case the passive part (IDES) suspected an intrusion.

Similar approaches are in use in the consumer industry. Credit card companies are now starting to carry out a verification based on customers' buying habits. In order to cut down on stolen credit card use, the companies propose to keep records of customers' purchases, so that gasoline and food bought frequently in Houston, followed suddenly by stereo gear in Hong Kong, alerts a company to check if the card is stolen. This particular approach is error-prone, it identifies the theft only after purchases, and it requires a record of data about buying preferences. A better system would reliably identify the card holder at the time of purchase.

There are other possibilities for identification based on skills and knowledge. Knowledge of, for example, languages, one's profession, ability in certain games, knowledge of specific geographical areas, knowledge derived from hobbies and special interests, or knowledge due to special training or acquired from specific upbringing. Each user would supply information to the system in a training session.

In order to impersonate a user, an intruder would need to know the correct answers, and he would need access to the user's current personal data profile, to determine whether to provide the correct answer. Thus as with a machine trying to pass the Turing Test, an intruder could not give correct answers to questions when the true user is not supposed to know the answer.

Here is an extended example. My own native language is English, and I know a fair amount of German, but no other languages (unless computer languages count). My recognition vocabulary in German]is better than my active one, so a good question to use for me would give me an English word, like "pencil," along with twenty possible

translations, including the correct answer, “der Bleistift,” and a lot of silly answers: “das Pferd,” “das Fenster,” “die Gabel,” and so on. I could answer such a question quickly and get back to work. If I happened to miss the question, the IVES system would give me several more similar questions, and if I missed *those*, the system would notify a security officer. Notice that an intruder pretending to be me must know what languages I am familiar with and must have, at the least, a German dictionary handy (perhaps an electronic version). The system could also give me a question about Spanish or Russian and start asking additional questions for a *correct* response. Asking me to choose the translation of a whole sentence, and providing less trivial answers, would keep an intruder from faking answers with a dictionary. A different set of questions would check for native German fluency, which I do not have. And the system would not have to ask questions about languages; it could ask about my hometown or about a school I attended.

As another example, consider questions for someone skilled at chess. At the first simplest level the IVES system asks the user how well he plays chess. This is the same question posed in the training session, and is simply a direct query about a personal data profile. In order to impersonate a user successfully, an opponent only needs to know the profile for that user.

At a second level the IVES poses a question about chess, chosen from a fixed list of questions and answers. Different answers could give different indications of the skill of the player. Obviously there is a moderate error rate with a single question, since even a skilled player might be wrong once and a weak player might make a lucky guess. An accumulation of such questions would give data on how well a user fits his claimed profile. Notice that here the opponent must know the user’s profile and must give answers to questions consistent with that profile.

At a third, more sophisticated level the IVES would create random chess problems and pose questions whose answers it would determine. Thus the IVES would use randomization techniques to make the number of questions large. An opponent would need to know the user’s profile and would need skill at chess or access to an equivalent

chess-playing program.

This system need not be time-consuming; it would be better to expect a quick response, within ten or twenty seconds. And an intruder would get no warning of the time a question is to be posed or of the subject of a question. Rather than chess, a question might cover bridge, or the go game, or a host of other subjects.

The use of psychological characteristics is particularly speculative. One seeks to measure subtle characteristics that a user may not consciously be aware of. There are simple tests that separate individuals from one another, such as "personality" tests used to screen job applicants, and a statistical analysis of writing style. One could ask users to visualize what an object looks like from its projection on a screen. From word association tests one could infer repeatable facts about an individual. It does not matter what the facts are, but only that they are different for different individuals. One could also search for a simple game or other activity that will distinguish users. Consider, for example, the problem of arranging 25 random playing cards into five "pat" poker hands. This can usually be done, but some people (even poker players) have much more difficulty than others. Better than just a success/failure measurement would be a way of checking and quantifying the approach and strategy of a user. Even in the poker example one could measure the time to a solution and the types of hands produced.

As a final example, consider the mathematician John Conway, who has programmed his computer so that he must identify the day of the week of ten random dates (e.g., December 4, 1602 was a Saturday) within a short time (usually twenty seconds) in order to log on. Conway can perform this lightning calculation in his head and so can verify his identity to his computer.

Identification.

As mentioned earlier, identification is a harder task than verification because the choice comes from a large pool of possible identities. At present the focus of identification is on pictures and ordinary fingerprints, but these methods pose considerable difficulties. The memory of a criminal's appearance may remain after a crime, but associating

the memory with a stored photograph is hard, particularly considering that an individual may change hair color and style, facial hair, and glasses, and the individual may age. Mostly this occurs more as a verification that a suspect's appearance matches the memory. The United States has now computerized and consolidated fingerprint searches, with a large database of fingerprints on hand at the national level. The use of fingerprints is an ancient and well-studied technique that will continue in use indefinitely, since fingerprints may remain after a crime. The newer DNA analysis is still mostly used for verification, but it should become widespread for identification as well. DNA analysis has special importance because of its accuracy and because samples of a criminal's tissue may also remain at a crime scene, particularly in cases of sexual offenses. For both fingerprints and DNA analysis one must be sure that the print or tissue sample comes from the individual being identified, to maintain a chain of evidence. The U.S. FBI is just now creating a DNA database for people convicted of federal sexual predatory crimes, though it is not yet fully implemented.

Other verification techniques using personal features will work for identification as well, such as retinal or iris patterns, or voice characteristics. A hidden camera can obtain the iris pattern remotely, while a microphone can record the voice of a criminal, so again such evidence may remain after a crime. With such new techniques, as with the old, emphasis should be on reliability, ease of computer searches, and on consolidation and coordination of searches, so that different jurisdictions do not withhold information from one another. Some techniques that work well for verification will not work for identification. For example, one company's hand geometry system uses only nine bytes of data for verification—too little data to be effective for identification, since for a given hand geometry there would be many similar hands. Hand geometry also fails because information about this characteristic is unlikely to remain at a crime scene.

National Identification.

American immigration officials in their search for illegal aliens often question Hispanics while ignoring Anglos—sometimes detain-

ing Hispanics for no other reason than their brown skin or their use of the Spanish language. This is not equality of application of the law; America should give equal treatment to everyone, using national identification. Notice the phrasing here: A physical card is not needed, just reliable and coordinated identification, since it is also an inequity to expect Hispanics to carry a special card, while Anglos need not. The terminology ought by rights to be "national identity verification," since in most instances the need is to verify a claimed identity.

Many people have proposed a national identity card in the U.S., while others have successfully resisted introduction of the cards. There is sufficient need for these cards that other imperfect cards have filled the void. The bewildering array of current cards in use, including driver's licenses, social security cards, and other job-related cards are "easily counterfeited and poorly coordinated." For example state driver's licenses now serve even non-drivers as an identity card. The state cards vary greatly, though the trend is toward more secure licenses, ones harder to forge, like the Minnesota license with its security features: a bar code, a 256-character magnetic strip, and a digitized photo and signature. The license is nearly the same as a Minnesota identification card, used most often for activities not involving driving.

Current technology allows the creation of excellent identity cards, difficult or impossible to forge. The U.S. needs strong and unforgable national ID cards, but only as a part of a system of national identification. A card would provide a simple means for identifying individuals using inexpensive hardware and without a requirement for transferring data. As mentioned above, the card would actually provide identity *verification*, using one or more of the personal features mentioned earlier, such as fingerprints, or retinal, iris, or voice characteristics. As indicated before, public key cryptographic techniques from Chapter 6 can encrypt the personal feature data so that cards could not be created by an impostor. The same personal features with the same recognition hardware would provide identity verification without the card, requiring only a data link to a central site. Cryptographic techniques can prove that one is truly communicating with the proper

site.

These cards are not at all like the U.S. 100 dollar bills foreign print shops forge so well that experts can scarcely detect them. Cryptography allows creation of truly unforgable cards, ones that a person with better technology than the card makers cannot forge. (Someone else could *copy* an existing card, but could not make a new card with a different identity or different features on it.)

The data describing every individual's personal features would likely be distributed over many sites in what is known as a distributed database. An identity verification would involve transfer of data about a single individual, usually from a nearby site—a simple query that remains simple no matter how many people are involved. Identification of an unknown person would still usually involve only the local site, but at worst it might be a lengthy process—made more lengthy with increasing numbers of people identified, but such identification is rare compared with the constant need for identity verification.

Many in the U.S. have vehemently opposed national identify cards, and of course these people would also oppose a proposal for cards as only part of national identification. One concern is that the cards could be forged and misused, and so not be effective. The unforgable proposal above handles that problem, but the larger concerns center on government misuse of the card. Such misuse is an all-important issue for opponents of cards.

The government might misuse cards (and misuse my larger identification schemes) by creating forged cards for insiders, for government employees with a "need" for cards, and for those outside the government with connections to the card-making bureaucracy.

More worrisome misuse would occur if a government used identification for purposes beyond the legal uses—say, to keep track of political enemies, or to maintain prohibited information about individuals. Thus people in Minnesota worry about just what information is stored in the 256 characters on their state's driver's license. Perhaps it records traffic violations that are not supposed to be on the card; perhaps it has inaccurate information.

The current array of different cards with different individual data stored along with them again argues in favor of a single card, with a

clear location for any personal data, where an individual could check the extent and accuracy of this data. Such checks are essential; as with credit bureau data, each individual must have ready access to all personal data regarding themselves.

Finally, there are worries that a reliable national identification scheme would tempt lawmakers to extend its uses beyond the initial concept. This would not be illegal use and need not even be misuse in a broader sense, but it is still cause for concern about identification out of control.

Governmental misuse is likely to occur, so plans for implementation must include plans to protect against such misuse. Society must monitor and control the sites that create cards and that carry out identification. (Cryptographic techniques allow for simple verification sites that do not need such tight controls, since they cannot create cards.) As for extending the application of national identification, this deserves wide and open debate within society.

Cost is another concern, but high-quality identification does not have to be expensive—conversion to a unified system might save money over the current mess in the U.S. of identification by each state, by separate government agencies, and by many companies or organizations. Reliability should be extremely high, especially if several features are used simultaneously. Data storage and retrieval requirements would be comparable to what the U.S. has now in various taxing and monitoring agencies.

I personally feel that I would be much better off if I could be reliably identified. It often happens that a person is mistaken, detained, and even jailed because he looks like or has the same name as a wanted criminal. People worry that the police will stop them on the street and demand their identity without cause, but such an incident is unrelated to issues of national identification. If the police are behaving unjustly (committing crimes, in other words), they must be controlled by society; the controls and identification and surveillance of the lawkeepers must be the most complete and stringent in society.

Deliberate theft of identity is also on the increase now and can be devastating. In the U.S., a criminal's knowledge of someone else's social security number and mother's maiden name (the latter often

used as an extremely crude identity verifier) can lead to major financial and credit problems, as the criminal assumes a new identity to steal or obtain credit.

Recommendations.

The United States should identify every individual, whether a citizen, a non-citizen resident, or a visitor, identify them reliably and from birth, with the identifying characteristics readily available to local, state, and national law enforcement. Other countries should do the same. There are few benefits from tolerating unidentified, unknown people in a society, except that the government could save the money and effort of keeping track of them.

Such excellent identification would only be desirable as part of the complete package of ideas in this book: combined with openness, free speech, and privacy. Perfect identification in a dictatorship would just make complete and efficient repression easier.

Another way to look at this issue is to say that a society ought to care enough about its citizens to keep track of them all—not just their identity, but their status and well-being. What sort of parents do not even know how many children they have or where their children are? The same reasoning should apply to an entire society.

The current system in the U.S. uses a haphazard and uncoordinated collection of partial identifying characteristics for a portion of the population: mainly fingerprints, pictures, and signatures. A variety of agencies maintain this identifying information and coordinate it with other information. But additional identifying information is also kept, such as records of the tattoos of prison inmates. This unsatisfactory hodgepodge of partial, inadequate identification schemes must be replaced with the excellent identification now feasible.

Reliable identification of individuals is the indispensable foundation for any scheme to keep better track of events and objects, and to hold people accountable. How can society hope to control crime when it does not know who its members are? Near-perfect identification is now possible, with steadily falling cost. Specific identifications could be carried out quickly and conveniently. Chapter 5 proposes in more detail that identities of individuals be determined and logged

when they travel by public transportation, when they take charge of anything dangerous, and under other circumstances. The U.S. is doing much of that now—just not doing a good job of it, so that an ordinary citizen cannot take an airplane trip anonymously, while someone with more resources is able to, either with a private airplane or with a fake identity.

4. Fingerprinting
for Tricky Monitoring

Misuse of legitimately obtained data will remain a security problem even if all other technical problems have been solved. Fingerprinting seems the only solution to this final problem. Our system will catch any opponent who misuses a sufficient amount of data. One need not assume a consistent or continued behavior.... The opponent himself would be able to monitor his increasing exposure ... , but he has only two choices: stop leaking data or risk increasingly certain detection.

— N. R. Wagner, R. L. Fountain, and R. J. Hazy,
"The Fingerprinted Database,"
6th Intern. Conf. on Data Engineering,
1990, pp. 330–336.

The previous chapter discussed ordinary human fingerprints and their use for identification. This chapter extends the notion of *fingerprint* to include characteristics of any object that distinguish it from other objects. The word *fingerprinting* refers here to the process of adding fingerprints to an object and recording them, or of identifying and recording fingerprints that are already present.

People commonly confuse these fingerprints with the digital signatures described in Chapter 6. Such a signature authenticates an electronic object to identify the object, perhaps through the individual who created it. Fingerprints are usually intrinsic to an object and not easily removed; in contrast, signatures cannot be forged but can easily be stripped off the object. Other techniques attempt to hide information inside objects, especially in images, as is described in the section after the next.

Fingerprints can either be inserted or discovered, and the insertions can take the form of additions, modifications, or even selected deletions. Fingerprints can occur on physical objects or on data.

Examples of fingerprinting in action illustrate these concepts. Most consumer goods come with a unique identifying number, such as the vehicle ID number on a car. Detectives routinely match typed characters with a specific typewriter, or a fired bullet with a specific weapon. Businesses may place similar advertisements in different markets with slightly varying return addresses, to determine the market yielding the best response. Mapmakers insert slight deliberate variations from reality to identify copiers. Theft of computer chips is a growing problem, with proposals for a unique ID number on each chip to help identify stolen chips.

As the author of a chapter about fingerprinting techniques, I could not resist putting a fingerprint on my own name. Until now I have not used my middle name professionally, but only a middle initial. I use my first name (a mysterious name starting with "N") about half the time. So if I see "N. Richard Wagner" on an address I will know it comes from a person who read this book, and the use of my first name will identify someone who knows me apart from this book.

Any object that might be misused needs a fingerprint to identify the object's owner after misuse. For identification to succeed, an authority must record the fingerprint along with an ID of the owner. The recording might take place at the time of sale or of delivery. A method from the previous chapter would then identify the individual taking charge of the object. Imagine the uselessness of identifying the purchaser of dynamite employed in a crime as "John Smith, address unknown."

Fingerprints should be hard or impossible to remove, as dictated by the particular application. For example, using different post office boxes for alternative return addresses provides a perfect fingerprint: the box used reveals the source of the address. In some cases one can have a perfect fingerprint like this, and in others one can at best make it difficult or expensive to remove the fingerprint. Thus a car with its vehicle ID number stamped onto half the parts and etched onto every pane of glass becomes more secure from theft.

My own research has included proposals for statistical fingerprinting—an approach that works even against an active opponent who knows the system in use against him. Here one supplies each user with data altered specifically for that user. If there is a leak, a statistical analysis of the leaked data will eventually catch the leaker with any desired degree of certainty ("confidence" is the formal statistical term). A fuller account of these issues appears later in this chapter.

Fingerprinting ought to be ubiquitous. Society can and should do a better job of tracking objects, especially stolen or valuable objects. Law enforcement agencies already keep lists of stolen goods or of items left at pawn shops. Sometimes the lists are computerized, and sometimes there is cross-checking of lists. Notice that the items need fingerprints to identify them; the lists record these fingerprints. The lists should be all-inclusive and coordinated. Initially, such measures might help recover what was stolen and help catch the thieves, but in time the use of these measures would be a powerful deterrent. A television set stolen in New York could not be pawned in California. Stolen goods taken across national boundaries pose another problem that cooperation between the involved countries can solve.

Fingerprints on Physical Objects.

Bullets illustrate many issues about fingerprinting physical objects. When a bullet goes through a gun barrel, it acquires characteristic rifling marks from the barrel. These are fingerprints that can match a bullet with a gun. In this way one can associate the same unknown gun with more than one crime; with the gun in hand, one can tie this gun to various crimes.

As a first step, laws should require determination of the rifling marks of each gun before sale and require the recording of these marks along with the identity of the gun purchaser and the serial number of the gun. Then it would be natural to enhance and expand these rifling marks, to make them show up more prominently and to identify the gun uniquely. The ideal would provide on each fired bullet a fingerprint that identifies a unique gun, traceable to an individual. (Stolen guns present an additional problem discussed be-

low.) It would take considerable research to determine how well this could work in practice, and the comparison of fired bullets is so inexact, depending on the condition of the bullet and other factors, that such fingerprints will never be completely reliable.

As a second step, manufacturers should fingerprint every bullet. The fingerprints could be the same for each batch or box of bullets sold as a unit to an individual. One method would add trace amounts of various elements to the bullet's material. It would then be feasible after the fact to analyze the bullet's composition and thereby read its fingerprints. These fingerprints would survive an impact that destroyed the shape and rifling marks on the bullet. As before, laws would require the presence of fingerprints and a record of the purchaser, holding the purchaser responsible for the use of these bullets.

As additional steps, one could fingerprint batches of lead or other materials used to make bullets to help trace those who make their own bullets, and one could add a volatile substance to bullets that could be detected in the air, say, at airports. Similarly, researchers could find ways to identify guns from a distance. The theft or illicit resale of guns and bullets creates another problem. A fine or even forfeiture of escrowed money would work in such cases. Eventually, society can manufacture high-tech guns that will not fire when stolen, as noted in the third quote at the start of this chapter, and further discussed at the chapter's end.

Adding different mixtures of trace elements to the material used to make successive batches of bullets need not in principle be much additional cost. The record-keeping would be more significant and would need to be computerized. Note that much of the work and expense would only be necessary in case of an investigation into a crime.

Some readers, particularly ones outside the United States, might find this discussion wrongheaded. They might wonder why the proposal is not to regulate and limit the sale of guns and bullets themselves. Such regulations would be a benefit, but even then, bullets will still be sold, and the fingerprints would still be useful.

Pollution gives another example of fingerprinting in action. Laws should require fingerprints on all industrial waste. There would be

requirements that suppliers of raw materials to industry add trace amounts of identifying elements or compounds to those raw materials. Thus a chemical company would have to supply solvents in fingerprinted form. There would be opportunities for cheating or bribery, so unannounced inspections and controls would be needed. A dishonest official might even insert another company's fingerprints, so companies would want to check for themselves that the proper fingerprints are present. At each stage of a complex process, the industry would add additional fingerprinting materials. In the face of environmental pollution, the pollutants themselves would indicate their source and even the percentage involvement of several industries. Pollution with no fingerprints would uncover cheating. Notice that these techniques attempt to catch polluters after the fact, to stop them and perhaps punish them. Chapter 11 talks about agents that could detect and halt pollution as it starts to occur—a better way.

Suppose a hit-and-run driver leaves part of his car and a paint sample at the scene. Then suppose an investigation reveals that only 100 cars of this type, with its special paint, had been sold in the U.S. Authorities narrow the search to just a few cars registered near the accident and are able to find the offender. The public would welcome the diligence and luck of the investigators, but society could make this the norm by requiring coded particles (or another identifying residue) in all cars, particles that would remain after an accident to uniquely identify the car.

In 1996, the U.S. Congress passed the Antiterrorism and Effective Death Penalty Act, which called for the study of tagging materials to add to explosives to make them easier to detect before an explosion and to allow identification of the source of the bomb materials after an explosion. These methods are promising but need further research; progress is blocked in the U.S. at present by various groups such as the National Rifle Association. In addition there were proposals for additives to ammonium nitrate to neutralize its explosive properties—methods which do not appear promising. Other examples of physical fingerprints include the serial number on currency bills in circulation. Society should use the fingerprint to track all currency, eventually tracking all electronic money as well. Admittedly, tracking all money

is more controversial than tracking bullets or dynamite, but money laundering is another crime that such tracking would address.

Endangered animals can also be fingerprinted, as is the case with badgers in the U.K., where the popular but illegal sport of badger-baiting faces badgers equipped with a waterproof coating containing a unique set of chemical tracers which can even identify those who handle a marked animal. The U.K. even has a database of shoe imprints.

These examples illustrate what one should do with every hazardous object or material, with anything valuable that might be stolen or destroyed or misused, and with many other objects as well: insert or identify fingerprints; record them; and keep centralized records and correlate the records. Often multiple fingerprints for the same object are desirable—identifying several characteristics already present, and adding identifying features, including residue that would remain after misuse as well as a volatile residue that instruments could detect during misuse. In the case of goods for sale that might be shoplifted, some manufacturers now insert standard tags that will trigger an alarm when an item is taken from a store without deactivating the tag. These tags lie deep in the item itself and are more difficult to remove than common anti-theft devices. Laws should require such tags in all dangerous or valuable objects. In collaboration with the fingerprinting (or sometimes independently), software agents, monitors, and sensors should track objects, recording and saving this data. Chapter 5 on surveillance and Chapter 11 on agents take up these issues in detail.

Hiding Information.

Concealing information in physical objects, in images, and in data extends back to ancient times, using, to cite two very old techniques, invisible ink and a secret text hidden inside a larger innocent-looking text. Researchers are reviving this practice, especially using images.

The term "steganography" refers to hiding a message (text or writing, say) by any means, to conceal its existence. In contrast, "cryptography" (see Chapter 6) scrambles the message so that only the intended recipient can understand it, but does not further hide the

message. This chapter has already introduced the similar terms of "fingerprinting" and "digital signature." A final term often used in the area is "digital watermark," in which an electronic version of a regular watermark is added to an image. The watermark would not usually be hidden, but might be hard to remove, so it could serve some of the purposes of a fingerprint: to identify an object and guard against theft.

If the goal is to transmit information, then steganography wastes a lot of space (or computer storage or transmission time) and conceals only from the uninitiated. However, computer storage is cheap now, and messages hidden by many methods in many images might prove burdensome to uncover. The message hidden in the image could be further concealed using cryptography (*encrypt* the message), so that it resembles a random string of 0s and 1s, as is typical of encrypted messages. One could just as well hide the message inside an actual random string of 0s and 1s, rather than inside an image, but such a random string, whether a hidden message or a directly encrypted text, alerts knowledgeable people that something secret is being transmitted. This is the advantage of steganography over cryptography: that eavesdroppers might not be aware of any hidden message. Another disadvantage of images for hiding messages is that some formats, such as JPEG, do not save all the data of the image, so that the message would usually be lost.

On balance, the methods in this section are interesting, particularly because their widespread use might overburden any agency looking for hidden messages, but the methods are not important for fingerprinting and are not as secure as cryptographic techniques.

Fingerprints on Data.

In this section "data" refers to anything machine-readable. Examples include English language texts, program source, executable files, files of raw data, database files, digital pictures, and digital video. All such objects allow inexpensive fingerprint insertion, which society should routinely require.

Suppose you are a staff member for a U.S. senator, working with one of the senator's committees. You have a confidential memoran-

dum ready for distribution to the committee. Recent events indicate that a senator on the committee either leaks such documents himself or has a leak in his staff. You could fingerprint the memo by preparing a unique version for each senator. Each version would have tiny variations throughout, say in the typefaces used or in the spacing—not noticeable unless one is looking for it. Now if a senator leaks a photocopy of a portion of the memo, an analysis would determine the leaker, assuming the fingerprints are throughout.

Once the word got out, any leaker would know that he must retype a memo before leaking it. You can foil this new strategy by making small *textual* changes in each version of the memo. It is easy to find places in a text that can be worded in several ways. Then one can employ different combinations of these variations for the different senators. As a bonus, this method can be automated to allow, under direct computer control, fingerprint insertion, recording of the memo version and the person to whom it is distributed, and determination of the version leaked in case a portion of the memo appears in the press. For readers familiar with computer jargon, the method could be the following: first determine individual points of variation in the text and then use a pseudo-random number generator, with the ID of the person receiving the memo as seed, to determine which individual variation is used at each stage.

A popular novel, *Patriot Games* by Tom Clancy, described exactly this strategy (referred to as the "canary trap" in the book).

> Each summary paragraph has six different versions, and the mixture of those paragraphs is unique to each numbered copy of the paper. There are over a thousand possible permutations, but only ninety-six numbered copies of the actual document. The reason the summary paragraphs are so—well, lurid, I guess—is to entice a reporter to quote them verbatim in the public media. If he quotes something from two or three of those paragraphs, we know which copy he saw and, therefore, who leaked it. They've got an even more refined version of the trap working now. You can do it by computer. You use a thesaurus program to shuffle through synonyms, and you can make every copy of the document totally unique.

In time, potential leakers will discover this approach also, and realize that they must paraphrase any leaked memo. They fall back to leaking the information in the memo. Now what can one do in an attempt to fingerprint the memo? The method from the Clancy novel fails completely in this case. It sounds extreme, but one can change the *information* in the memo: altering facts slightly, adding pieces, leaving pieces out. The challenge is to find facts to alter without changing the thrust, meaning, and completeness of the memo, and without calling attention to the fingerprints. In this environment potential leakers know that they must alter the basic information and facts of any memo they leak in order to escape detection.

This example sets the stage for the next section.

Statistical Fingerprints.

Imagine that you provide information to various individuals, one of them an opponent who intends to leak portions of this data to unauthorized individuals. Assume this opponent has all your technical knowledge and has access to more computing power than you. The previous section indicated how to foil and trap such an opponent: place fingerprints on the data itself, that is, alter the actual data values provided to each individual.

Alteration of data is a controversial step, not easily carried out, and full of pitfalls. This is an extreme course, but such fingerprinting will often prove essential and effective. At the simplest level each individual receives a different collection of data out of all available data, but the separate data items are unaltered. One keeps a log of all data retrieved by each individual. In cases where few people access the data, that may be enough to pinpoint the leaker, as from a detective novel: "Only the real murderer can have known…." In cases of wider access to the data, the only choice is to alter data values.

More specifically, each individual gets a collection of data values—on the surface the same values go to every person, but each user actually gets values that are slightly altered, for that user alone, from the true values. Different users receive different alterations, but for a given user the alterations must be consistent. Thus a user gets the same consistent values if he asks for them a second time. If a

value represents, say, the average of other values, then this average must be the average of the altered values.

The problems here are to find values to alter, and if they can be altered, to decide how much to alter them. Clearly one cannot change certain data values at all. For example the data in a U.S. Federal Reserve Bank consists of interest rates, ID numbers, account balances—nothing that can be altered, though one might slightly modify account balances if users knew these fingerprints were present.

As another example, a medical record contains many items to alter. Of course not an individual's blood type, but the exact date of a vaccination could be altered within some range depending on the type of vaccination. Blood pressures or results on standardized tests could be altered by a few points without changing an evaluation.

Note that this approach calls for the *alteration of data values*, and some users would object to any alterations at all. Imagine telling a student seeking entrance to college that his test scores have been lowered by a few points. He might feel that those few points could make the difference. A policy of only raising selected scores is equivalent to lowering the others and would meet with the same criticism. The criteria for data fingerprint insertion should be that the application is important and that the alterations have no significant adverse effects.

Assume one carries out alterations and sends fingerprinted data to a number of individuals. When the data returns after the leak, a statistical analysis can test the hypothesis that each individual is the source of the leak. The knowledgeable opponent will counter by altering values himself before leaking them, perhaps by rounding them. This tactic will not work indefinitely for the opponent, however. First, the opponent's values have already been altered within acceptable limits. If he alters them much more, the leaked data will be too inaccurate to be of use. More significantly, no matter how much the opponent further alters the data before leaking, given sufficiently many leaked values, a statistical procedure will correctly identify him as the opponent with any desired degree of confidence. An opponent who continues leaking cannot protect himself from eventual detection.

Consider a specific scenario. Suppose the U.S. is to build a new line of tanks and trucks for use by its allies in Europe. Early in the

project, each country wants to know the width, height, and weight of the various vehicles. (They may wish to know which roads and bridges the vehicles can travel on.) Suppose further that one of these countries is the source of a leak to an opponent ("the enemy"). The U.S. could supply each country with data altered within an acceptable range, since one would want leeway in the measurements anyway. After a leak, if the data returns to the U.S. somehow, the U.S. could try to identify the leaker. If the returned data was not further altered, this data itself would identify the country of the leaker immediately. But even if the opponent further altered the data, beyond the initial fingerprints, the hypothesis testing mentioned above would eventually pinpoint this opponent. The smaller an opponent's alterations, the quicker he would be identified, but larger alterations make the data less valuable, since it is less accurate. The opponent faces a dilemma: the more valuable his data, the more quickly he is caught, and he cannot avoid eventual detection.

To get a feeling for specific numbers, suppose one provides 78 data values to each of 50 individuals, and suppose that each data value has alterations (the fingerprints) of plus or minus 2 applied. (For some users 2 is added to a given supplied value and for others 2 is subtracted.) Suppose the opponent further alters these values by rounding them to the nearest 5 points, and then leaks them. From the leaked values, a statistical procedure will correctly identify a single individual as the opponent at least 95 percent of the time, i.e., with at least 95 percent certainty. With the same 50 individuals, and the same degree of alterations, but with 111 data values, the opponent would be identified with at least 99.5 percent certainty, that is, the procedure would fail only one time in 200.

Subtle Fingerprints.

I proposed the widespread use of data fingerprinting in 1983, and two co-authors and I provided statistical procedures in 1990. Simple fingerprints are often employed, but more interesting are subtle uses. In outline, the fingerprinting process sends multiple copies of data out into the world. If a copy comes back, even an altered copy, the fingerprints may allow one to deduce the source of the returned copy.

There are more subtle ways to proceed than those discussed so far. For example, one could orally brief a number of people, using a different vocabulary for each person, but presenting exactly the same facts. A later leak might be phrased in a vocabulary identifiable as that of a specific briefing session. (This technique is similar to those at the start of the previous section.)

It may be possible to deduce from alterations in the returned copy something about the path through the world that the original data took. For example, if 500 miles is sent out, and 497 miles returns, one might suspect that the 500 miles was converted to 804.675 kilometers, rounded to 800 kilometers, converted back to 497.095 miles, and finally rounded to 497 miles. (Different agents are rounding by different amounts, and so leave the fingerprint.)

Along similar lines, a news agency recently reported that a giant floating iceberg was 656 feet 2 inches thick—a precise-sounding measurement that in metric units is exactly 200 meters, the true approximate figure. The same report said that the iceberg was the result of a 36.5 Fahrenheit temperature rise since the 40s. But the actual rise is a 2.5 Centigrade increase. A reporter converted the temperature rather than the increase, which should have been given as 4.5 Fahrenheit.

As another example, a mathematician named J.L. Doob once wrote a probability book that the soviets appropriated and translated into Russian. Later, around 1946, the U.S. Navy thought it had found an original Russian technical work and appropriated the book back, translating the Russian back to English and transforming the author's name to "Dub." The transformed name is a fingerprint suggesting the transformation the book had undergone.

A fingerprint left by the Unabomber gives a final example, where he wrote in his "Manifesto":

> 185. As for the negative consequences of eliminating industrial society—well, you can't eat your cake and have it too. To gain one thing you have to sacrifice another.

The phrase about eating and having cakes also appears in an early letter of the suspect in the case. American reporters termed this a

"twisted cliché" and said it was "turned around." Its presence in writings by the Unabomber and the suspect provided a link between the two. Current American usage expects to hear the words "eat" and "have" reversed, so it is surprising to find that the *Oxford English Dictionary* lists only the Unabomber's version of this saying. Other dictionaries of idioms (British and American) list both versions. It now seems likely that the Unabomber used this as part of his normal English, and not as a clever reversal of a standard phrase. He may have inadvertently left this subtle fingerprint because he was not familiar with the modern American preference—after all, he seldom talked with people and had no electricity for radio or television. This fingerprint supports the *verification* of an identify after the fact. Imagine carrying out an earlier *identification* based on similar fingerprints, using an automated search through vast amounts of published materials. Such identifications will be increasingly feasible as more library materials become machine-readable. The same process occurs when a literary researcher tries to decide whether a "lost" play was written by a particular playwright or when searching for plagiarism in published material.

Similar techniques will check if computer students copy or exchange programs for an assignment, as well as checking for other academic plagiarism. Software is readily available to compare two programs in a variety of computer languages or even to compare two term papers in English. If a whole class hands in programs, the instructor can check all possible pairs for similarities. The plagiarism detection software is subtle and hard to deceive; it easily copes with the common tricks of students who copy programs: change program identifiers, rewrite all the comments, reorganize the program in a new style, and arrange elements in a different order. As for detection of plagiarism in ordinary English writing, the grand opera singers of detectors are two employees of the National Institutes of Health, Walter Stewart and Ned Feder, who started out looking for scientific fraud and ended up checking for English text plagiarism.

Crime-proof Hardware.

At this point the discussion will move beyond fingerprinting, from

methods that identify misuse, to those that will not allow misuse. For example, if a thief steals a fancy radio/CD player from a car, he may find that it no longer works when removed. This is a simple case of a piece of hardware that does not permit successful theft.

Most consumer goods are getting electronic innards and are developing higher intelligence—from cars to refrigerators these machines are capable of more sophisticated actions—even of adaptive behavior. In time, there will be enough extra computing capacity in electronic objects in the home or workplace so that they can be programmed to work as intended and in the assigned environment, and not to work if there are any changes, such as removal from the environment. For example, appliances could repeatedly verify that they are still in the proper house, using cryptographic authentication techniques described in Chapter 6. Such verification can be made foolproof, but with current systems this would substantially drive up the price of the appliance. Future appliances will have computing power to spare for this task. Appliances may broadcast their position, as with some stolen laptop computers that now try to "phone home" at random times to give their current location.

It must not be inexpensive to replace this module that controls appliance operation. Many of these appliances of the future will consult their brain before doing anything, and these brains will be a significant part of the appliances' cost. Thus the problem of theft and re-engineering should lessen also.

Some software vendors require that the authorized user retrieve a special enabling password or code, needed to run the software. (They may also require a hardware device inserted in the back of the computer.) Such software can be copied and backed up, but it does not run without the special password. It is even possible to use an identifying hardware ID within a specific computer and supply a password that will only work with that specific copy of the software and that specific computer. Take the software and the password to a different machine, and it will not run. Cryptographic techniques can create passwords that users are not able to break.

In the same way, manufacturers of microprocessors may one day protect against theft by requiring a special password that is tied to the

specific microprocessor chip and to the specific computer. When the *hardware* is started up by the user, it could first insist on accessing the microprocessor vendor by phone or over the Internet, to let this vendor verify that the chip was not stolen.

Society could use similar techniques to make automobile theft nearly impossible. If an unauthorized person tries to start or even enter the car, the car's computers could be programmed to lock up in a way that would require resetting by a dealer.

A cartoon image showed a parking meter spewing hot tar over the car of a hapless motorist who violated the time limit. But a serious Philadelphia inventor has a real parking meter which resets itself when a car leaves. It then demands fresh money from the next car. The meter, equipped with infrared sensors, does not add time for inserted money if the meter has expired and the car has not moved. The meter also keeps track of the expiration time, to counter claims that the meter had just run out. This prototype meter is an early example of the new line of intelligent autonomous machines. Whether or not this particular meter is successful, similar machines will soon be available in many application areas.

Now move the level of sophistication yet one notch further up, from hardware that will not allow theft, to hardware that directly disallows the commission of a crime. A simple first example illustrates the idea: In some societies, such as Singapore, laws require the flushing of toilets after use, with a stiff fine for not flushing. Many new public toilets in the U.S. sense that a user has departed and flush themselves automatically, making it impossible to carry out the "crime" of "failure to flush."

As another example, if the U.S. society is unwilling to restrict the sale and ownership of guns, it could create guns that only the owner would be able to fire, as mentioned in a quotation at the start of this chapter. An implementation might involve verifying the owner's hand geometry or fingerprint before firing, or might use a special enabling ring the owner wears. Such a system is not much different from a reliable trigger lock, but an owner can leave the trigger unlocked, while the other systems would reset themselves after each use. Guns could also have disabling mechanisms that would prevent them from

discharging in public areas, since a gun owner ought to buy a gun to protect himself in his home, not to shoot at someone in an airport or a store.

Summary.

Objects ought to be made crime-proof if possible, though the techniques must not interfere with legitimate uses of the objects, and it must be difficult to disable the crime-proof features. Otherwise, objects should be fingerprinted and tracked—especially dangerous, valuable, or stolen objects, or objects that might be misused. Data should also be fingerprinted and tracked where the data is essential or valuable, and where theft or a leak are likely. The tracking will lead to a great deal of computerized record-keeping and data retrieval—a problem I do not want to minimize—but rapid progress is making it easier and cheaper to work with huge data files, and developing such record-keeping software is simpler than many other software projects.

5. Surveillance
everywhere in Public

And moving through a mirror clear
That hangs before her all the year,
Shadows of the world appear.
...
"I am half sick of shadows," said
The Lady of Shalott.

—Alfred Tennyson, *The Lady of Shalott,* 1842.

In this and the next chapter, the discussion of surveillance and privacy requires the concepts of public and private space. These concepts help determine which information about individuals should be accessible, either openly and publicly, or by law enforcement with a court order. I contend that it is now beneficial, even necessary, for governments (or the proper authorities) to carry out extensive surveillance in public, while it is equally desirable to restrict or eliminate private surveillance carried out by companies and individuals. In fact, the public surveillance should help identify and limit the private surveillance. Surveillance by a government can spread across a country, with comparison and correlation of the data. Combined with attention to the country's borders, this would eventually reduce the areas where crime and criminals can hide. In contrast, surveillance by a company or a gated community must be limited in scope; such surveillance is inherently undemocratic and will just encourage crime to move elsewhere, especially to poor areas.

Imagine you are a homeowner in a rural area, sitting on your porch watching a stream of large trucks drive past, delivering mysterious chemicals to a newly constructed nearby plant. You are

concerned—by some law or other the words "Hazardous Material" appear on the trucks, but nothing else. In the U.S. there may have been zoning hearings when the plant opened, but that says nothing about the trucks' contents now. If you tried to follow or investigate as an individual, you would be at a disadvantage compared with the plant owners, who could easily put you under private surveillance. Proposals in this book will redress the imbalance of power by requiring that information be available about all such movement of commercial goods through public space.

Surveillance goes hand-in-hand with the personal identification of Chapter 3 and with the object identification of Chapter 4. For example, an observed automobile needs reliable identification as an object, but the owner and the driver of the automobile need equally reliable identification.

The abuse of surveillance technology for illegal or unethical ends is of particular concern. This book suggests wide surveillance to limit crime, but misuse of these new capabilities would negate any advantages. Thus, controls and oversight, as well as the logging of data about those carrying out the surveillance, must be in place from the beginning.

Public Space and Private Space.

Divide all activities, including physical movements and data transmissions, and all objects, including physical objects and data, into two separate areas: *public* space and *private* space. It is difficult to give formal definitions, but as a rough guide, public space refers to what a nosy neighbor in a small town might know, where the nosy neighbor might go. Private space is what the same nosy neighbor should not know, or where he or she should not be. Completely different rules should apply for access to the two realms. Again as a rough guide, public space is accessible to all, and information about public space should be openly available. In contrast, private space is inviolate and inaccessible, except with permission or under special circumstances. These "special circumstances" will require an emergency or a court order.

Everyone should have their own private space, both physical pri-

vate space and data private space, at home and in the workplace. Private space at home includes the physical home itself, any actions inside, and any data stored inside. Each individual should have private space set aside in the workplace. The workers at the bottom of a corporate ladder should have their own physical private space that is secure from intrusion by the head of the company. Similarly each worker should have secure private data space, separate from the data space devoted to shared company business. In this model, the world looks like a sea of public space with isolated islands of private space; most connections between these islands of private space would go through public space.

There should also be provision for private communication whenever two or more parties mutually desire it. The contents of any such communication must be private, but the fact that communication occurred, the parties to it, and the time are all public. If either party wants to make a private communication public, then that conversation moves into public space, but whether it is legal to release the contents depends on complex laws related to confidentiality, such as laws about doctor-patient, priest-confessor, or lawyer-client relationships. Also in private space are the contents of private vehicles unless these contents are hazardous, and the identity of a person on foot or in a private vehicle, although camera images of the people are in public space.

Examples of public space include the external movements and identity of vehicles, the *contents* of commercial vehicles, the external movements of persons (that is, scanned images of people in public), the identity of persons in commercial vehicles, the identities of parties to ordinary mail or electronic communication, actions at a trial, actions at a meeting sponsored with public funds, and contents of public documents as long as revealing them does not compromise individual privacy.

A number of actions and records in public space should only be available under court order. These include health and financial records, and more generally, records from businesses and from governments about transactions between them and an individual. This includes the transfer of cash, as well as electronic transfers of money.

Also requiring a court order would be logs of data about the parties to conversations by mail, electronic mail, or by phone. Phone logs are the only ones carried out at present. This logged phone data would not include actual conversations, so voice analysis would not be an issue. In contrast, logs of image data of persons on foot or in cars should be accessed for processing under court order to attempt to identify the individuals, using feature analysis software.

Cyberspace, the new electronic realm, also should have private and public areas. Except for anonymous users, society should log the participants of forums, chat rooms and other such interactions of individuals. Just as the phone companies must keep track of phone owners, laws could require that Internet service providers track their users—who they are and when they are using the service, but not the contents of their interaction. Individuals should not have to worry that the content of their electronic conversations might be recorded and used, even under court order. Of course any participant could record what goes on in a chat room.

The United States has partially met these requirements with freedom-of-information laws, open meetings laws, and privacy laws in various states. I suggest going much further, so that the public information mentioned above is always logged and is often immediately and continuously available to individuals. (In computer jargon, one says "available on-line.") As mentioned above, the remaining logs would be available only under court order.

Current Surveillance in Public Space.

The world is experiencing a vast increase in the amount and sophistication of surveillance. Problems such as crime and terrorism give motivation, while improving technology provides the means in ever more effective and cheaper forms.

For example, the use of video cameras for surveillance in the United Kingdom has recently been growing fifteen or more per cent annually, to an estimated 200,000 cameras. All public areas and vehicles are candidates for such increased surveillance. The technology in use is astonishing: pin-hole cameras, full pan, tilt and zoom, infrared capacity for night vision, computer-assisted operation, motion

detection, and tamper-resistant casings. Face recognition software is under development.

Many in the U.K. fear that this technology is "out of control"—progressing without debate or challenge. Opponents worry about misuse and claim that improved crime statistics are misleading or wrong. One claim is that the surveillance moves crimes to areas without cameras, but if all public areas have cameras, there will be nowhere in public for the crime to move. One must then worry about crime moving to private areas where cameras are not allowed. All access to private areas should be through public space, so that surveillance data will show the movement in and out of the private areas. Opponents are also concerned that surveillance technology from the U.K. is helping support secret police and military authorities worldwide. It is an important "arms industry" for the U.K.

Police officers in vehicles now frequently turn on a video camera whenever they stop a motorist—thereby providing protection for both the police and the public. Just knowing that the video camera is running may constrain both police officers and the individuals they stop, a fact consistent with this book's goal of limiting crime, rather than just detecting it.

As other examples, drug enforcement agencies in the U.S. are shifting to new sophisticated detection techniques. The U.S. government wants to use social security numbers to track individuals for welfare reform and paternity proceedings. California has proposed sensors on cars that will report compliance with pollution controls of cars during their operation. An Internet provider is logging, cataloging, and indexing all news messages sent over the Internet. Airline travelers must often show a picture ID in order to check baggage—current policies are not uniform and depend on the level of security alert at the airport, but if trends continue, anonymous air travel will no longer be possible.

It has always been easy for law enforcement (or even private agencies) to keep track of a few individuals, using personal surveillance and other labor intensive methods. Now that computer technology has enabled the same level of scrutiny of large numbers of people, objections are raised not because of any new capability, but

because of the extent of the capabilities. As mentioned elsewhere, I wish to see the technology used with great care and restraint, so that data is mostly retrieved after the fact with a court order. At present, law enforcement officials favor the increased surveillance, while privacy advocates fear and oppose it. I suggest using the capabilities fully, but with care and with tight controls.

Surveillance in the Workplace.

Much surveillance already goes on in the workplace, but employers of workers using computers can now track every keystroke—what the keystroke was for and when it occurred. Employers can also track their employees' on-the-job activities, such as web use or e-mail. They can track higher level performance data, at worst turning the company into a sweatshop. This tracking is not necessarily bad; much depends on the intent and the use of the information. For example, a productive employee might welcome the surveillance of unproductive co-workers. As businesses shift toward telecommuting, work will shift toward pay for performance, and one hopes for humane and effective performance criteria, rather than counting computer keystrokes. Then the amount of time spent working and the time of day that work occurs will be increasingly irrelevant.

Here are several examples of current surveillance practices.

Employees who read residential meters commonly carry a computerized data entry terminal into which they log their readings. That looks like a simple efficiency step except that the terminal logs the time of data entry. Before the terminals came along, employees could hurry through their work, finish early, and claim they worked a full day. Now they are partial slaves of this electronic device, called "the boss" by one of my meter readers. Most delivery services (except for the U.S. Postal Service) have similar data entry devices that are looked upon with paranoia and hatred. While such devices might uncover crimes, they are primarily used to monitor performance.

One U.S. Federal Reserve Bank carries out surveillance checks not fully understood by the supervised employees. This bank has a flood of arriving bags of currency, which employees carefully open under continuous videotaped surveillance. If a packet of bills turns

up missing, the videotape proves it was not in the original sealed bag, and therefore the problem is with the sender of the bag. Individual packets of bills may contain an extra bill or may be missing a bill. A given bag may have a deficiency or excess of money in this way. As employees count the money, there are opportunities to palm a bill and take it home. These employees, typically unsophisticated high-school graduates, understand that they cannot grab bills from each bag, making every bag deficient, but they know nothing about the elaborate statistical analysis of the excess/deficiency data over their entire employment period. Just one stolen 20 dollar bill per week will show up in time as a statistical anomaly, unsuspected by the dishonest employee. These statistics do not prove theft; nevertheless, the bank can transfer and has transferred such employees to less sensitive work without a confrontation.

In my view, companies may carry out surveillance of their employees, and of the employees' electronic mail, but these employees must know the full extent of this surveillance. Thus it is not acceptable to trick them as the Federal Reserve Bank does above. Avoiding tricks is simple self-interest for a business—this avoids the side-effects of an employee finding out about the trickery and avoids the antagonism and paranoia that such policies engender, policies that lead ultimately to demotivation and lack of productivity.

Surveillance and Control.

Beyond surveillance, many societies withdraw the right of privacy from criminals, and often desire to exert that ultimate control over individuals: imprisonment. The effort attempts to make crime impossible by sending the criminals to prisons. The U.S. recently has seen a vast increase in the prison population, with the largest growth from non-violent offenders. Whole industries are now nourished by prison systems in the U.S. Prisons are breeding grounds filled with hatred and mental illness, and with criminals who can continue their wrongdoing from inside a cell. Though crime is indeed down, the price to individuals and to society is high, including intangible costs of ruined and non-productive lives. The prisons are not working; the associated parole, retraining, and drug treatment programs are just

as bad—limited and overburdened. Surely the U.S. society can do better.

Leaving aside issues of rehabilitation in prison, the goal is not really confinement—the goal is control, and a variety of devices similar to those used for surveillance will provide effective and inexpensive control. These include monitors attached to a wrist or leg or around the waist, as well as special monitors in cars and homes. Devices attached to a person can have additional control features, such as administering an electric shock, while features provided with a car could stop or disable the car. Readers may regard such devices as cruel and manipulative, but a prison—that "black flower of civilized society"—is the truly cruel method. Surely most convicted criminals would choose a monitoring device over prison, and often the choice is probation with a monitor or continued confinement. Problems in the U.S. with convicted criminals and prisons are very complex, but surveillance tools like these should be used on a far wider scale as an inexpensive and effective way to deal with many lawbreakers, a way that can allow a cooperating individual to participate fully in society.

Probation officers are charged with the supervision of released prisoners. In the old days, these officers might set an alarm for the middle of the night so that they could wake up and call the home of a probationer in their charge, to verify that the individual was at home. Then there were telephone-based monitors that determined if an individual was home, but not where they might be, and it only checked now and then, every few hours. Hardware from the Global Positioning System will now keep track of a monitored individual's location, accurately and continuously.

Stalking has become a serious problem, especially for celebrities or divorced parties, and even great wealth will not always protect the stalked party. Restraining orders issued by a court to a stalker do not work, as numerous cases show; the stalker simply violates the order and kills, often expecting to be caught. As a means to control stalkers, society could require, subject to court review, that a convicted stalker who was not in jail wear a device indicating his or her position. Law enforcement, and the stalked party themselves, would always know where the stalker was and would be alerted if the stalker came close.

Autonomous agents (see Chapter 11) could enforce restrictions on geographic movements.

The potential is great for abuse and overuse of the surveillance devices described here. For example, a defendant at trial who is regarded as a risk may be required to wear restraining shackles, restraints that are considered prejudicial to a jury. The option is now available for a stunning waist belt that the defendant can wear without revealing its presence to the jury. However, in a recent trial in California, the defendant, acting as his own attorney, talked and interrupted the trial to a degree that finally angered the judge, who ordered the belt's stun features activated. The eight-second electric stun is incapacitating, but the manufacturer claims it is safe. In this case parties agreed that the defendant posed no threat but was just behaving in an irritating way. Aside for the obvious risks, say to someone with a heart condition, society must not tolerate possible abuse of these control features, and any use of stunning devices seems indefensible, tempting law officers to abuse their power, possibly harming the victim, and leading to difficult lawsuits. The ultimate form of control would have devices implanted in every person, a dark scenario hinted at in science fiction and now in the mainstream. People who fear that soon everyone will wear these control devices would be better off worrying that soon everyone in the U.S. will be in a prison.

Individuals might willingly choose to wear surveillance devices. These could keep track of the location, health, and well-being of the wearer, perhaps monitoring vital signs and allowing the user to sound an alarm. The elderly sometimes use such devices, while a modern mobile phone can provide similar functions. Truly voluntary use by lawbreakers can occur in cases such as child abusers who would like to have the knowledge of surveillance to help them keep their temper in check.

From "finger" to "Mirror Worlds".

The display of surveillance information is another challenge. The "finger" utility of Unix systems provides the crudest possible display: "finger xyz" prints brief messages about the location and activities of an individual (actually a computer account) named "xyz." A finger

can be invoked from a remote location over the Internet and will typically say whether the individual is currently using the machine, what the individual is doing, and the latest unread mail. It is possible right now to issue continual finger commands, twenty-four hours a day, about a given individual. One can then assemble a log of that individual's computer activities.

This finger utility provides anyone (in the world!) with information, including facts from private space. As these systems get more widely used, many people are rethinking their old permissive policies about what finger should provide. Machines now often give little information or nothing at all in response to finger. The public space/private space distinction in this chapter will help answer questions from the current debate about finger.

At the opposite extreme in display sophistication from finger are the "mirror worlds" of David Gelernter. This computer scientist has written a book that describes spectacular possibilities for the display of information about the world—he would provide most facts anyone could imagine though these displays. In his new world, an individual could electronically visit a city's government, learning everything about the current questions under consideration by the government, visiting with other electronic eavesdroppers, or leaving software agents to monitor for specific activities. Gelernter does not emphasize the issue of which information should be publicly available and which should be private but concentrates on novel display methods and on implementation.

After writing his book, Gelernter was the victim of a vicious package bomb. I am happy to report that he is back on-line, disabled but still well able to function in his role as a leading computer researcher. The Unabomber sent this bomb, one of a sequence of attacks against prominent academics and others, decided on by a strange "Luddite logic"—in this case because of the popular book Gelernter wrote. Many of the activities related to mailing the package that exploded would be in public space as defined here. Perhaps not yet, but one day it will be simple to keep such complete records that law enforcement officers could trace this bomb back to the individual who mailed it. Society should disallow anonymous package mailings,

or at least log the identity of an anonymous mailer, and determine the identity in a reliable way. (See Chapter 7 regarding anonymity.) Other techniques in this book would help catch bomb-makers early in their career, without waiting for an explosion, but in the end only an oppressive society could be sure there were no bombs.

Proposals.

Some level of surveillance has long been part of daily life. Neighborhood block patrols jot down license numbers of unfamiliar cars on the block, saving the numbers for use in case of a crime. As another example already mentioned, phone companies keep computer logs of long-distance calls, including origin and destination of the call and the time interval. Courts and law enforcement officers can access these records, which often play an important role in trials. There is little public outcry about the existence of the records; people affected by a crime welcome the information. These telephone logs are a model for other information in public space.

Individuals often oppose surveillance and control as described here until they are victims of a crime or suffer a preventable tragedy. Then they change their mind and long for methods that would have prevented the crime or would bring the criminal to justice. A single crime, such as the death of a loved one, can affect and even poison one's entire life.

Society ought to log all activity and to track all objects in public space, though this is at present a distant goal. Here "log" means to keep computer records that remain accessible indefinitely. Selected parts of this information would be openly and immediately available to individuals, for example, information about the transport of hazardous materials near the individual's home or workplace. The remaining information would be available under court order. Keeping track of everything and everyone dovetails nicely with the identification and fingerprinting proposed earlier in Chapters 3 and 4, and with the monitoring by agents discussed later in Chapter 11.

Each time authorities identify an individual in public (for example, as the individual takes public transit), computers would log the time, the location, and the person's identity. Cameras in public space

would record images that computers analyze in real-time and after the fact in case of a crime. The computers would compare recorded images with files of images of criminals.

Notice that similar low-tech logging occurs now, as with the block watches mentioned earlier, or with a company's parking lot that videotapes all entering cars. Companies and governments carry out such surveillance and logging in an uncoordinated, haphazard fashion. Coordination of all this data is the hardest and most important part, but part of the coordination work can be put off until the data is needed to solve a crime.

Gathering such vast quantities of data, and saving and processing the corresponding huge files of information about events and objects in public would not be as hard or as expensive as it might seem. The computers would create cross reference files based on the vehicle ID for cars, on the person's name for individuals, and on the fingerprint for objects. Then searches for the location and movement of specific objects would be feasible and eventually efficient. The cost of hardware keeps dropping, and consider that the U.S. society spent over $50 million searching for a catching the Unabomber; such money could be better spent on strategies that would lead to early capture of such people.

There was a long-term commitment in the U.S. to modernize and automate the Air Traffic Control (ATC) system. The goal was to eliminate most human controllers, replacing them with software. Attempts to produce this software have now been abandoned. Within a multi-billion dollar budget, the programmers could not get it to work. Such a cautionary tale might make this chapter's ambitious-sounding proposals seem problematic. However, the ATC system needs to guide planes in for a landing in real-time, with a vanishingly small probability of a software failure, such as guiding two planes into one another. The surveillance systems proposed here need only log time and location and identity for later computer processing with a court order. This is a far simpler task.

Along similar lines, consider attempts of the U.S. to monitor and control its border with Mexico. This is a more difficult problem than simple traffic surveillance because not just surveillance and logging

of data is wanted, but control of people and objects moving into the U.S. The U.S. needs to spend more in order to track cars, trucks, planes, and boats as they enter, and it also needs to track individuals on foot, difficult as this is. The alternative of no control on the border will not work, nor will the strategy of raising the standard of living outside the U.S. so that people do not want to come in as illegal aliens.

If the only goal was making crime impossible, then maximum surveillance and tracking would be best—everyone and everything tracked all the time. Law enforcement would type in a name and immediately find out where that person was. But such tracking is not technically feasible and is undesirable as too great an infringement on privacy and freedom. Hence comes the compromise of keeping records of objects and people, records that a court order will give access to when needed.

People want basic privacy rights, even in public space, like the right to solitude, to intimacy, anonymity, and autonomy. The problem is that crime defeats this, so that without control of crime, these rights are gone anyway. People would like to wander in a park or go backpacking in the woods without fear of government intrusion, or even government monitoring. But these same people want to be free of crime, of anxiety about crime, in their solitary walks. The solution of taking weapons for security does not work; no one could carry enough weaponry to insure their safety. Instead, people need the government's help to make their walks safe, so that people will have the illusion of freedom, the illusion of a lack of intrusion.

These surveillance proposals must include a description of the checks and limitations on the surveillance machinery and on those who control it. This is an all-important issue, particularly for opponents of surveillance systems. Surveillance and control by the government with no limitations could lead to total oppression. Abuse of surveillance by individuals might expand crime. Elsewhere this book argues that the primary check on the power of those who control the surveillance mechanisms is open access to all information about these mechanisms. It would even help to have public surveillance images publicly available. Individuals must know what data is gathered and how the data is used; this applies particularly to data related to the

individuals themselves. Another important check is the logging of all surveillance activity, logging that cannot be turned off by those carrying out the surveillance—a standard practice for administrators of computer systems: they can do anything on their system except turn off the record of everything they have done. Then there must be oversight committees and review procedures to follow the actions of those in control.

6. Privacy
Using Cryptography

Apple's chief pledged to fight federal demands to help mine data from an iPhone used by one of the shooters in December's [2015] terrorist attacks in San Bernardino.

"... the U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create. They have asked us to build a backdoor to the iPhone."

"Once created," he wrote further, "the technique could be used over and over again, on any number of devices. In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks from restaurants and banks to stores and homes. No reasonable person would find that acceptable."

Individuals from the U.S. government said: "This is the kind of case where companies like Apple need to demonstrate that they're good corporate citizens and comply with lawful court orders." They also said: "No device, no car, and no apartment should be beyond the reach of a court ordered search warrant."

—E. Nakashima, "Apple vows to resist FBI,"
The Washington Post, February 17, 2016.

Privacy has always been an important issue, particularly in the U.S., but many Americans assume the existence of legal privacy guarantees that are in fact not present. U.S. citizens mainly have privacy rights in their homes and privacy against wiretapping, but relatively little privacy in public. In the context of this book, privacy inside one's own private space is an absolute necessity, as is protection of private conversations and private data.

Ironically, just at the time that technology has made surveillance and computerized record-keeping available to invade privacy, theoretical and technological advances, especially cryptography and its computer implementation, have given society the potential for absolute privacy of communication and data storage. These cryptographic techniques—intricate, clever, and effective—alter the whole privacy landscape. If society fully uses them, individuals can be certain of the privacy of their personal communications and of their personal data.

Consider the security of a communications line between two points. Without cryptography, one must resort to physical security—barbed wire, guard dogs, land mines, or whatever—to prevent a physical tap on the line. With cryptography one can easily secure the line against a tap, and the cost of this method is independent of the distance between the connected points.

Society should fully use this technology, so that individuals can talk to one another or write in diaries without fear. Information and communication can pose threats and cause harm, but the benefits to society in enhanced free speech and individual privacy outweigh these problems. It may sound simplistic to assert an unrestricted right of individuals to secure communication and secure data storage, but this right has always been present with extra effort: individuals can talk alone in the woods or can employ special code books. As A.M. Froomkin says in an Internet document about cryptography, attempts to abridge these rights using a form of "cryptographic prohibition" will certainly fail, as prohibition failed.

The U.S. government, partly under the influence of the National Security Agency (NSA) and of law enforcement, has for twenty years attempted to suppress the development and use of cryptography. With widespread cryptography use, government spokesmen argue, information might no longer be available through wiretaps, and the country would have more trouble combating crime. A later section in this chapter goes into the issues more thoroughly, but in brief, wiretaps are no longer desirable or effective, while suppressing cryptography actually endangers our national security.

There are three benefits to the use of cryptography, benefits that the U.S. has not been fully enjoying: First, proper use of cryptog-

raphy is the very best way to ensure privacy. Second, cryptography, again properly used, is absolutely crucial in helping protect computers and networks against attacks by hackers or terrorists or even an act of war. Third and finally, strong cryptography will help our computer hardware and software vendors compete more effectively for business in global markets. Enhanced privacy and security are the all-important reasons for society to embrace cryptography use, yet in the U.S. the main push for relaxation of cryptography restrictions comes from a desire for business competitiveness.

The next three sections go into technical details about cryptography, since readers cannot fully understand the issues without these details. Less technically oriented readers may want to skip these sections.

Cryptography.

The words "cryptography" and "encryption" refer to methods of scrambling a message so that its content and its meaning are hidden if it is intercepted. The intended recipient of the message knows the method of unscrambling (the "key" for "decrypting") and is able to recover the original message.

People have used cryptography for thousands of years. For example, the Caesar Cipher, which was used during the time of Julius Caesar, wraps the alphabet from A to Z into a circle. Encryption employs a fixed shift, say of 3, to transform A to D, B to E, and so on until W to Z, X to A, Y to B, and Z to C. Thus a message "ATTACK" becomes "DWWDFN" and appears incomprehensible to someone intercepting the message. At the other end, one can reverse the transformation by stepping 3 letters in the opposite direction to change "DWWDFN" back to "ATTACK."

This example illustrates many concepts from cryptography. The basic method used, moving a fixed distance around the circle of letters, is the "encryption algorithm." The specific distance moved, 3 in this case, is the "key" for this algorithm. Often the basic algorithm is not kept secret, but only the specific key. The idea is to reduce the problem of keeping an entire message secure to the problem of keeping a single short key secure. For this simple algorithm there are

only 26 possible keys: the shift distances of 0, 1, 2, etc. up to 25, although 0 leaves the message unchanged, so a key equal to 0 is not going to keep many secrets. If an interceptor of this message suspects the nature of the algorithm used, it is easy to try each of the 25 keys (leaving out 0) to see if any meaningful message results—a method of breaking a code known as "exhaustive search." In this case the search is easy.

Attempts to break a code, to decipher an encryption algorithm, are called "cryptanalysis" and are usually a difficult enterprise carried out by professionals. In this century, more sophisticated encryption algorithms were devised, mostly by those involved in warfare. During World War II the Germans used a complex algorithm called the "Enigma" code, implemented with a machine like an old-fashioned mechanical calculator. British intelligence, with the help of others, carried out the difficult cryptanalysis of this code and knew many of Germany's secret messages during the war, knowledge of critical importance to the war effort and perhaps to shortening the war. Much of the story reads like a lurid tabloid story considering that a principal architect of the successful cryptanalysis, the brilliant young computer pioneer Alan Turing, committed suicide after the war because of British persecution of him as a homosexual.

From 1945 to the present, enormous increases in computer capabilities have allowed use of ever more sophisticated encryption algorithms. Cryptanalysis capabilities have increased correspondingly. It is remarkable that, just as the vast expansion of data communications calls for new security methods, similar hardware improvements enable new approaches to cryptography which provide the needed security.

A standard fallacy in this area, popularized by movies like *WarGames*, has to do with the ability of teen-aged hackers to break into computer systems. Such hackers, clever though they are, rely on security holes in systems and on their own patience. The public thinks that these same hackers would be able to break the security of modern cryptographic codes. While such cracking of an encryption method is a logical possibility, in practice, skilled researchers must try to break these cryptographic systems for years before they are con-

sidered secure. The difference with breaking into a computer system is that such a system is extremely complex and constantly changing, continually leaving places for security holes.

Another fallacy comes from people enamored with cryptography and its use. These individuals expect complete and perfect security (called *unconditional* security in the literature) if they just use a strong cryptographic algorithm. (The word "strong" refers to an efficient method that is hard to break.) Even with strong systems, the cryptographic key must be kept secret, and this key becomes a point of weakness, a point for opponents to concentrate on. In the complete cryptographic process, distribution and maintenance of keys is the most difficult part of the use of cryptography, subject to endless errors and bugs and security holes.

Now for a subtle point. There exist "perfect" encryption methods with a mathematical proof that cryptanalysis is impossible. The simplest of these methods is called the "one-time pad." A later section discusses this area further and explains why these perfect methods are not practical to use in modern communications. For the practical methods, there is always the possibility that a clever researcher or even a clever hacker could break the method. Also cryptanalysts can break these other methods using brute-force exhaustive searches. The only issue is how long it takes to break them. With current strong cryptographic algorithms, the chances are that there are no short-cut ways to break the systems, and current cryptanalysis requires decades or millennia or longer to break the algorithms by exhaustive search. (The time to break depends on various factors including especially the length of the cryptographic key.) To summarize, with these methods there is no absolute *guarantee* of security, but experts expect them to remain unbroken.

A scenario at this point may help clarify matters. A user could maintain a diary or other secret text on a personal computer in encrypted form. He could enter a secret password to gain access to the information, both to read or change old entries and to add new material. One could set this up using today's technology so that the security would be proof against any anticipated method of breaking the code for the next twenty years, say, or longer if desired. Thus if

the person dies and his equipment is taken into custody, no manipulations with supercomputers or by the smartest cryptographers in the world would allow decryption. Without the secret password the data remains inaccessible. One could try all possible passwords, but that would only work if the user had not chosen a long enough password, or if he chose a common word or phrase for his password. Software is available to keep unbreakable secrets. Nothing on earth will keep individuals from availing themselves of this capability.

In addition to the ability to keep secret diaries and other secret data, cryptography allows one to transmit data in secret. This includes all data transmission, from phones and cellular phones and pagers to television and internet traffic. In fact, computer scientists often do not distinguish between data transmission and data storage, since the latter is regarded as a transmission from "now" to "then."

Public-Key Cryptography.

Cryptography gives other very useful capabilities. One can affix the electronic version of a signature onto a document in a way that detects any change in the document and that authenticates the entire document as originating with the signer. It is as if an ordinary signature were scrawled across the entire document, preventing any changes. It is not feasible for a person to fake a digital signature. These near-perfect signatures make the digital realm much safer than the non-digital. For example, one can sign and authenticate anything that can be represented digitally: music, pictures, and videos, as well as transmitted text.

One can provide both signature and secrecy for a message, so that only the intended recipient can read the message, and only the designated originator can have sent the message. Encrypting for secrecy, adding a signature, and later authenticating the sender, all have been automated with software to provide convenient practical systems for users who need not know how these systems work.

There are also the capabilities of public key cryptography. In such systems each user creates a pair of keys: a secret key for decryption and a separate public key—available in a public directory just as a phone number is available in a phone book—for encryption by the

person sending the message. In order to sign a message, the user employs his secret key, normally used for decryption. Secrecy and authentication systems now available on the Internet are based on one of several standard public key cryptosystems, and again users need not know how they work to employ them.

For example, suppose Alice and Bob wish to communicate using public key cryptography. (In the literature on these matters, the involved parties are always named Alice and Bob. During the cold war the bad guy who pretends to be Bob was called Boris.) Both Alice and Bob create pairs of public/private keys, and they each make their public keys available to everyone in some public key file. If Alice wants to send a signed secret message for Bob alone, she first fetches Bob's public key from the public key file. Alice uses Bob's public key to encrypt a message that only Bob can decrypt with his private key. If Alice only wanted secrecy, she could send this message as it is. Since she also wants to prove she is the sender of the message, she uses her own secret key to further scramble the already encrypted message for the purpose of adding her signature for authentication. Alice tells Bob to expect this message from her (without worrying about the secrecy of this latter message), so at the other end Bob fetches Alice's public key to carry out the first stage of message retrieval. Then he uses his own secret key to come up with the original message Alice sent him. Because of the signature (decryption with Alice's secret key), only Alice can have originated the message, and because of the encryption with Bob's public key, only Bob can decrypt and read the message. There are additional subtle problems, but modern systems handle these without worrying the user. In practice, these systems use a hybrid of public- and private-key cryptography for efficiency. Alice and Bob can communicate securely and secretly in this way using software without understanding public key cryptography at all.

In the discussion above, Alice received Bob's public key from a public file on a server computer. This computer must authenticate *its* message using public key cryptography also, so that Alice can be sure she's really getting Bob's key. There is a clever way to do this using a signature of the computer supplying the key. If Alice has already registered with this computer, she can verify the signature directly.

Otherwise, this signature will in turn be signed using the public key of yet another computer. In this way a sequence of signatures is created, called a *certificate*, and the certificate terminates in a signature that Alice can verify from having directly visited the given computer. This may sound confusing, but it works, and users need not understand how.

Perfect Cryptography.

This section discusses an interesting subtle technical point about cryptography. Consider the Caesar cipher of the previous section, and associate the numbers 0 through 25 with the letters "A" through "Z," that is, "A" is associated with 0, "B" with 1, "C" with 2, and so on until "Z" with 25. One can represent the previous shift of 3 in the example by the letter "D," so that each letter specifies a shift. A special encryption method called the "Beale cipher" starts with a standard text like the U.S. constitution ("We the people ...") and with the message to encrypt, say "ATTACK." Write down the letters of the standard text on one line, followed by the letters of the message on the next line. In each column, the upper letter is interpreted as a shift to use in a Caesar cipher on the letter in the second row. Thus below in the second column, the "E" in the first row means a shift of 4 is applied to the letter "T" in the second row, to get the letter "X."

```
Standard text:      WETHEP
Message:            ATTACK
Encrypted message:  WXMHGZ
```

The person receiving the encrypted message must know what the standard text is. Then this receiver can reverse the above encryption by applying the shifts in the opposite direction to get the original message back. This method will handle a message of any length by just using more of the standard text. Notice that in this example the two "T"s came out as different letters in the encrypted message. For more security, one should not use a standard text as well known as the one in this example. Instead the sender and receiver could agree on a page of a book they both have with them as the start of their

standard text. All the security of this system resides with the secrecy of the standard text. There are a number of other subtle pitfalls with this method, as with most of cryptography, but these details are not helpful in this discussion.

A variation on this method, known as the "one-time pad," starts with a random sequence of letters for the standard text. Suppose for example one uses "RQBOPS" as the standard text, with the same message. Then encryption takes the form:

```
Standard text (random):  RQBOPS
Message:                 ATTACK
Encrypted message:       RJUORC
```

The receiver must have the same random string of letters "RQBOPS" around for decryption. As the important part of this discussion, I want to show that this method is *perfect* as long as the random standard text letters are kept secret. Suppose the message is "GIVEUP" instead of "ATTACK." If one had started with random letters "LBYKXN" as the standard text, then the encryption would have taken the form:

```
Standard text (random):  LBYKXN
Message:                 GIVEUP
Encrypted message:       RJUORC
```

The encrypted message is the same as before, even though the message is completely different. An opponent who intercepts the encrypted message but knows nothing about the random standard text gets *no information* about the original message, whether it might be "ATTACK" or "GIVEUP" or any other six-letter message. It is in this sense that the one-time pad is perfect.

In this century spies have often used one-time pads. The only requirement is text (the pad) of random letters to use for encryption or decryption. The party communicating with the spy must have exactly the same text of random letters. This method requires the secure exchange of pad characters: as many such characters as in the original message. In a sense the pad behaves like the encryption key, except

that here the key must be as long as the message. But such a long key defeats a goal of cryptography: to reduce the secrecy of a long message to the secrecy of a short key. If storage and transmission costs keep dropping, the one-time pad might again become an attractive alternative.

U.S. Cryptographic Policy.

The United States has been fortunate in its preeminent position in cryptography. Government employees specializing in cryptography enjoyed an advantage over colleagues in other countries and were reluctant to give it up. The year 1976 brought a revolution in the form of an unclassified article, "New directions in cryptography," by M. Hellman and W. Diffie, introducing the concept of public key cryptography. This was followed in 1977 by a *Scientific American* article describing a specific system, now known as the "RSA public key cryptosystem," presented with full details in 1978 ("RSA" after its three inventors: R. Rivest, A. Shamir, and L. Adleman). There followed a flood of articles and research on cryptography, including much work abroad. Government cryptographers in America, especially those working for the National Security Agency (NSA), were alarmed and wanted to suppress research in this area. One proposal would have rendered all cryptography research "born classified," that is, restricted as it was produced, as is still the case with nuclear weapons research. But reason held, and a voluntary agreement asked U.S. researchers to send cryptography articles to NSA for a "security review": does any of the content affect national security? Some researchers complied while others did not (I did comply). My feeling now is that it was a wasted effort. The cows had already escaped, while they worried about an open gate. There is plenty of theory published openly world-wide to construct modern strong applications using cryptography.

Cryptographic technology is still classified as "munitions" in the U.S., as if it were an explosive device. Special export restrictions apply, and the State Department must give permission for export of any of this technology; permission for the export of strong systems is always withheld. The effects of these export laws have been grave.

U.S. computer vendors cannot usually afford to create two systems: one with weak or with no cryptography for export outside the U.S. and one strong system for local use. Thus strong systems to support individual privacy have not been as available as they otherwise would have been, cryptography has not been widely used for system security, and the bans have limited the competitiveness of U.S. exports. For example, the Data Encryption Standard (DES) algorithm (see the description below) uses a 56-bit key—too "strong" for export, so that companies cannot export a Unix system with DES included, even though one can find DES implementations everywhere, in texts and on the Internet. These export restrictions are under continual revision; recently oversight has moved from the State department to the Commerce department. There are also U.S. proposals to allow export of cryptographic algorithms with longer keys as long as the keys can be delivered to the U.S. government under a court order. Of course foreign governments do not want to go along with such ideas.

In an attempt to heap deserved ridicule onto the U.S. policies, Adam Back of the University of Exeter coordinated implementation of the RSA cryptosystem—a strong system indeed—in just 3 lines of code (222 characters), using a powerful language called Perl. Back is selling T-shirts with this code printed on them—legal to export *to* the U.S. but not *from* the U.S. (I own a shirt.) Back says, "A few people over in the U.S. are thinking of having this tattooed—for an export-controlled torso. One useful application for the tattoo idea is that illegal immigrants in the U.S. could get the tattoo in place of a green card—[regulations] would make it illegal to deport them." By including the text of the code here, this book becomes munitions and is also export-controlled (in theory only, I hope). So here goes ...

```
#!/usr/local/bin/perl -s-- -export-a-crypto-system-sig -RSA-in-3-lines-PERL
($k,$n)=@ARGV;$m=unpack(H.$w,$m."\0"x$w),$_=`echo "16do$w 2+4Oi0$d*-^1[d2%
Sa2/d0<X+d*La1=z\U$n%0]SX$k"[$m*]\EszlXx++p|dc`,s/^.|\W//g,print pack('H*'
,$_)while read(STDIN,$m,($w=2*$d-1+length($n||die"$0 [-d] k n\n")&~1)/2)
```

When this story first appeared (June, 1995), two major U.S. newspapers printed the code, each with one end blurred so that they did not actually print the full code—but they blurred opposite ends: two

newspapers, scissors and tape will reconstruct the code. Both newspapers are shipped world-wide. One Internet user asked which newspaper broke the law. The Exeter group also encourages Internet users to include the code in signatures at the end of mail messages and news postings. Their message says, "Have *you* exported a cryptosystem today?"

On the hardware side, IBM Corporation originally designed a conventional encryption algorithm for commercial use. Soon IBM's lawyers made frantic noises about the company's potential liability if the system were broken, so IBM secured the involvement of the National Institute of Standards and Technology (NIST—then called the National Bureau of Standards) to design and create a hardware chip for conventional encryption. The rest of the story is long and involved, but in the end the NSA helped them design an algorithm called the Data Encryption Standard (DES) that was easy to implement in hardware. At the time there was speculation that the NSA deliberately weakened the algorithm just enough so that they alone could break it. There was also speculation about "back-door" access inserted into DES, meaning a shortcut way to decrypt if one knows how. It now seems unlikely that any such back door exists. However, the final system used a 56-bit key inserted into 64 bits, so that 8 bits of the key were wasted for no apparent reason. At the time (in 1980), Martin Hellman estimated that with a U.S. 3.6 million dollar investment one could break DES in about a year. The extra 8 bits would have made it 256 times as hard to break, so there was speculation then, continuing to this day, that the NSA carefully chose the key length so that they could break the cryptosystem while others could not.

The DES was supposed to be secure for 10 years, and its time has run out. Technology has overrun the algorithm, evidenced recently by teams of up to 22,000 volunteers using over 50,000 computers, who broke the DES using these distributed Internet resources over five months and later over thirty-nine days. Even more recently, US $250,000 of special hardware allowed the Electronic Freedom Foundation (EFF) to break DES in just 56 hours, winning a contest sponsored by RSA, Inc. Current DES cracking systems use brute force to

try all 72 quadrillion possible keys, or at least try them until finding the right key—in half the time on the average. (The number of keys to try is just 2 to the 56th power.) Similar machines are surely in the hands of the U.S. government and foreign governments, so that it is time to use a longer key. Even a 64-bit key would take 256 times as long to break DES, so that a similar machine would take nearly two years. More recent systems use 128-bit keys—far too long for a brute force search to succeed with current technology.

At the same time the RSA system has been gaining acceptance worldwide as the best public key cryptosystem, though it is slow even when implemented in hardware. In the early 1990s the NIST was to choose a standard for public key cryptography and was apparently poised to choose RSA. However, NSA convinced them to pick as standard a new method that would allow authentication but not secrecy. In fact it was quite an accomplishment for NSA to devise a public key scheme which worked for authentication but could not be adapted to secrecy. The intent was to make this a widely-used and widely-available standard that would replace RSA. If RSA were used everywhere instead, it would allow ready secrecy as well as authentication. I expect that RSA will become the world standard in spite of NSA's machinations, and that this whole issue will be moot. An recent alternative public key cryptosystem, the elliptic curve algorithm, is under scrutiny, and there are yet other possibilities.

On an even crazier front, NIST and NSA proposed the "Clipper" chip to replace DES. If NSA had had its way, Clipper will have been in every phone, fax machine, and ice cream truck. During manufacture two keys were to be generated for each Clipper chip, and the two would be "escrowed" with two federal agencies. Given a court order they would deliver the keys for use in overhearing conversations. The U.S. government keeps putting new proposals forward, but it looks like Clipper is dead. There are a book's worth of reasons for abandoning this project, but suffice to say that it would violate the principle of absolute privacy of personal conversations. A joke attributed to Whitfield Diffie says that far from needing "back-door" or "trapdoor" access to Clipper encrypted data, the Clipper provides a *front* door for access, meaning that Clipper would allow law enforcement to waltz

right in and grab any data they like (with a court order).

In 1995, the U.S. Congress enacted the Communications Assistance for Law Enforcement Act (CALEA or Wiretap Act), with the objective "to make clear a telecommunications carrier's duty to cooperate with law enforcement with regard to electronic surveillance related interceptions for law enforcement purposes." Chapter 5 discussed this issue more thoroughly, but in summary, this requirement that the FBI can wiretap any desired phone conversation is misguided, expensive (far more expensive than the US $28 million per year estimated by the FBI), and will not be effective, since criminals will be able to use readily available private codes to defeat it.

Led by the guardians of the RSA Cryptosystem (RSA Data Security, Inc.), there has been a worldwide effort to provide to all users security tools based on RSA. One current system, Pretty Good Privacy (PGP), has a modest name but performs well indeed, using the slow RSA for exchange of keys and then DES or a better alternative for the actual transmissions. The inventor, Phil Zimmermann, was threatened with legal problems in the U.S. for releasing and distributing this software over the Internet. (He denies doing it.) An unrepentant Zimmermann continues his work by releasing a PGP version for telephone conversations—a direct challenge to U.S. government policy, and he has recently formed a company utilizing his software. I expect this and similar systems to dominate world-wide digital electronic transmissions. When used by individuals, these systems are free, readily available, and easy to use. Newer software automates their use so that the unsophisticated need only know that their communications are secure, without knowing how it is done. Unfortunately, if the U.S. were to mandate Clipper chips in all government phones or mandate a similar system, it might become a standard that most people used. More worrisome are U.S. government proposals to require by law the escrowing of any keys used by strong cryptography, providing cryptographic keys to the government and to law enforcement under a court order. Then American users would be secure against everyone but the U.S. government. These escrow systems themselves will be complex and full of security holes. An advisory committee formed by the U.S. Department of Commerce worked for

two years on an architecture for implementing such escrow schemes, but their mandate was not extended when they were unable to finish by the deadline. A group of academics has provided two versions of a report arguing that the governments goals are completely unworkable.

Is Privacy Important?.

Privacy in the U.S. is a confusing and misunderstood issue, since the word "privacy" does not appear in the U.S. Constitution. However, the U.S. courts have given citizens privacy rights under the Fourth Amendment guarantee of rights of "people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." In practice this has meant that without a warrant or probable cause, U.S. citizens have considerable privacy in their private space and little privacy in public space. (The inside of a person's body and the interior of their car are in their private space.) The situation actually fits well with this book's suggestion for widespread public surveillance, and for privacy laws and policies that allow individuals to protect their private space, including private communications and private data.

Why is privacy important? Alderman and Kennedy, in their book *The Right to Privacy* gave the following answer:

> [Privacy] protects the solitude necessary for creative thought. It allows us the independence that is part of raising a family. It protects our right to be secure in our homes and possessions, assured that the government cannot come barging in. Privacy also encompasses our right to self-determination and to define who we are. Although we live in a world of noisy self-confession, privacy allows us to keep certain facts to ourselves if we so choose. The right to privacy, it seems, is what makes us civilized.

These authors then quote from Justice Louis Brandeis that the right to privacy is "the right to be left alone."

In the terms of the present book, removing all privacy would be a greater crime, a crime against citizens committed by government or society. Nevertheless, it is not obvious that privacy is the only

way for mankind to go forward. I can imagine successful human societies with no privacy: no secrets, not even secret thoughts, and glass houses. Many problems and fears might disappear, replaced by the comfort and certainty of communal activities. Some societies, such as Navaho Indian tribes, or natives of Western Samoa, lived that way. Privacy, and its companion, individuality, may be overrated now in the West. It is a relatively new concept; the Middle Ages had little privacy.

In the U.S., there are also Fifth Amendment problems with the absence of privacy, since a violation of privacy could incriminate someone. There are problems of blackmail, plagiarism, stealing secrets, and espionage with privacy violations. People can be subjected to emotional distress or humiliation or ridicule if privacy is violated—think of Prince Charles and his intercepted cellular phone conversations. He had a right to expect privacy; strong cryptography should have protected him, but instead his lovers' conversation was paraded before the world.

In the end, individuals must decide for themselves how important privacy is to them. The trend has been to accept some loss of privacy in public, a privacy that was only present because no one bothered to violate it, in exchange for additional safety and security. An expectation of privacy of electronic conversations promotes the free exchange of ideas and thus promotes free speech and open access to information. This is one reason for this book's emphasis on the right to privacy in private space.

Privacy of Data.

Recently in the U.S., when the issue of privacy abuse comes up, the subject is often privacy of data. The concern is about invasion of the privacy of one's personal data, particularly that carried out by government and private industry. In the United States agencies and companies collect vast amounts of data about individuals. The collectors proceed to copy and exchange and sell the data, to correlate and cross-correlate. Companies want a profile of the individual's activities and interests to target advertising better. There is data about lifestyle, about crimes, about finances, about preferences, and about family

history; companies track purchases at stores, magazine subscriptions, catalog purchases, vacation destinations, movie rentals, and so forth. Much of the data is inaccurate—a notorious problem with credit data. The usual discussion proceeds to ways of limiting the data collected, limiting its spread, and correcting inaccurate data. Privacy advocates propose laws to limit the collection and spread of data. They would use the new laws to correct inaccuracies and also would provide open access by individuals to their own data, to amend or delete it.

A large number of recent books deal with issues of privacy of data. From the point of view of the present book, all the gathering and sharing of data about individuals by companies is undesirable but usually not relevant to crime prevention. Current personal data privacy laws are strong in Europe, while they are confused and uneven in the U.S. For example, American laws now forbid releasing the titles of videos rented, but allow dissemination of information from medical records.

It is easy to imagine problems arising from inaccurate data. A bank may deny a loan application because of past loan defaults by someone with a similar name. Similarities can lead to arrest and imprisonment. Part of the problem rests with inadequate personal identification. I would feel personally more secure if I knew my activities could be accurately ascribed to me, and that no one else could impersonate me. In addition to improved identification, agencies should expand open access to one's own personal data. Note that here again accurate identification is a crucial issue: Everyone wants access to their own personal data and wants any impostors denied such access. One current method of obtaining data about an individual is to pretend to be that individual. Alternatively, people desiring data pretend to have a legitimate need for the data, whether related to health, finances, or other matters.

Suppose a person accesses data (books, tapes, or online data) about AIDS, perhaps because a friend is ill, and later finds that he can no longer get insurance or a job, because a computer data bank has kept track of this "suspicious" reading material and now is using the data for a different purpose. Society needs laws against the correlation of such data by private industry, but governments still ought to

gather the data by logging, for use by law enforcement with a court order.

It is also possible to abuse *legitimate* access to data. For example, there are often news reports about misuse of personal data, as illustrated by the second quote at the beginning of this chapter. The rest of that story mentioned the sale of criminal records to private detectives, lawyers, and politicians in defiance of the right-of-privacy laws. Examples included an angry ex-policeman tracking down and murdering his former girlfriend, and a drug-dealer getting help from police computers to verify the background of clients, to check for undercover agents. The story recommended strong criminal sanctions as a deterrent. One could also use fingerprints as detailed in Chapter 4. Access to personal data in the U.S. by the "proper" authorities is far too easy, usually with no auditing or controls. This must change, with logging of the accesses to personal data and with auditing of these logs.

The World Wide Web has added a new dimension to problems with personal data, since sites can collect information about visitors—information that can be saved, combined, reused, and sold. There is a recent push for web sites to list their privacy policy, that is, to tell users how much personal information the site saves. Even more worrisome is the current practice of web browsers to save information about browser use in the user's computer—the so-called "cookies." Other web sites can access this cookie information to learn about a user's activity on the web.

Recommendations.

Recall the concepts of public space and private space from the previous chapter. Society should deny access to information about activities in private space, and there ought to be absolute privacy of the content of individual conversations, of individual data, and of individual physical private space, both at home, at work, and elsewhere. Here "absolute privacy" means that society protects the privacy as well as possible with technology, and enacts and enforces laws against invasions of privacy that occur in spite of technology. This stand is not far from the current situation in the U.S.

Cryptography will protect personal communications from most interceptions except for physical ones, such as a bug planted in a room, though it is also possible to exploit weakness in the computer system in an attack—a large headache in current complex systems. The absolute right of privacy should include ordinary telephones, electronic mail, faxes, cellular phones, pagers, and similar devices, as well as diaries and other personal data, but society will log the fact that communication took place and the time of it. This communication privacy should extend to all but a class of convicted criminals, who could be denied the right of secure communication as part of probation conditions. Keep in mind that such denial could keep them from using standard cryptography-based security systems, but they might well devise their own method of communicating in secret. Everyone, even a murderer on death row, even after execution, should have absolute privacy of their personal data, such as a diary. Privacy of a diary is similar to privacy of one's own thoughts, and I consider it immoral to invade either of these.

Law enforcement should discontinue all wiretaps of phones and similar devices. Wiretaps are no longer cost effective, and U.S. government proposals to maintain wiretap capabilities get increasingly unreasonable as technology improves. More important are the free-speech issues: the right to secure private communication is desirable, because it promotes free speech. In extreme need and under court order, society should be prepared to protect itself by placing an actual "bug" in physical private space. The norm, however, is to judge people by what they say and do in public, and society must use the tightest controls on and audits of any surveillance of private space.

Society must think over the issues related to privacy in the workplace. The only requirement is that a company clearly identify the private space an employee has in the work environment. If there is any such private space, its security must be absolutely enforced. It is in every company's interest to provide private space for employees, but the company must determine this policy. For example, some companies monitor all electronic mail of their employees. Such all-inclusive monitoring is acceptable, though not desirable, as long as employees understand this policy. Completely unacceptable is to promote the

privacy of personal electronic mail and then to subvert it. Similarly as mentioned before, employees should have private personal data space and private personal physical space. Again the one unacceptable action is to claim there is such privacy and then to violate it.

The public space of my new world would have relatively little privacy, as is the case now. In the United States, in the absence of a court order, there is nothing to keep your nosy neighbor, a private investigator, or a stalker from following you with a video camera. The difference between this proposal and the current situation is that the individual (and law enforcement) could obtain information about the person doing the following, since the follower is also in public space and has no absolute right of privacy.

7. Anonymity
no longer Desirable

… I do not believe we have the appropriate technology to make an anonymous service work on the net. Furthermore, I remain completely unconvinced that there is a legitimate need, nor is the level of maturity in the user population sufficiently level where it can be effectively used. It may only be a small percentage of people who cause the problems, but that is true of nearly everything in history.

I am a firm believer in privacy, but that is not the same thing as anonymity. Anonymity can be used to violate another's privacy. For instance, in recent years, I have had harassing anonymous notes and phone calls threatening XXX because of things I have said on the net. … I have seen neighbors and friends come under great suspicion and hardship because of anonymous notes claiming they used drugs or abused children. I have seen too many historical accounts of witch-hunts, secret tribunals, and pogroms—all based on anonymous accusations. I am in favor of defeating the reasons people need anonymity, not giving the wrong-doers another mechanism to use to harass others.

… any such service is a case of willingness to sacrifice some amount of privacy of the recipients to support the privacy of the posters. You will not find the recipients of anonymous mail being the supporters of such a proposal.

—SOMEBODY (anonymous user), "Anonymity on the Internet," L. Detweiler, 1992.

Society has long seen anonymity in such forms as suggestion boxes and anonymous letters. During the American revolution, Madison, Hamilton, and Jay originally published *The Federalist Papers* in New York newspapers using the name "Publius" as the anonymous author. Anonymity has assumed more importance with recent attention

to whistle-blowers, who may suffer in many ways, often destroying their career if they do not report anonymously or if they lose their anonymity. One young anti-nuclear power activist even died under mysterious circumstances (Karen Silkwood, in 1974). Other recent important examples are anonymous leaks from government agencies in the U.S. Such leaks have become a common method for these agencies to further their agendas, as well as serving as an outlet for frustrated employees. If media agents can verify the leaked information, then this at least serves the goal of more open access to information. I myself once called a newspaper to give an anonymous report of what I regarded as wrongdoing. I found that a reporter was already working on the story and that I was at least the sixth caller. I had no information to provide that the reporter did not already know.

Traditional anonymity is prone to technical flaws that might reveal the anonymous source. One has the cartoon image of an undersized boss sitting inside his own suggestion box, watching employees drop off suggestions. Paper forms for employees to fill out anonymously are subject to a variety of fingerprinting techniques, as discussed in Chapter 4. In fact, fingerprinting, surveillance, and other technologies in this book attempt to detect and uncover anonymity, though in most cases the data supplied by the technology would only be accessed in case of an actual crime. At the same time computer technologies also provide better implementations of anonymity, with emerging methods that even suspicious employees could trust.

Privacy and anonymity are similar, intertwined issues, with anonymity often helping individuals maintain their privacy. Thus a person making a truly anonymous health query is better assured of privacy than if he had to rely for his privacy on the discretion of those answering the query.

Anonymity as a service is another way to support free speech, since without the service speech may be inhibited. As the quote at the start of this chapter makes clear, there are also disadvantages to anonymity, giving a tension between advantages and disadvantages. Unlike the anonymous author of the quote, I contend that appropriate technology and structuring of anonymous services will alleviate the disadvantages and make the anonymous services work well.

However, anonymity makes it easy to violate other people's privacy, to reveal information about them without fear of reprisals or consequences, and such information, once released into the world, cannot be taken back. This applies to the new electronic world as to the old one. The anonymous identity of the Houston "bubble baby" (a child with no immune system to protect against disease) remained confidential, though many people knew it. Release of the identity would have been an irreversible transformation.

Individuals are losing anonymity in a global sense as they are transformed into numbers to allow manipulation, to entice them to purchase consumer goods, to convince them to agree with a stand they would oppose on their own, or to exploit them, as journalists sometimes do after a tragedy. Individuals are subjected to private and public surveillance and to identity searches; companies gather customers' buying and renting preferences to store and resell. At the same time, anonymity is increasing locally, as homeowners no longer know their next door neighbors and fear every stranger who walks past their house—a trend destroying the sense of family and community.

Both the global loss and the local increase of anonymity are detrimental to humanity, and society must reverse these trends. Technology, especially computer technology, is both a contributor to the problems and a provider of partial solutions. Society should limit the accumulation of data about individuals' private lives, especially by businesses. Admittedly, certain of the surveillance methods explored in this book would lead individuals to lose the anonymity they have enjoyed as they went about their public activities. However, this anonymity in public was present only because no government or corporation bothered to violate it. Properly used, computers will foster a sense of community for those who have lost it. Isolated individuals will contact others with similar interests anywhere in the world.

The computer revolution brings new possibilities for anonymous services—to improve lives and to create new problems. Good anonymous services will allow an individual to reclaim the sense of anonymity lost to computer monitoring.

Traditional Anonymity.

Standard types of anonymity include suggestion boxes, unsigned letters, whistle-blowers, newspaper reports from unnamed sources, anonymous refereeing of scholarly articles, anonymous dating services, leaks from government agencies, and reporting of statistics about individuals without identifying them. From the nuclear power industry to tobacco companies to the medical establishment, insiders have played decisive roles in reform by contacting authorities or the media—sometimes anonymously. These traditional forms of anonymity are welcome and beneficial, or irritating and destructive, depending on the perspective. Most traditional anonymous services suffer from a lack of control over the service and from imperfections which can compromise the anonymity.

New "Caller ID" services from U.S. phone companies provide the phone number of the caller (and other information) to the person called. There are bewildering possibilities for preventing the phone number from being sent, or for blocking out calls that do not provide the calling number. Understanding the implications of this new technology will take time, since most phone users are accustomed to anonymous phone calls. In the old days, if the party called did not recognize the voice, one could insult them in any way, with the expectation that tracing the call would require prior arrangements and extra time during the call. Now the norm for calls is changing to attribution all the time, so that one could only get anonymity by calling from a pay phone. Anonymity would be better as an unusual special case that is tightly controlled. Thus phones should allow anonymous calls, but should also allow recipients to block anonymous calls and should require that users of pay phones identify themselves. The phone company has a profit motive here: they want to provide a service and extra income to businesses, who could save phone numbers of people who called the business and profit from these numbers. These businesses may make extra money, and may even provide welcome services to users, perhaps through solicitations targeted at the users' interests, but the benefits to society of extensive logged data, as envisioned in this book, are mostly missing. One needs, for example, coordination

of logged data about purchases of dangerous objects.

Agencies that report statistics try to keep from reporting information about individuals. For example, the U.S. Census Bureau does an excellent job of releasing only summary statistics, so that individuals remain anonymous. For an extreme instance of statistical data leaking individual data, I once taught at a school that revealed my salary even though their policy was not to do so. The school generated a report giving average salaries by category, with no identities listed. My category was "Associate Professors of Computer Science," and the report said there was only one individual in the category; the "average" salary listed was my actual salary. Whenever a large amount of statistical data is reported, and especially if a system supports statistical queries, clever methods may break the system's anonymity and allow deduction of data about individuals.

Most people see partial benefit from each anonymous service listed at the head of this section. There are other less common services that illustrate benefits. Anonymous AIDS queries provide one example. Anyone worried about AIDS is usually also concerned that a query or test they initiate remain confidential. This is especially troubling in smaller cities. Even the knowledge that an employee has been tested can lead to problems, including loss of a job and of friends. This particular issue is crucial because those infected with AIDS might put off a test for fear of repercussions. Recent trial programs have handled AIDS questions and AIDS testing by mail, using unobtrusive packaging and mailing addresses. It is expected that a number of people will use this service who might be afraid of a normal clinic setting.

There are still pitfalls in the processing of anonymous services. In one current AIDS information system, users in the U.S. dial an 800 number to access the system. Many of these users do not realize that even with the blocking of Caller ID services, the user's number is transmitted in case of an 800 call. More serious pitfalls are illustrated by a recent murder in San Antonio, Texas. The victim had been hiding from her boyfriend, but he located her through Caller ID at a mutual friend's house.

Young people seeking answers about sex provide another exam-

ple of the benefits of anonymity. This particularly applies to gays of high-school age, who often have nowhere to obtain information—not from peers in school, or from teachers, counselors, or anyone else. Anonymous and confidential contacts, especially over the Internet, can be a big help.

Anonymity on the Net.

Chapters 10 and 11 will discuss Internet services that are important because they promote free speech and the wide and open dissemination of information. Anonymity and anonymous services are part of the larger picture and will assume greater importance in the future. In fact, many Internet users do not realize the extent of their loss of anonymity—when they browse the web they unknowingly leave their Internet address. And the browsed site can leave information on the user's machine in the form of a "cookie": an entry recording the use, one that other sites can access as well.

At present, the Internet is conducting a vast experiment with anonymous services, in which dozens of individual sites volunteer to function as free *anonymizing remailers*, that is, as sites that take an input message, strip off identifying header information, and forward the message (mail or news) with an anonymous identifier. They may also add a "handle," known formally as an *anonymous net identity,* to the message. In this way readers or recipients of messages will know when several such messages come from the same source. Individuals can also send a message to this anonymous source, without knowing the recipient's identity in the "real" world. For additional protection of anonymity, users will go through more than one stage of remailer, or go through several telephone or telnet connections. Several proposals add new ways to provide Internet anonymity.

One widely-used remailing site was the Finnish "anon.penet.fi," which until recently processed 6000 messages per day. This site and others periodically shut down when someone uses them to send a particularly loathsome message, such as a death threat to the U.S. President, racial or ethnic slurs, or a posting to a dog-lovers group about how to cook dogs. Complaints to a remailer will seldom elicit anyone's identity, but may result in loss of remailing privileges. This

Finnish site was less vulnerable to pressure from U.S. agencies than were sites in the U.S.

An infamous anonymous posting to the "sci.astro" newsgroup gave a purported transcript of last desperate crew dialog during the U.S. Space Shuttle Challenger disaster. This posting went through the Finnish site, and there were outraged cries for the system administrator to reveal the poster's identity. This was never done, and his identity remains a secret. Recently, however, the Finnish site was involved in a court battle asking them to reveal another anonymous identity and has temporarily closed. Dozens of other anonymizing sites are available, and one can even use a free e-mail service, giving a false name, for modest security.

More recently, companies have emerged that supply anonymous services for a fee. One of the largest of these provides free anonymous e-mail, anonymous browsing for a fee, and soon will allow telephone connections to their service that are protected by 128-bit cryptographic keys for considerable security. However, this particular company provides its service from the U.S. and so could be ordered by a U.S. court to reveal anonymous identities. With this service, a person browsing the web would only reveal the anonymous service's address to the visited web site and would not provide any cookies to reveal personal preferences.

Another company now allows participants in anonymous chat rooms to switch from typed discourse to an automatically connected voice connection, one that remains anonymous. Thus two or more parties can continue their discussion more conveniently on the phone and yet remain anonymous.

Uses of anonymity have evolved that are similar to the occasional anonymous letters published by advice columnists. The usual motive is that revealing their identity would embarrass themselves or others. Such unsigned letters are the newspaper equivalent of a moderated Net newsgroup willing to post unsigned contributions. More serious uses include electronic discussion groups and support groups where the subject area is sensitive, such as sexual abuse. Groups like these may function better than traditional ones because there are no face-to-face encounters and no identities to get in the way. Without

anonymity it is hard for an important person, say, an army general, to get psychotherapy, let alone group therapy.

The Internet is just now entering the era of split identities. Human society has always had individuals with secret identities or secret lives. Now just at the time when proposals for tracking in public would make a traditional form of secret life harder to conceal, Internet anonymity services will make secret electronic identities feasible. Imagine the benefit when well-known individuals can contribute to a discussion group anonymously—without appearing to make official comments on matters of public policy.

Future Anonymous Services on the Net.

This section presents a collection of related proposals for new and enhanced services which, taken together, would make anonymity work better on the Net. However, further experimentation would be needed to design and implement such a system. Similar proposals apply to the U.S. Caller ID systems.

First, one should require that any anonymous message be identifiable as such from header information. This is currently the case with many remailers, but is not "required." With such a guaranteed addition, automated software systems (such as the autonomous agents that Chapter 11 describes) would recognize anonymous messages and could deal with them as the user, or newsgroup, or other human agent might dictate. A user or newsgroup could decide not to receive anonymous messages.

Second, provide two kinds of official anonymous remailers: one with logging of user identity information and one without logging. In extreme cases, the identity of a sender of a message to the logging remailer would be revealed—perhaps for certain crimes. The sender's identity for the unlogged remailer would not even be available for retrieval. Both versions would identify the message as anonymous and would identify in the header which type of remailer was used. In this way a user or newsgroup might elect to receive messages for which the identity of the originator was logged and not to receive the other type of message. In case of abuse, the logged remailer would terminate the service. If termination were globally coordinated, it would

be a serious sanction, though coordination across cultural boundaries might be difficult. Rules determining abuses must be unambiguously formulated and widely disseminated; rules for revealing logged information would also be needed. Termination would not be possible with the unlogged remailer.

These anonymous remailers would work well in conjunction with the authentication services described in Chapter 6. Cryptographic techniques combined with identity verification allow authentication of a message. Because senders of messages attach digital signatures to verify their identities, the recipient can be certain of the sender and can be certain that the message arrives unaltered. Such a system allows only two kinds of messages: authenticated and anonymous. A recipient of a message or reader of news would know either that the message was formally anonymous or that the identity of the sender had been verified. Users should keep in mind that authentication also protects against fake messages mailed in their own names.

Any non-authenticated message should be regarded as anonymous, even if it says "Your loving Grandmother Thora" at the bottom. Traditionally, confidence in the origin of a letter has been based on clues like handwriting and personal references, as well as postmarks and return addresses. All such clues can be forged with effort. In the new electronic world there are (usually) no handwriting clues, but the other clues, though present, can be faked as easily as before. The new electronic signature bears a resemblance to the old-fashioned signature scrawled across the sealed flap of an envelope, but the electronic version is much more secure. Signatures would prevent poison pen letters—not anonymous, but falsely attributed—that can have a devastating effect. In the U.S., if the President receives a non-anonymous threatening letter, the purported sender will at the least spend a bothersome time explaining that he did not originate the letter.

Authentication is important for new filters attached to mail and news software. In this context a *filter* is software that eliminates selected portions of the data. A given newsgroup or individual could elect to receive only authenticated messages. One could remain unaware even of attempts to send anonymous messages. Any message received would have a clearly indicated sender identity. On the other

hand, a given newsgroup or user could elect to receive logged anonymous messages or even unlogged ones. If a newsgroup posted such messages, each user could elect to filter them out while reading news. (In the current system, some newsgroups are also *moderated*, meaning that an individual moderator receives all prospective postings and decides whether, and in what edited form, they will be posted to the actual newsgroup. Currently, such newsgroups are bothered with bogus, anonymous postings.) The same filters on mail and news can sift through, looking for messages that seem objectionable, uninteresting, or otherwise undesirable. As time passes filters will arise with higher "intelligence"—better able to decide what a user wants to see and what the user is not interested in.

There are clever tricks from cryptography that implement more complicated anonymous activities. For example, there are methods whereby anonymous senders can identify themselves unfailingly as members of a certain group—any group at all, like say, female company employees. A company official receiving an anonymous message about female employee grievances would know with certainty that the message originated with a member of the affected group. It would also be easy to authenticate that a message was signed by a certain specific number of members of the group, while revealing nothing about the identities of the particular senders. Anonymous messages from a group can be implemented using *secret-sharing* schemes. As the name implies, these methods allow several individuals to share a secret. Using schemes like these, one could be sure that access to any object, such as a safe or a computer or a contract, depends on cooperation and agreement of a fixed number of individuals from a larger group.

There are other trickier uses of cryptography, too complicated to explain fully here. For example, David Chaum has proposed methods for using anonymous identifiers to support anonymous credit reporting, similar to the current credit bureaus but without the names attached.

Summary.

Anonymous services are important—worth undergoing the effort to

provide, worth enduring the problems with abuses. In the end, the improved freedom of speech is reason enough to retain anonymity, and specific applications mentioned in this chapter give further reasons. Online service providers can prevent most abuses by using firm control over the anonymous service itself. Authentication of messages will allow such service providers and their users to regard each unauthenticated message as anonymous. In this way a user can ignore attempts at anonymous communications and need not even be aware of them.

8. Education
not just in Schools

> *For four or five years we could provide a life in which no important need would go unsatisfied, a life practically free of anxiety or frustration or annoyance. What would* you *do? Would you let the child enjoy this paradise with no thought for the future—like an idolatrous and pampering mother? Or would you relax control of the environment and let the child meet accidental frustrations?* But what is the virtue of accident? *No, there was only one course open to us. We had to* design *a series of adversities, so that the child would develop the greatest possible self-control. Call it deliberate, if you like, and accuse us of sadism; there was no other course.*
>
> —B.F. Skinner, *Walden Two,* Macmillan, 1948, Chapter 14.

This book's title calls for the use of computer technology to make crime impossible. The emphasis so far has been on coercive and deterrence techniques—either to prevent the physical act of crime, or to provide means to catch the criminal. Neither technique removes the desire for crime. Some of these proposals also remove the motive for crime, if not the desire, by removing the target of a former crime or by making a former crime meaningless. Thus crime-proof hardware will not work when stolen, so a thief gets no benefits from stealing such items unless his motivation is vandalism. Similarly, a thief cannot steal cash from a "cashless" society, though of course he can redirect his efforts toward electronic wealth.

Modern society must improve its strategies for raising citizens who do not want to commit crimes—using education, conditioning, instillation of morals, and the like. Society has always had this mission and has often more or less fulfilled these goals, but either could

not sustain the production quality or the idealism (as with the introduction of monasticism under St. Benedict's rule or the Shakers in 19th century America) or failed to address other important societal concerns (such as humane tolerance of differences in current U.S. society). A society with such educated citizens would be the ideal—leaving the technological gadgetry in place to catch or deter the few pathological remnants: those disaffected or alienated or unhappy people still intent on actively committing crimes.

Of all the methods discussed in this book for preventing crime, in the long run education should prove the most important, the most effective. And it should change the most with the maturing information age. After all, the open access to information emphasized in this book as mankind's salvation is one facet of education. This revolution in education is just starting, with only hints so far of the future to come, but already many learning tasks can be automated with adaptive, tutoring computer programs that provide immediate feedback. These same "intelligent" tutors will measure progress and effort, providing a good learning environment even with today's technology. Hardware advances support affordable simulation and virtual reality systems, while data transmission improvements make world-wide educational resources available and provide interactive video and other multi-media for educational exchanges.

Moving beyond the computers, the family unit has traditionally been responsible for the instillation of morals. Unfortunately, the family and its influence on children have often been failing of late in the U.S. Society should pursue policies to strengthen the family, but if that falls short, for children with no family or with inadequate family support, caring adults must recreate a sense of family. Troubled children need intervention: early, frequent, and intensive. Community organizations, including schools, religious groups, and various agencies must all help.

These ideas are independent of computer technology, and chasing this technology might lead educators to miss all that is important, as with a school district so busy buying computers that no one has time for the children. School districts often buy hardware, but leave no money for maintenance or training, no money for release time to

allow teachers to learn to use the equipment. Worse yet, some districts redirect money spent for worthwhile causes to the purchase of unneeded computer equipment. Computers can only help if they are properly and judiciously used and if their use is supported financially and by policy. Schools must understand the conditions when the computers are *not* essential, as with all-important areas like critical reading, reasoning, and writing. Thus society cannot wave a magic computer wand and conjure up better education. In a recent Internet document, Lowell Monke wrote:

> … the computer promises to provide my students with an endless supply of information, but what good will that do if they can't make sense of any of it? It promises to help my students express their ideas better, but what good will that do if they don't have any ideas to express? It promises to help them develop marketable skills for a technological society, but how valuable is that if they have never developed the good judgment needed to live a fulfilling life?
>
> The key question for me was, How is computer technology going to help my students develop those inner qualities, such as insight, creativity and good judgment, which education at its best has always sought to inspire? To put it another way, Is there a way to harness the power of computer technology to serve my students' search for meaning in their learning and in their lives?

When Thomas Edison produced the first practical motion picture machine, he and others expected this new medium to revolutionize education. Similar predictions were often made for television, yet the results in both cases have been disappointing. Movies and television in a classroom may keep children quiet and entertained, but these tools must be used in a careful, limited way to be useful for education. In contrast, society's latest fads, the computers and the Internet, can be interactive and adaptable—key features to support education.

Making effective use of computers for education will be difficult, but individuals will soon have convenient and inexpensive access to vast resources of information, of computing power, of software that includes responsive and conformable agents. The problem is to transform these resources into education, to improve those education

strategies that already work without computers, to invent strategies only possible with the new technology.

Information as Wealth—Knowledge as Power.

Information is the new form of wealth in the computer era. In contrast with traditional material wealth (gold, jewels, houses), computers can easily copy this new form, and networks can distribute it, both at steadily decreasing cost compared with the cost of physical objects. This is shared wealth that keeps growing, with enough for everyone.

In this terminology, data, or "raw" data, denotes letters, digits, and other characters strung out in a row, without any concern about what they might mean. Data becomes information when it acquires a meaning or use. Thus one can extract information from data. No one is interested in data without meaning or use. Often data is arranged ("packaged") in forms that make the information content readily discernible.

Not everyone has access to information. Many of the information-age "destitute" live without this wealth. Even in the U.S., information "rich" as it is, access to information divides people into classes. For example, a typical inner-city U.S. high school may have an adequate number of computers at the school, but most students will have no access to a computer at home. Just as a community's free library in the U.S. has given many citizens means to better themselves, the same community now needs affordable access to information—to prepare for the information economy, to share the new wealth.

I use the term "knowledge" for information that has been transferred to a human being. Knowledge can confer power because a person can make use of the underlying information. In such terms, knowledge would not reside in books or electronic media, but only in people. However, the computer revolution is forcing a rethinking of the meaning of knowledge; mankind now produces software that behaves as if it understands the data available to it—software that can act on the basis of that data in the same way that a person would.

I regard education as the change that occurs through acquiring knowledge. Then the educated person's advantage is not primarily the specific knowledge already acquired, but the skills developed while

getting knowledge. These skills are subtle, traditionally involving the ability to reason, to analyze situations logically, to understand written material, to write clearly, in the end to tell sense from nonsense. The skills also involve facility in the use of research materials like those in libraries. Such useful library skills are shifting now to familiarization with the new electronic sources of information, so that the electronic catalog may bewilder an old-style scholar in his initial search for references. Thus an essential part of education in the information age is intimacy with the electronic media, with the new sources of information and the new technologies. Available computer technologies are changing so rapidly now that the future is hard to predict, but computer-related tools for scholars and professionals should mature eventually into forms enormously more powerful than today's versions, and yet much easier and more intuitive to use. Music and architecture provide two examples of professions in which a practitioner usually now needs familiarity with computer use to be regarded as a professional. The future may see a shift back to the basics in the education of students in these two fields and in similar ones. The use of computers will be ubiquitous and essential, but also so user-friendly that musicians or architects can concentrate on more important matters: creating beautiful music, or designing environments that meet a community's needs and desires.

The Latin root for "education" means "to lead out," in contrast to the word "indoctrination," which implies "a forced pushing in." Education ought to be a wise application of both extremes: rote learning and the more creative fostering of talent. There is also "training," a form of education with short-term goals, and "conditioning," a gentler word for indoctrination. Computers will support all these activities: education, training, conditioning, and their variants, but a broad education is indispensable for higher human aspirations.

I fear that American society may be splitting into two classes now, based on education. Thus America may replace a class structure partly based on culture or race with a new education-based structure. The logic of events, and not individuals, will direct future forms of discrimination against the under-educated. People who do not understand the basics of the modern technical society will not be able to

participate fully.

Intelligent Tutors.

Starting in 1954, B.F. Skinner worked on "teaching machines," partly to correct defects he saw in traditional education. Skinner observed his own daughter's mathematics class and saw that "the teacher was violating two fundamental principles: The students were not being told at once whether their work was right or wrong ..., and they were all moving at the same pace regardless of preparation or ability." Skinner worked for a frustrating decade on various teaching machines without success. One can see that his machines were doomed for lack of the necessary technology, but far-reaching advances have now provided the powerful inexpensive computer hardware and complex software needed for successful teaching machines. The machines of the future, yet to be fully developed, will not just give immediate reinforcement and move at the student's desired pace, but will adapt to each student in ways that resemble human intelligence. The key change is that in today's machines the most complicated part, the source of "intelligence" if you like, resides in the software. This software runs on standard inexpensive hardware; it can be copied for next to nothing; and its development cost, often many man-years of work, can be amortized over the use of millions of copies.

An example of how *not* to use this new technology comes from one segment of calculus teachers, who promote the graphing calculator as the single, final, and perfect tool needed to teach calculus. Inexpensive and easy to carry, the calculators may help instruction, but they fail to provide the thousand-and-one capabilities that future calculus teaching tools will have: reacting adaptively to the student's performance, monitoring and reporting this performance over time, and providing interesting multi-media displays to illustrate concepts. There will be pre-defined segments leading students through specific material, immediate links (including hypertext links) to related material, and other capabilities no one can imagine yet. A different segment of calculus educators is currently working on better tools that use symbolic manipulation packages (such as Mathematica or Maple) and interactive Web sites as a basis for teaching calculus, tools that

include interactive graphics "produced *by* the student, rather than delivered *to* the student."

There are on-going experiments with small laboratories, especially in introductory college courses, that claim to do a better job with less money than traditional methods. Calculus is a good example because all approaches require disciplined students, willing to work hard, and there are limits to how much fun or entertainment calculus instruction can involve. A recent software package is typical of the computer assistance available for specific courses, in this case a course in ordinary differential equations.

Other educators are using artificial intelligence techniques to build more capable intelligent tutors. For the near term, these tutors will just do a better job of adapting to the user and of presenting material, but eventually such software could call on enormous resources in real-time: libraries, museums, archives of data, calculation packages in many fields, and simulation software.

Simulation.

Simulation and modeling are now fundamental tools for understanding the world. Computer simulations appeared during World War II, when they helped the United States develop the atomic bomb and later the hydrogen bomb. As early as four decades ago businesses would test the effects of decisions on their profits using ever more complex simulations. For example, a railway company might investigate the result of installing a shortcut rail segment: how long would it take to recover the building cost? At the same time, one started seeing simulators for airline pilots. This flight simulation technology progressed rapidly, reaching a peak with the NASA space simulations.

When astronauts landed on the moon, they saw familiar landscape outside the windows (except on the first mission, which strayed from its intended landing site), for they had trained endless months using simulators that provided realistic pictures of what they would eventually see. These early simulators used a detailed model of the particular portion of the moon chosen for landing, coupled with clever computer-controlled cameras that would swing down to the model's surface as the simulation pretended to land. Such expensive models

have now been replaced with software to provide simulated real-time video images. Again one sees expensive hardware (models and cameras) replaced with software—a replacement made possible through relentless computer advances.

People not familiar with simulation see the NASA Space Shuttle simulators or airline simulators as useful training devices which could be dispensed with if necessary, using the real shuttle or airline. In fact, the shuttle was designed using a variety of simulators. Ultra high-fidelity aeronautic simulators helped design the external shape of the shuttle—a complex task because of the many different regimes of speed and air resistance the shuttle had to fly through. Procedures simulators allowed NASA designers to test the proposed interior of the shuttle with real astronauts, using simulated activities, especially simulated failures. Suppose a major simulator "accident" occurs because an astronaut fails to notice a crucial meter reading. Designers may decide that the meter needs relocation or enlargement. Such changes are relatively inexpensive in the early planning stages: modify the simulator and make changes in plans for the real shuttle. The cost of relocating a meter on a completed shuttle is hard to imagine. Thus, using simulators, the astronauts helped design the shuttle and learned a great deal about it before construction of an actual shuttle started.

Another benefit from simulators like these is the capability to train for disastrous failures. Who would want to turn off two engines of a real Boeing 747 airplane to allow pilots to practice landing under such emergency conditions? These and greater failures are easy to try out in a simulator. Along similar lines, a recent Boeing investigation of a 1994 airplane crash used simulators to reproduce effects found on flight recorders, while in another case, the simulator itself contributed to a 1987 DC-9 crash.

Simulation techniques like these are only now starting to filter down to more mundane levels. As costs keep falling, one can simulate more and more activities with ever greater fidelity. For example, electrical engineers have always needed to study electronic circuits. In the old days they worked in a laboratory with circuit boards into which they would plug hardware components and wire them together. Now

these laboratories are simulated with inexpensive computer hardware and software. The main defect of the software version is its perfection: the old devices were subject to random component failures, but such random problems are also easy to simulate.

How far can one go with these simulators? Consider electronic pianos. In my terms these are simulators of real pianos, since there are no wires or hammers. Piano simulators have gotten very good indeed, at least the best of them. If I listen carefully with my eyes closed, I cannot tell the difference between a new expensive grand piano and a top-quality electronic piano (not so cheap either). Piano experts scorn these electronic gadgets. They say there is no comparison between the real and the electronic. For example, they will hold down several keys, while playing others. On a real piano, the wires controlled by keys that are held down, released from their padded hammers, will vibrate in sympathy with the other struck wires. This feature is not built into current electronic pianos, so the sound is different—subtly different to ears like mine. But this just becomes one more feature to implement on piano simulators. Current electronic pianos fall short in other ways, too, including the "touch" of the keys. One day, though, the grand piano may disappear even from concert halls—real pianos found only in museums.

Virtual Reality.

The public has embraced the term "virtual reality" for high-end simulators, those that simulate more of the real-world experience. This flashy phrase is partly justified by the all-encompassing nature of current and proposed systems. High-quality, enclosing 3-dimensional images, especially images that follow head movements, can provide startling realism. Proposals for future virtual reality systems use full-body suits that monitor all movements. An individual sees a 3-dimensional image that moves as he moves his head; he hears with changing stereo sound; he even gets tactile feedback from movements, such as grasping an object, as well as realistic smells.

A standard joke asserts that one would not want brain surgery performed by a physician who had trained only on virtual reality systems. But the medical community is putting forward precisely this

activity, neurosurgery, as a good candidate for virtual reality training. Other medical applications abound, such as replacements for the messy and smelly (and expensive) anatomy course doctors have endured. Here doctors could avoid nastiness, but as with neurosurgery, medical schools will have to determine to what extent computerized courses can meet their needs.

Notice the change brought about by technological advances: In the past, high-quality simulators were available only to the ultrawealthy of government and business. But soon much better simulations, re-labeled virtual reality, will be affordable by small schools, even by individuals. These virtual reality systems will transform whole fields of education, such as the music and architecture mentioned earlier, and anything involving subtle human skills that are hard to describe in books. For example, future systems will record the actions of master craftsmen in such accurate detail that a lost craft could be recovered without rediscovering it.

Telephone conference calls are common in business. Real-time video calls and video conference calls are now emerging. Soon it will be feasible to participate in a virtual discussion group that can interact like a real discussion group except for touching or shaking hands, the actual physical contact. Critics of the Internet as a learning tool often complain that socialization—conversation over coffee or in a lecture hall—is essential. However, improved technology will give most of this—all but sharing the same cup of coffee or holding hands with a friend, and a virtual discussion group could include anyone in the world, any group of individuals in the world. Such virtual interactions are replacements for real contact, and as long as they do not completely supplant actual physical socialization, they should be beneficial, greatly extending an individual's possibilities for contact with others. Over the coming years society will experiment with many forms of computer-mediated contact, and part of the experimentation must include protection against reclusive activities by individuals, especially by alienated younger people.

Conditioning.

Conditioning is not a fashionable term. The public pictures the use

of behaviorist conditioning to turn children into little automata—perfectly behaved robots. There is the feeling that one could ruin the children's minds with conditioning, destroy their creativity. A cartoon version has electric shocking devices attached to children, giving them a jolt when they misbehave, so that the thought of bad behavior will reduce them to quivering jelly.

Many people think that conditioning and education were synonyms for B. F. Skinner, but he understood the longer-term, more generalized goals of education. The image in the previous paragraph presents several misconceptions. The emphasis will be on positive reinforcement, rewarding children for good behavior. But the larger misconception centers on the common belief that one should not condition children or adults, that they should remain free, whatever that means—with no interference. Instead I would maintain, along with others, that adults always interfere with children in their care, always condition them. The main differences in current society are that the conditioning is often poorly done, without a clear idea of techniques and goals. In my youth I was "interfered" with many times by mentoring adults interested in my welfare and development. What would be a crime is to fail in providing proper conditioning and interference. The problem is with the word "proper." Similar problems arise when one talks about instilling *values* in children. Whose values? Values come from so many places: from family, religion, ethnic group, social group, country, and society in general. American society is responding to these problems by providing *no* interference, instilling *no* values—an obvious mistake. Agreement is hard to reach, but who would not agree that a child who later ends up with a long prison sentence ought to have been dealt with differently. I think that society can agree on core values and on acceptable interference

The first quote at this chapter's start raises interesting issues—ones that would take another book to fully discuss. Skinner advocated deliberately arranging activities to elicit anger and frustration. He wanted this done in a planned and graduated way to help children develop self-control. Skinner's question "But what is the virtue of accident?" struck a chord in me over thirty years ago. Why should society let random chance dictate the upbringing of its children? There are

obvious dangers from too much interference, but the absence of interference is not working in current American society. Parents, teachers, and others often employ chance in raising children because they lack the energy or the plans to interfere effectively. This is where the computers can come to society's aid: they will not get tired and can keep track of each child's progress, each child's strengths and weaknesses. One often reads about abused children who "fell between the cracks" in child welfare agencies. Keep track of these children and leave no cracks to fall through. In the future, computer programs will monitor and plan, and design appropriate interference, following policies determined by human beings.

The Future of Education.

A revolution in education is coming, like no other before. A friend suggested a list of previous great educational advances: introduction of an alphabet and writing, the great classic libraries, the burst of new approaches to education among the early Greek philosophers, the introduction of the modern university in the Middle Ages, the invention of the printing press. Each person could add to the list, but only the invention of writing will be comparable to the full use of computers in education.

In contrast with many businesses, the education establishment has been slow to make use of modern computer technology. The promise of improved efficiency, of doing a better job with fewer resources, is viewed by many educators as a "down-sizing" threat, rather than as an opportunity. This applies in the U.S. across the full spectrum of education, from primary to graduate school. The education bureaucracy, with its emphasis on teaching methods over content, on facts over skills, and with its fondness for standardized tests, is an actual impediment to progress. There is such a gap between the possibilities for improving education and the current level of achievement, that future vast changes are inevitable.

Certainly, educators should stick with traditional ways that work. Many old methods and new experiments involve no computers at all, but may have great merit. For example, the traditional classroom can be dreadful, with students paying no attention to a teacher's droned

inaccuracies (or worse, students *learning* those inaccuracies). But at its best, this model is good—an outstanding teacher inspiring students with wisdom and wit. After all, students have always gathered round a great scholar or poet, to learn. And large numbers of less-gifted, but dedicated teachers have sacrificed to push their students to achieve. An encouraging recent trend rejects the notion that many students are hopeless, asserting flatly that most students are capable of high achievement. Other trends teach students to read critically and to write frequently.

A group of students discussing issues and readings with peers, perhaps aided by a discussion leader, is another good model for learning. Computer technology has relevance insofar as it helps like-minded young people communicate, and current computer communication also forces students to write a great deal. A final excellent model has students receiving individual tutoring. Here computers can supply the free time to enable such tutoring, and the tutor may himself be a student, learning from the experience.

Computers can make a variety of tasks in education easier, including much of the drudgery of homework, exams, and records. Selected subject areas are good candidates for automated machine learning, such as mathematics, language skills, and parts of the sciences; most other areas will benefit. This is not to replace teachers but to relieve them of tedium. Skinner himself never intended his teaching machines to replace teachers. The machines were to assist, particularly in the difficult tasks of providing immediate feedback and of letting students proceed at their own pace. Future software tutors will be far better than anything Skinner imagined, but a human's interaction will still be needed. Skinner did not go far enough in actual implementations of his ideas in classrooms. He should have proved his methods to the world, but he likely would not have succeeded due to technological limitations.

American education is moving toward project work, where students work individually or in groups on an extended project that involves a number of different subject areas. The available computer technology does not support these activities well right now, but future schools will have remote conferencing capabilities for their stu-

dents. Members of a project team will be able to access worldwide resources. These members need not belong to a special economic or cultural group and need not be in the same geographic location. In this way the Internet acts as an engine to level opportunities for everyone. Eventually, one hopes for automatic language translation, so the members will not even be limited to the same linguistic group. Machine translation of natural languages has proved far more difficult than the artificial intelligence community initially envisioned, but imagine a future where diverse students can interact in their own languages.

Training in specific areas or tasks will also be available, for adults as well as children, including the new concept of "just-in-time" training to transfer skills as needed. Enhanced displays that overwrite a real scene with additional guiding information will provide certain types of computer-enhanced skills with no training at all.

Optimism about the future collaboration between computer technology and education is based on the capabilities of computers to do anything at all that people can articulate. It is in their versatility that these machines excel, though the decreasing costs and ease of accessing information world-wide also help. Education is the perfect application area for mankind's new creation. Pick another area, such as food service, and one sees the difference. Computers can greatly aid the task of feeding the planet's teeming population, but in the end a farm or factory must provide actual physical food, and an agency must move the food to consumers—it cannot be virtual food. In contrast, education can in theory be reduced to the transfer of data, retrieving it and presenting it to individuals. The practice and the details, as opposed to the theory and the overview, will be a daunting task, just getting started in my lifetime, but as with other areas of human endeavor supported by computers, there are no limits to the help that computers can provide.

9. The Dark Side
Harm from Computers

Hütet nun ihr der Wissenschaften Licht
Nutzt es und mißbraucht es nicht
Daß es nicht, ein Feuerfall
Einst verzehre noch uns all
Ja, uns all.

—B. Brecht, *Leben Des Galilei,* 1939, Akt 15.

Now tend the light of science
Make use of it and don't abuse it
So that it will not, a firefall
One day yet consume us all
Yes, us all.

—B. Brecht, *Life of Galileo,* 1939, Act 15.

I have examined Man's wonderful inventions. And I tell you that in the arts of life man invents nothing; but in the arts of death he outdoes Nature herself, and produces by chemistry and machinery all the slaughter of plague, pestilence and famine. When he goes out to slay, he carries a marvel of mechanism that lets loose all the hidden molecular energies. In the arts of peace Man is a bungler. … There is nothing in Man's industrial machinery but his greed and sloth: his heart is in his weapons.

—G. B. Shaw, *Man and Superman*, 1903, (middle of Act III).

… in the visible Church the evil [is] ever mingled with the good, and sometimes the evil have chief authority.…

—*The Book of Common Prayer, Articles of Religion,* 1979, p. 873.

Writers have always had a problematic relationship with evil. Think of Milton's masterpiece, *Paradise Lost*, with critics calling Satan the "hero" of the poem. Dostoevsky told friends he feared readers of his novel *The Brother's Karamazov* would follow the wrong example.

I expect to fare no better, but misuse of technology is a serious topic. Innovators, for example, those involved in nanotechnology, are reluctant to describe the full range and nature of possible misapplications, for fear that someone will be inspired to try them. Nineteenth century optimism has given way to twenty-first century despair: We are our own worst enemy.

The creation of a new technology often brings forth new categories of crime, not possible before, and the computer revolution is no exception. First, there are new environments for old crimes, like the new world of the Internet, which is a ripe area for old-fashioned swindling schemes, chain letters, say, or pyramid schemes, along with many other familiar crimes. Second, there are variations on old crimes in the new environment, like buying and selling sex on the Internet, and sexual exploitation, which show considerable differences from old versions of these activities, as with an older predator using the anonymity of the Internet to interest a young person before arranging a meeting. Third, computer crimes become possible with new technology that were impossible or not even imagined before. For example, information itself becomes a target for criminals to steal, and sell, and even to buy for resale. And hackers commit a variety of new crimes with motivation that can be difficult to discern—even just for the challenge and excitement. Fourth and finally, individuals with legitimate access may misuse the available technology. This book discusses fears that the surveillance technology would be used for personal ends, to keep track of enemies, say. The possibility of such misuse is the most worrisome of the many crimes that might occur, because it would be carried out by insiders who are authorized to access the computer systems.

This chapter includes only a few ideas; human inventiveness will come up with new ways to misuse computers, ways not imagined by me. However, computer crime does not have to spin out of control. Mature computer technology will eventually provide such thorough oversight that monitors and agents will stop many computer crimes in real-time; the tracking and data logging will identify and analyze most of the others after the fact.

Warfare.

The march to utilize computer technology in warfare proceeds on many fronts, like war itself. Governments have embraced the contributions of all technology, but especially the computers. Up to now, non-computer hardware, perhaps under computer control, has carried out the actual killing and destruction, but looming ahead is all-software warfare: attacks on a computer system through network connections.

Since World War II, nations have used computers for the gathering and dissemination of information, and for related communication, if not directly for warfare. There are myriad sources of information and endless ways to pass it along; the latter causes problems for the U.S., since it can be hard to get information across incompatible systems. Related uses for computers come from control and remote control of devices. Remote control and communication can use cryptographic techniques to ensure security and authentication—after all, the enemy must not be able to intercept or inject messages or to take over control. Remotely controlled weapons systems, whether in the air, on land, or under water, promise to transform warfare, eliminating danger to human controllers, and allowing the use of smaller and faster units.

During the last decade the U.S. pursued its Strategic Defense Initiative (SDI). People whose opinions I trust have called the whole idea misguided, which is the mildest epithet they used. From hardware to software, from computers to physical weapons, the approach was misguided. On the hardware side, the system was to knock out incoming missiles, using other missiles, ordinary lasers, and X-ray lasers, all under computer control. I am no expert in this field, and the details are classified, but the use of a laser to destroy a missile from hundreds of kilometers away clearly requires tremendous power—either a huge conventional power plant in orbit, the means to transfer energy from the ground, or detonation of a nuclear weapon in orbit to provide the energy. Without any back-of-the-envelope calculations, the physical side of these proposals sounded preposterous—even with no enemy countermeasures. So it surprised many people that experts

identified *software* as the most difficult part of the project, or depending on the expert, as the part that absolutely could not be created with existing and anticipated technology. The software requirements called for a distributed database, keeping track in real-time of all the threats from hundreds or thousands of missiles that are part of an all-out nuclear attack. This distributed software, more complicated than anything created before, would have to function after elimination of randomly-selected nodes—a level of fault-tolerance far greater than any previously achieved. Finally, this Strategic Defense Initiative, though billed as a defensive system, always seemed better-suited to offense.

After spending US $55 billion without getting a workable system, the U.S. renamed and repackaged its SDI as the Ballistic Missile Defense (BMD). This new BMD represents a more realistic and more limited version of the old SDI, with intercepting anti-missiles and airborne lasars in the megawatt range, the latter carried on Boeing 747 airplanes. This system is more alarming because its lowered expectations may be realizable and because it still works better for offense than defense.

Software-only attacks can be a part of warfare. Though it may sound like a science-fiction movie, these attacks are of great concern. Hackers have carried out so many successful attacks against military computers that the worries are understandable. Conventional acts of terrorism or subversion destroy power plants or poison water supplies. But what if a country's financial institutions were crippled with a software attack? Other targets could be the air-traffic control system, the phone system, or the computer controls on the electric power grid. As warfare gets dependent on computers, the computers themselves and their software become new points of attack. An enemy could attack a country's computer networks directly. Consider the insertion of viruses and logic bombs in military software and hardware, written not by teen-aged hackers but by experts supported with the resources of a country. Talk about moles! Instead of planting an agent inside a country to use decades later, the new warfare will plant a virus in their computer systems.

I heard rumors from friends that during the cold war, American

and Soviet satellites played games with one another. According to these rumors, each side had hunter/killer satellites, designed to take out the other side's satellites. Just sidling up to the other device and blowing both apart would be easy, but the others would know what had been done, so—still relaying a rumor here—both sides shot the equivalent of BBs at one another, little pot shots not designed to destroy the other satellite but to make it malfunction.

The devices just described (if they existed) were more likely remotely controlled than autonomous. The prospect of autonomous, war-making robots, mobile versions of the agents discussed in the next chapter, is terrifying. These agents need not pass the Turing intelligence test; they only need enough brains to complete their mission, whether destruction or killing. Right now researchers have difficulties just getting a large autonomous vehicle to navigate a road. For these robots, even scene analysis is a big problem that has long occupied the artificial intelligence community. But progress continues. The field is not yet ready to develop small, mobile robots wandering around looking for humans to kill, or with another lethal mission, but they will come. Such robots do not have to be all that capable, and developers should find it easy to kill a person. A variety of approaches will do, say, a tiny air-powered gun firing a minute pellet, almost too small to see, with one of the terrible poisons in a cavity inside the pellet.

I am personally afraid of lethal robots because, unlike the Strategic Defense Initiative hardware and software (and its successors), robots like these should be feasible in a decade or so, assuming reasonable progress. Each individual robot has a simple mission that builds on what the others are doing to carry out higher, more complex missions. These ideas—complexity emerging from simple parts, with bottom-up control—currently occupy one segment of the computer research community.

The techniques of modern biology and of nanotechnology may eventually be adapted to warfare, with unknowable results. And future wars may change to more sophisticated activities—not directly killing people or destroying physical objects. Malicious attacks could destroy electronically recorded history, undermining education, cul-

ture, and a nation's ability to progress. If one views these activities from the present background and vantage, it might not seem like war at all, but it will be serious just the same and may result in destruction of cultures or vast changes in human history, as wars always have.

Pornography.

In the United States, lawmakers have discovered pornography on the Internet. Whether or not they enjoy it themselves, they want to legislate against it, forgetting that America does not own the Internet, forgetting about the U.S. First Amendment free speech rights. Attempts to eliminate pornography will likely fail. To give one reason, illegal non-computerized child pornography is still around despite efforts to get rid of it. And the new electronic medium offers more opportunities for disguise and distribution. For example, with methods from the section on perfect cryptography in Chapter 6, one can easily create two text files: the King James Bible and a random-looking file of garbage. When the two are combined as described, whatever pornographic text you like can be the output. One can make this "perfect" by using two truly random text files that combine to yield the pornography. Each file by itself is random, but the two together will form pornography. If each file is mailed separately, which mailing will break the law?

The current Internet contains raunchy material. There are newsgroups on every conceivable nasty topic, web sites supported by skin magazines. Pick a newsgroup at random, not too far off track, one that illustrates the repetition and banality of many of these newsgroups: `alt.tasteless.jokes`. Individuals send jokes to this newsgroup ("post" them) and others get to read tasteless jokes. After each disaster, no matter how horrible, tragic airline crash or lethal bombing, ugly jokes about the disaster appear, followed by postings about how disgusting the jokes are, and these latter postings are followed by postings to the effect that if a user does not want to read tasteless jokes, he should read a different newsgroup. Posters also like to "flame" their critics—they post even more offensive messages with personal references to these critics. Only half the postings are actual jokes, and fewer than five percent are witty even with a charita-

ble definition of the term. Like all pornography it quickly gets boring.

Other newsgroups are much more explicit. Then there are the pictures: again every possible subject matter, including child pornography, people with animals, the usual ugly material. Digital video technology is rapidly coming on-line, and video clips will be a hot new area. In addition there are "chat rooms" available from commercial vendors, supporting "cybersex," safe sex that uses imagination, fantasy, and sometimes filthy speech—bondage or bestiality or whatever. No need for condoms here, but anonymity often plays an important role. There are still other possibilities I know little about (better not to know).

Pornography on the Internet is similar to what has always been around, but it is far more easily accessed. Another difference now is that a child can download material into the computer at home. I feel that the current applications barely scratch the surface. What are the limits? There are no limits to this digital realm. In a virtual way one will be able to do anything—slay a dragon and make love with a maiden. Or perhaps make love with the dragon. Be Jack the Ripper, to see the blood flow. One can get all that and more, and worse.

Not all the activities described above are harmful, and many are protected in the U.S. as free speech. The chat rooms allow adults to meet one another electronically, and eventually perhaps in person, or for teen-agers to talk about issues they consider important. This situation is like the "pen pals" that have been around for ages, except that the new electronic version is more convenient and rapid. Pornography has even helped promote Internet innovations, as with the "streaming" technology, in which an image is built up partially, and then with more and more detail.

Some people would monitor and control conversations between consenting adults, though I consider even monitoring unacceptable. Students who use a university's equipment, and others who set up a free web page through a service like Geocities, may break rules against pornography in their respective services. This is not a free speech issue since they are not paying for the service; they are using someone else's equipment. But the main concern should lie with interactions between children and adults, and possible exploitation of

children. Early proposals in the United States used technical means for parents to selectively block their children's access to adult material, but these proposals required too much oversight on the part of parents, with cartoon images of parents asking their own children how to enable Internet access controls. More recently the World Wide Web Consortium has released flexible technology that will allow each group to set their own blocking standards. The Platform for Internet Content Selection (PICS) uses content labels to allow users and organizations to choose which sites to block. Thus parents can sign up with the blocking service that suits their philosophy. The technology also allows a user to block outgoing data, such as phone numbers or credit cards (but beware of a clever youngster who could phrase such information in a way the blocking software would not recognize). Soon this software will do a good job keeping children from accidentally accessing a web site that might disturb them.

Gambling.

Legalized gambling has vastly increased in the U.S. during the past decade. Now the Internet is getting into the act. Hundreds of sites allow credit card gambling on sports or horse races, or on electronic versions of traditional games using cards or dice—from online casinos to online bingo parlors. To avoid U.S. laws, most Internet gambling operations have located offshore, especially in the Caribbean and in Central America, where they are becoming important to the local economies. Electronic casinos might even float, with no fixed location, a virtual casino. Whose laws would apply then? Whether gambling should be a crime is debatable, but U.S. efforts to criminalize Internet gambling with legislation and using the FBI for enforcement will only induce the owners to cover their activities better. One might suspect that the larger motive is to protect U.S. gambling and lottery revenue, rather than protect U.S. citizens from unregulated gambling. For example, the only U.S. Internet lottery, run by an Idaho Indian tribe, seems under legal attack more because it is profitable and is cutting into the profits of others, than from any desire to curb crime or protect the youth.

Much of the current Internet gambling is credit card based, with

US $10 minimum bets, and a recent lawsuit may cut into the ease of using credit cards, but the operators will find other ways to get money, since deposits into special accounts are easy to arrange.

Other Problems.

Traffic in stolen information, including trade secrets, computer software, works of art such as music and videos, and phone and credit card numbers, is a major headache on the Internet that will continue indefinitely as a problem. The criminals advertise their services on the same Internet. They then proceed to use for their illegal acts the identical strong public-key cryptography (PGP, say) that supports privacy for normal users. Law enforcement agencies in the U.S. propose the elimination of strong cryptography as the solution. I find it sad to see such short-sighted policy. Even with no cryptography, criminals will find other ways to traffic in their stolen secrets. Equally important, these criminals will be able to disguise their use of cryptography. And ironically, the same strong cryptography can protect against computer crime, especially against intrusions by hackers and others. Society must make it harder to steal the data, harder to hack computer systems, as well as making it hard to traffic in stolen data. Interestingly, some illegal hacker activities serve only to support other illegal ventures, as with stolen phone credit numbers used for computer access.

The Internet is filled with bad information (how to build a bomb) and with incorrect information (cancer is really just an allergy). These are old problems, but the ease of use and rapid availability of the Internet have worsened them. The Internet has also made it far easier to disseminate and promote hate speech.

Countermeasures.

For many of the evils and problems in this chapter, the U.S. is attempting legal remedies—passing laws against activities on the Internet. So in a sense the Communications Decency Act (CDE) is a failed countermeasure, like the newer congressional proposals to outlaw Internet gambling. These measures try to legislate against human nature and

are thus doomed to fail. In such areas a much better method is to decriminalize, while controlling access of minors to the materials and services.

As for the evils of warfare, the crimes here are crimes against humanity. What could society do to make war impossible, to outlaw war? Not much, it seems, if the past is a guide. As with other crimes in this book, factors like poverty, population pressure, disease, and hunger promote war, so one belated strategy would strive to improve these factors. Rapid and open information about wars in progress may help keep them in check, while a huge technological lead (the current U.S. approach) only works in limited cases and until opponents catch up.

Mankind has mostly succeeded in outlawing the use of poison gas in wars, but the gas and other weapons of mass destruction are making a comeback. In a similar way anticipated computerized weaponry promises to bring war up to new levels of slaughter, with the prospect of tiny killer robots or with smart weapons that the armies might lose control of. Try to imagine the equivalent of land mines that are small, smart, and active—seeking ways to kill. Humanity must find a way to prevent the manufacture of such weapons.

For years hackers and computer vandals, as well as true computer criminals, have been gaining ground in their efforts to break into computer systems. Such hackers can launch an automated software attack from their home with only a personal computer. In a matter of seconds, the attack can go forward and often succeed. The same techniques apply to cyber warfare.

People wanting an inexpensive full-featured operating system may install the Linux system (a version of Unix) on their hardware. Once connected to the Internet, such a system is in immediate peril from hackers unless a current list of security patches is also put in place. The person maintaining the system must continue adding these patches indefinitely.

What does an attack get for the hackers? Many of these intruders are just looking for an interesting or sensitive file of data. They would also like to find passwords to continue their adventures. The Holy Grail of breakins is “root access”—in Unix terms, permission to do

anything at all on the system. With this privileged access they can create new accounts for themselves or load special software to make a later attack easy. Other more-serious criminals are after valuable information, while spies, terrorists, and agents fighting a war have grave objectives indeed.

Fortunately for society, strong measures are available to protect computers against the hackers, criminals, terrorists, and foreign agents. Companies and governments are implementing such measures now out of fears of major future attacks; successful past hacker attacks would give anyone pause. Though potentially effective, the measures are not yet widely used and not yet developed in a mature form.

Computer systems are vulnerable because of their complexity, their continual evolution, and the many services they provide. The complexity means that it is impossible to understand the system perfectly or to anticipate every possible attack. The evolution assures that there will always be new parts of the system to attack. Finally, the provision of services implies that a system is open to the outside world in many ways, and this openness to legitimate users provides multiple entry points for attackers.

One can protect a system by making it simple, with few services. For example, a system can be configured so that it sits waiting for a phone call that will give the proper password. If simple, unchanging software responds to a single correct password and to nothing else, then such a system may be secure against attack. This assumes that the password is hard to guess and that the system will not allow endless repeated login attempts using different passwords.

A system that accepts electronic mail from the outside may have many vulnerabilities. Hackers can sometimes trick the system into accepting mail and putting part of the mail into execution. This executing program then might take control of the computer. Since mail systems evolve, it is hard to protect against such weaknesses.

Similarly, any newly-installed software may have modifications incorporating hidden features that will carry out actions on the system the user did not intend. Software with such extra functions is called “Trojan horse” software, because it sits on a computer sys-

tem like a wooden horse, full of enemy soldiers ready to emerge and wreck havoc at the proper signal. Viruses and logic bombs are special cases of this scenario. Legitimate users and even the system's own programmers and maintainers may be interested in subverting the system, making control all the harder.

One protection against bad software uses the authentication described in Chapter 6. In brief, each piece of software installed in a computer system would be authenticated as having no extra Trojan horse code, using cryptographic checks. One can also authenticate that the entire operating system on a computer is unmodified. The authentication system itself can be attacked, and there are many potential pitfalls, but if the authentication is done with care, one can be certain that the software running on each machine is without flaws or additions. Another approach (like the Java virtual machine, for example) runs programs in a controlled environment, where access of a program to local resources is strictly limited.

Now one needs to protect against unauthorized users coming into such a system. In one advanced approach, each user first signs on to a special authenticating computer. This computer checks that the user is legitimate and has the proper passwords or personal features or hardware ID. Then this authenticating computer issues the user an electronic "ticket" with which he can gain access to other computers on the system. The idea is that one gets nowhere without the proper ticket, and that only the authenticating computer will issue tickets. Cryptographic techniques protect against forged tickets. Cryptography also protects against listening in on the network the computers are attached to.

Many other techniques under development will improve computer security. For example, so-called "firewalls" protect against intrusion at the boundary between the outside world and the individual local network. Chapter 3 mentioned intrusion detection systems that check for successful attacks. Right now the hackers almost have the upper hand against computer users, but taken all together, the measures above and more refined versions should close the door on hacker attacks. However, computers may never be safe against an insider, the person programming that particular machine. To protect against such

insiders, a company's own employees, the company must monitor them, pay them well, and do background checks when hiring.

10. Communities
Virtual and Future

Boy—after a hard day at work, there's nothing I'd *rather do than log on to the* congressional internet site! *Except maybe shove large spikes into my eyeballs.*

—Tom Tomorrow (D. Perkins), *This Modern World,* Feb. 1, 1995.

Computer technologies support traditional communities in numerous ways, but despite widespread use of computers, the era of computer applications to communities is just starting. It will take many years for mature forms of these applications to arise. In fact, support for communities is the topic of this book, particularly support for improved security, and for openness, privacy, and free speech. More exciting is the prospect of new communities, the virtual communities, which have their own problems with crime and their own need for support. But the possibilities are scarcely imagined. Distributed Internet communities, such as newsgroups, groups connected by mailing lists, groups that meet at a Web server, and commercial service providers, are so crude that one pictures cavemen huddling underground as a comparison with ordinary communities. The cavemen analogy leads to another point: Primitive men sitting in front of a fire telling stories were not so different from modern men in front of an electronic image, watching a broadcast drama—the nature of human beings has not changed much in ten thousand years; the culture, the technology, and the means of communication are what have changed. And the story-telling around a fire was interactive, while watching television is not; after three generations of passive listening to the ra-

dio and then of passively watching television, society is returning to a full range of interactive possibilities.

Creating Communities.

Four great revolutions in communication and information have created and expanded communities. There have been other important revolutionary events in history, such as the development of agriculture, or the industrial revolution, but they are not directly related to the communication that is central to a community. (And communication is usually also crucial for a revolution.)

The first revolution was the development of speech, occurring as the human species evolved, leading to the formation of communities of individuals who understood one another far better than before. And speech does not have to be sound waves produced by the mouth—the sign languages of the deaf are types of speech in the broad sense. The primacy of speech for human beings can be appreciated by considering the consequences of its absence: Without speech, an otherwise ordinary young individual will often present to the world as if retarded. One sees this clearly with a profoundly deaf person who does not have the opportunity to learn to sign; he may fail in intellectual development, yet the introduction of a sign language to such a young deaf person soon leads him toward normalcy. Speech is mankind's most important means of communication, the most effective aid in creating communities.

The second revolution was the invention of writing and of an alphabet, happening at different times in different places. A society without writing can be technologically sophisticated, with astronomy and medicine, say, but the lack of writing forces societies to depend on oral traditions often controlled by a "priest-like" monopoly, a few individuals possessing immense power. With the introduction of writing, knowledge becomes more readily available to many more people. Writing extends human memory, expands the access to knowledge, and makes true history possible by allowing knowledge to continue reliably beyond its time of origin.

The invention of the printing press is routinely put forward as a revolution, the third in this list and a curious revolution, since books

had existed long before, as far back as the Egyptians and Chinese. The heart of this revolution was that the printing press increased by orders of magnitude the rate at which books could be produced. (A revolution requires order of magnitude changes.) Far greater stores of knowledge could be produced and disseminated far more widely than before. People did not need the mediation of any elite class for the information they could now readily find in books. Libraries were cheaper and easier to create, even personal libraries, and mankind could work with a common base of shared "world" knowledge.

Society is well into the fourth revolution, the computer age of communication, but it actually started in the previous century with the invention of the telegraph, and with wireless radio communication and all the technology that followed, based on information transmission, storage, and manipulation. One hears references to the "silicon" age, but wafers of silicon with computer circuits etched onto them are just one of many computer technologies: Current proposals use disparate materials, from light to DNA. The long-term changes from this fourth revolution will be as pervasive and significant as from any previous one. The order of magnitude increases are in the amount of knowledge that can be captured, stored, communicated, modified, and used—not just writing, but pictures, videos, sounds, and who knows what else eventually. But the revolution is also about the human interactions that can now take place, about the new possibilities for communities of men. The boundaries implicit in old-fashioned communities are crumbling with the onset of virtual communities, while all the old "priestly castes" are changing: from the political power brokers of government and nationalism to the knowledge elite of specialized areas like medicine. Whether good or bad, these changes are accelerating toward a destination not yet perceived.

Traditional Communities.

Previous chapters contained lengthy discussions of surveillance in public and logging of data to improve the security in a community, as well as the use of identification and fingerprinting techniques to keep track of individuals and objects in the community. Chapter 11 discusses agents used to monitor individuals and objects. All these

activities aim to control and limit crime, to make some crimes impossible and to deter others. Also presented were ways to support free speech, privacy and anonymity. The other important area is openness of access to information about the community—a subtle but important means to deter crime by raising its visibility.

Many regions in the United States have pushed open meetings laws and freedom of information laws as important ways to keep citizens informed. The difficulty is that one must go to the meeting or request the document. The new electronic world addresses this problem: David Gelernter's "mirror worlds" will give easy electronic access to all public information about a community—meetings as they take place or videos of meetings archived for later viewing, laws in creation by a legislature or an overview of the history of laws up to the present, current and past official activities of public servants and departments—in short, information about every public aspect of the community, in a form easy to find and use. The same access to information will apply to larger communities: counties, states, nations, and the entire global community—all their activities will be illuminated in many useful ways.

This electronic solution creates another problem: an excess of information. But that will be handled increasingly well by agents that look for information of interest and screen out the rest. One must not underestimate the difficulty of such screening (called "filtering" in computer jargon), but its effectiveness should improve just in time for the glut of information that will assail society.

Yet another problem is the lack of time or interest or energy by individuals who might inform themselves about public events. The quote at the beginning of this chapter illustrates the problem: Who would want to review the congressional internet site? (In fact, though, early in 1997 the congressional site appeared fourteenth in a list of most-linked-to Internet sites.) In the new world, more than in the old, society will need watchdog groups that find time to worry about a particular aspect of life. Such groups already provide summary information for individuals and for the media. The electronic world can be similar, with electronic media and with more rapid dissemination of information.

Equally troublesome is the presence of incorrect or inaccurate data on the Internet, leading to fears that individuals will lend more credence to advice from an Internet discussion group than advice given by their barber or grocer; urban legends are a growth industry on the Internet. Untrue information about areas like medicine could be harmful or even deadly to trusting users. Bad advice will always be a problem, and people will need to rely more on moderated news groups, on special Web sites, or on prestigious electronic newspapers, run by experts the users have learned to trust. After all, that is what one does now in reaching for trusted sources in newspapers, magazines, or on television, and in seeking help in person from professionals.

Adults want to shield children from some information on the Internet. In the U.S., the proposed Communications Decency Act (CDA) would have limited the whole Internet to material appropriate for a child, but fortunately the U.S. courts struck down that law, affirming the right of free speech on the Internet.

There are many other ways for computers to support communities, but for the rest of this section I will emphasize health care and human services: an area of interest to everyone, and as I will show, relevant to the crime focus of this book. Medical services worldwide are moving toward crisis and collapse. Up to now computer technology has been poorly and inefficiently used; society can and will do much better, in this as in so many application areas.

Consider data entry of health information. The computerized hospital chart can be a nightmare of poorly conceived templates and forms, both preventing proper data entry. It need not be this way, and eventually there will be long-term solutions without paper. All-electronic records allow software agents to comb through these digital charts gathering data, looking for problems, supporting research efforts. At present the software doctor is not very good when compared with a real doctor, but these programs already do well in specialized areas such as antibiotic use.

The health-care system as a whole must switch to coordinated records: starting at birth, through schools, and in each private office, clinic and hospital. The problem is to protect privacy of personal

data while enabling the coordination. Here reliable identification is essential. Society must expand the requirements of preventive care for children, and must do even more to encourage preventive care for adults. Why not help and encourage people to stay healthy?—a goal that pays for itself.

Health care mistakes are often treated like crimes, with malpractice trials and monetary judgments and even jail time. Mistakes such as the wrong dose of medicine are usually related to missing or mistaken information. Instead, computerized records will keep track of all health data and will check medicines for consistency and reasonableness. There is no excuse for the occasional order of magnitude errors in dosages. A patient under anaesthesia should not have his health depend on a few monitor readouts and alarms that might beep, but instead he ought to be in the care of a continuous watchful software program, with sophisticated monitoring of many factors at once, individually and in combination. Intelligent doctor and nurse agents can help the real doctor or nurse, never getting tired and, within limits, never making a simple mistake, never overlooking anything obvious. Software can monitor for subtle factors related to health, such as correlations between vital signs and a deteriorating state.

However, the machines, the software, and the monitoring agents must be reliable. Between 1985 and 1987, four sophisticated cancer treatment machines (the Therac-25) killed, burned, or paralyzed six patients seeking treatment. A software error caused the machine to deliver a huge radiation overdose under unusual circumstances when the machine's operator became proficient at changing incorrectly-entered data. Thus the machines may make errors of their own if insufficient care is taken in the programming.

Intelligent doctor agents will do the initial diagnosis, as well as later monitoring. Progress is this area has been disappointing, partly because of the complexity of the application and because of factors that are difficult to measure and quantify, such as "poor" color, "dehydration," or a "stiff" neck. I expect researchers to invent hardware that will allow amateurs to measure such factors. In the end much of diagnosis and treatment will be computer automated.

The provision of human services poses even greater problems

to current U.S. society, especially attempts to cope with child abuse and neglect. These problems are a challenge to techniques from this book. For example, child neglect usually results from poverty and ignorance. Society should educate the neglecting parents and help them overcome their poverty. Computerized and coordinated tracking and even monitoring can provide support, but involved social workers who are not overburdened are more important. In contrast, child abuse crosses class lines, but it is also difficult to deal with. Again careful tracking of coordinated health records will help. In cases of known abuse or neglect, the involved individuals' right to privacy in their homes should be eliminated, with monitors on the child or parent or in the home. Especially if a monitor is installed voluntarily, its presence may enable an offender to regain self-control and keep from committing abuse.

Virtual Communities.

The explosion of activity on the World Wide Web in the past few years should convince skeptics that a revolution is taking place. There is even a proposal to measure Internet progress in "dog years": Seven years of change on the Internet would occur in one year in the "real" world. Yet experts continue to complain about the Internet, about its failings and immaturity, as if what one experiences now is all that will ever be available. The current Internet is like an infant just starting to look around and crawl; the mature Internet will give vast new capabilities. As each new generation of the Internet has given way to the next, no one seems to have the imagination needed to predict subsequent generations.

Bob Metcalf has given a list of the different kinds of Internet that have appeared over the past two decades. The original Remote Login Internet allowed individuals to employ a standard utility (`telnet`) to become a remote user of any machine (with an account on the machine). Then the File Transfer Internet appeared, where another utility (`ftp`) facilitated convenient downloading of files from remote machines. The Electronic Mail Internet let users of machines send each other e-mail, while the Newsgroup Internet completed the picture by encouraging discussion groups on specific topics. The World

Wide Web brought accelerating changes. With the Web Publishing Internet, each organization and individual published their own home page. Now, the web has moved on to the Electronic Commerce Internet, with everyone trying to do business on the Internet. Metcalf suggests that next may come the Telepresence Internet, followed by a multitude of experiments leading to "many next-generation Internets, each evolving at its own pace, and some of these are evolving very rapidly indeed." There is the Portal Site Internet and the Internet of Connected Communities, the Electronic Gaming Internet, the Multimedia Internet, the Agent-mediated Internet, and a host of others.

It is remarkable how quickly the old paradigm of the Newsgroup Internet was replaced by newer web-based Internets. The old version, still widely used, has newsgroups sending all articles to all Internet nodes. Each news service copies the articles and selectively makes them available to individuals interested in a particular newsgroup. In effect, all news comes to each user, and the user selects what is of interest. The new paradigm has each server web site supply information to users based on their request for it. In this case the user goes to the data. Both modes are more complex than the above discussion might indicate—for example, with mailing lists used under either the old or the new methods. Still, the new interactive and accommodating paradigm will supplant the old one in short order, and the pace of change will continue. Society can expect a continuing flood of changes, of new paradigms. These are examples of experiments to empower people. Many users are still typing text on a screen and reading typed replies; later evolution may favor content over the current enchantment with glitz.

Crime will continue to exist in new virtual communities; in fact it is now emerging as a problem, but it should be easier to deal with than in corresponding physical communities. While many kinds of traditional crimes are non-existent. there is a new emphasis on crimes involving privacy (and its violation) and involving anonymity (and its use to spread lies or hate speech or even child pornography or libelous speech). A given community can choose to support a limited version of anonymity or can ignore it. The use of anonymity by criminals is an insufficient reason to make it illegal.

An avalanche of books about virtual communities has nearly smothered interested parties in possibilities.

As for the nature of virtual communities, they will be whatever the users desire. Any group of individuals in the world that wants to band together electronically will be able to. And what will they do? Almost anything will be possible. Lovers will not be able to hold hands from a distance, nor will someone pat his remote brother on the back. Touching and feeling activities will be curtailed in a virtual community, but eventually one will experience the realistic three-dimensional presence of other people almost as if meeting them physically in the same room. The new medium mainly extends the possibilities, rather than limiting them, since many striking visual experiences will be collectively available. Critics of the new technology say that live, face-to-face interchanges are essential, but there has been little experience with full-motion, high-quality video exchanges, and these may even be an improvement over face-to-face meetings. People picture hard core computer users of the future parked in front of a screen with an intravenous line for food and an inserted catheter for bodily functions. In time, however, users and computers will communicate using natural speech, while technology will bring 3-dimensional images to individuals wherever they are, in convenient, easily-used forms. Virtual meetings will eventually function better than the old face-to-face ones.

Future Communities.

The Internet may relieve the alienation and isolation that many in larger cities are experiencing. Modern technology has aggravated this isolation, so it is only fair for the technology to help with a solution, although some writers feel that the Internet is only making matters worse. In communities both large and small, society must improve its provision of services such as health care, education, crime prevention, entertainment—in short, the factors related to quality of life for citizens. Much of this book concerns these issues. Cities across the U.S. are experimenting with a community network to enable discussions of problems and to give access to information about all aspects of the community—government, education, health care.

At the same time, the Internet will rescue small towns from economic oblivion, as it becomes feasible to live in smaller communities remote from work and away from one's extended family and friends. Towns that are physically remote need not be remote in any other sense. Many jobs already lend themselves to telecommuting, that is, carrying out the job at a distance though a data link. At present, one starts with a job and tries to perform it as a telecommuter, but in the future, one will start with the idea of telecommuting and adapt or create a job within this constraint. With a base of just a minority of telecommuting families, a small, isolated community becomes viable again, where it is possible to live and yet be gainfully employed. The same small town can enjoy electronic versions of cultural events, sports, museums and other attractions of a larger community.

Opponents of extensive surveillance picture scenes out of a horror movie about a small town: all individuals constantly monitored—fined, jailed, or worse for the smallest infraction, such as chewing gum or crossing against a traffic light. I picture such a future town as almost the opposite: an idyllic setting with residents who hardly think about crime at all, let alone worry about it. People will chew gum even if they are not supposed to, but unobtrusive surveillance cameras will target rare random serial killers, catching them early in a crime spree.

The outward simple look of such a town will mask hidden sophistication and complexity. The community will not just be alert for criminals, but will protect itself against a variety of threats—environmental, economic, and social—threats from the inside as well as the outside—subtle threats against its way of life. Open information, free speech, education, and long-term planning—all supported by computer technology—will help protect against these threats. And the town will be a part of a hierarchy of larger communities, culminating in some global organization.

11. Agents
Acting on Our Behalf

The words on pieces of paper in desk drawers don't change one day to the next. But, a paragraph in a compound document constructed by linkage to a corporate reporting system might be automatically revised to reflect updated information. This is a benefit in many situations, automatically pruning our personal libraries of obsolete information. But while-we-sleep revisions also carry Orwellian overtones of archives that always seem to say the "right" thing.

Peter Coffee, *PC Week,* 1995.

Agents are computer programs that do routine tasks on one's behalf. (More inventive and active agents are also called "bots" now.) Agents are constructed in software, though they often control hardware devices. They are *autonomous*, that is, working on their own without minute-by-minute direction from their owners. As time passes they will be increasingly *intelligent*, meaning that they can learn from past experience and will do ever more complex tasks—tasks that have required human intelligence. Society stands at the threshold of the era of autonomous, intelligent machines.

These agents are important for all areas of computing, from browsing the web to controlling a factory to fault detection in a network, but they are particularly significant for the surveillance technologies discussed in this book. Combing through databanks searching for the identity of a lawbreaker is an arduous task, best done by a computer agent. The widespread tracking and logging advocated here will require agents for any practical implementation, since human supervisors could not keep up with or coordinate all the data.

Either immediately (in real-time) or after the fact, these agents will call suspicious activities to the attention of a human being. Computers will have agents monitoring each other and even themselves; the activities of *these* agents will be monitored as well, and so on in a circle or a regression.

People might picture an agent as a tiny robot, with clever miniature gears and wires and sensors, but the reality is much more interesting and exciting: These are *software* agents, electronic information. They are expensive to create initially, but replication is nearly free. The agents can be stored like any other data, on disk or CD or tape. They are easy to transmit over a network, so one can copy them into a home or office. They will run on standard hardware, for example, on personal computers. Here is the new breed of machines: *logical* machines created as a set of instructions to hardware, the most complicated machines ever constructed. Already they can have millions or even billions of components—soon much more. Advanced agents are also mobile, meaning that they move between machines on a network (making copies of themselves), and they can cooperate with other agents toward a common goal. These versatile machines, with all their advantageous properties, as well as their potential for mischief, are transforming society.

Ancient History.

Computer scientists love to refer to anything not current as ancient. Leaving aside devices initiated by a timer, the earliest autonomous agents were elevators. Elevators work well on their own, though impatient people may curse a bank of elevators for all going up at the same time—not very intelligent of the elevators, no coordinating movements. Modern elevators have sophisticated behavior based on anticipated passenger demand. Elevators work so well now that it is hard to think of improvements. For example, many people do not want elevators talking to them. There would be less resistance to elevators that listened and understood; one tells it the floor that is wanted, or even *what* is wanted: "I'd like the floor with Dr. Rogers' office on it, please."

The first computers did one thing at a time, what the machine

instructions told them. But in early Unix systems and elsewhere, designers created programs that would run all the time, concurrently with other user programs, looking for problems to attend to or carrying out periodic routine actions, such as purging unwanted files. These programs ran even when no one was around to monitor them—the first true autonomous agents. By a twisted ominous fluke, the programs were called "daemons," with the archaic spelling to help one imagine the worst from these creatures if they ever got out of control. I do not think this use of the word "daemon" has yet intruded into the paranoid religious segment of the public, who would distrust and personify these entities in any event. Each modern computer system has dozens of these busy software creatures—some working intermittently all the time, others waking up periodically to work, say at midnight (more ominous imagery) and then going back to sleep until the next midnight. Of course, these programs are just another form of machine and do not have personalities, though as they get more complicated, more capable, the word "just" will apply less well to them as machines. Modern systems will help programmers write their own daemons—I mean, *agents*, to work for them. A trend already in progress will make it easier to create agents using friendly, high-level interfaces.

Until the recent advent of web-centered systems, client-server computing was a technical term linked with agents, the latest term that every prospective employee needed to mention during job interviews. A *server* is a computer with agents ready to work over a network to render a particular service to a *client* computer—hence the name client-server. Any network-connected computer that is in a position to provide a service can become a server. For example, a computer may have a Spanish language dictionary that is not found on the other machines. Rather than distribute the dictionary to all machines in the network, the modern approach arranges the system so that a request for the dictionary entry of a Spanish word is routed to the proper machine. This way everybody else saves the space needed for the dictionary. More importantly, only one machine has to worry about this particular dictionary, so that if the dictionary is replaced with a better one, everyone gets immediate access to the better copy.

Another example of advantages of the client-server approach comes with lists of electronic addresses. Most machines need such lists, or at least *access* to the lists, and that is the key idea. One could distribute each list to every machine, but then changes in a list would need careful distribution. If only one server provides access to each list for all machines, then it is easier to keep the list up to date, and inconsistent entries for the same entity are impossible. This example leads to the quote at the start of the chapter: Increasingly, information will not be stored directly, but as a link or a chain of links to the real data, so that one always accesses the latest correct version of data.

The client-server approach involves excess network traffic, as the two sides communicate. In a modern agent-based system, the client will send the data needed for a request to a server, but the client will also send an agent to help the server manage the request. In the end the request is handled better and communication requirements are much less.

Two other concepts are often linked with agents. First is the Personal Digital Assistant (PDA). Versions of this little device are announced weekly. It is supposed to assist in all personal activities: the calendar and appointments, note-taking, letter writing, and so forth. Some PDAs can recognize handwriting, so that one need not type comments. These are mere precursors to the important agents to come. The second concept is the Graphical User Interface (GUI). This is touted as a world-saving issue, but a GUI is just a particular way of communicating with agents. In the end one will talk with these agents, rather than writing notes to them or typing commands.

Re-inventing the Wheel.

This section's title is a derisive phrase in engineering. After inventing the wheel, after solving a particular problem, one should not spend time and resources inventing the wheel again from scratch, or solving the problem anew. Modern computer technology embodies this idea in the important theme of *caching*. Computer information storage is arranged in a hierarchy, from slow and cheap to fast and expensive. At each level in the hierarchy, recently used data is saved on the fast side in case the computer needs it again right away. If the same data

is needed a second time, the system may be able to find it in the fast cache storage, without having to spend time fetching it from slow storage. In the same way the writing of data to the slower medium is delayed in case it is soon written again in a newer form. In essence, the system is *saving answers* to common questions so the answer can be reused, and one need not compute or fetch the answer again.

The retrieval of web pages at the request of users (mentioned in Chapter 10) also uses caching: the most recent web pages are saved in a user's own computer so they will be available again without fetching them. Advanced systems employ more levels of caching with "proxy servers," that is, extra web servers closer to the users that save recent web pages.

But what if it is easier and cheaper to compute the answer from scratch? Engineers and scientists once made extensive use of tables: logarithmic and trigonometric tables, among others. It turns out that it is far easier to compute these quantities fresh each time with an algorithm than to store the results in a table. Consider the mathematical constant π, now known to over 50 billion decimal places. In the previous century a mathematician named Shanks made his reputation calculating 707 digits of π. His triumph was not spoiled in his lifetime, but his last 180 digits were wrong—twenty years of effort wasted. It might seem reasonable to store a few thousand digits of π in case they are needed, but a modern workstation can calculate these digits from scratch in a fraction of a second.

As a thought experiment similar to this book's title, one can ask what computer systems might be like if unlimited storage were free, and access to stored data instantaneous. In that case one might keep track of all answers, of all calculated quantities, only calculate any given item once. On the other hand, if computing power were free, and anything could be computed instantly, one would re-compute everything from scratch. Reality lies between these two extremes—neither storage nor computing power is free. In practice, systems do whichever is better, either save results or perform the experiment again. Autonomous agents commonly solve problems fresh each time a solution is needed, though these agents can also save answers for reuse if that is convenient.

Intelligent Agents.

The real excitement in any discussion of agents is their possible intelligence. The computer genius Alan Turing developed an abstract concept of a machine in the 1930s before there were any real computers. In 1950, he addressed the idea of machine intelligence by imagining a remote-controlled typewriter, either connected to a human at the other end, or to a machine pretending to be a human. What came to be known as the *Turing intelligence test* for a machine is whether the machine could fool a human being into thinking it was human, too. Debates about the Turing Test swing back and forth, as one person argues that there is more to intelligence than typed responses, no matter how clever, and another says that the ability to write convincing answers would prove intelligence. Current agents are not remotely close to this goal yet, but they should be able to do useful work even within their limitations.

For thirty years the artificial intelligence community has predicted the imminent arrival of intelligent machines. I am not being entirely fair, and the early optimism has long since waned. Decades ago the artificial intelligence community started a debate of morality issues when dealing with intelligent machines that continues to this day. Should they be created? If created, is it immoral to terminate them? There are many similar questions, ones that will not need answers in my lifetime. But even if not truly intelligent, these complex and capable machines will be doing ever more significant tasks on behalf of their creators.

Computer scientists are now transforming the Internet from a passive network into an active entity, a collection of interacting, intelligent agents. Sun Microsystems has the current hot proposal, but whether or not Sun's specific products survive long-term, the promise of cooperating, transferable agents is here. Sun named its language for creating portable and downloadable agents "Java." Now other caffeine-laden names permeate this area. In the future, to get a service from a Web site on the Internet, one will not ask questions and figure out how to obtain the service and how to use it, but will fetch an intelligent agent from the remote Web site into the local computer;

the agent will proceed to deliver and carry out the service without intervention.

Or consider what a library is: a repository of information, right? One goes to a library, physically or electronically, and retrieves the desired information, perhaps with help from a librarian. I foresee a future with all the emphasis on library agents and none on the library itself. The intelligent library agent will retrieve data from anywhere: remote archives of data or databases, libraries, museums, special collections of every kind. The agent will be willing to take action: calculate answers to questions, experiment, access the real world, apply inference rules. For example, if one wants a map, the agent might fetch it from an archive, or might create it from raw data describing the region in the map, or might use an orbiting satellite to photograph the area of interest in real-time.

These agents will do *anything,* not just data processing and computing activities. They will run businesses and homes, governments and their agencies. They will manage personal affairs. Each home microwave oven will have its own address on the world's network and its own agent running it, protecting against theft or accidental misuse, cooperating with other agents in the home, calling for remote diagnosis of problems and for repairs, whether remote repairs or actual physical ones.

Agents for Monitoring.

I propose to use extensive monitoring and surveillance of the physical world and of society's new electronic realms. Software agents should do this monitoring because there is too much of it for the humans and because the agents will do a good job, at least in their capacity and in their never-sleeping attention to detail.

An extended example concerning environmental pollution will help clarify these proposals. The chapter on fingerprinting (Chapter 4) discussed ways to catch polluters after the fact, using fingerprints placed directly on the industrial materials, so that trace amounts of additives would show the source of pollutants. But monitoring and detection of the earliest stages of pollution is a far better method—to eliminate the pollution before much of it occurs.

Underground storage of gasoline provides a serious pollution problem for discussion. The U.S. uses such underground storage tanks everywhere, storing gasoline or oil or other liquids that will harm the water table in case of a leak. Gasoline floats on top of water, so a water well near a leak will bring up even more gasoline than might be expected from the size of the leak.A pilot project carried out by Dr. Jerry Keating in San Antonio does a good job of detecting gasoline leaks at filling stations. A floating sensor in each tank accurately measures the tank's gasoline level in a manner similar to the gasoline gauge of an automobile. Other sensors access the gasoline pumps and determine the amount of gasoline removed. Using these sensors, a computer at the station can keep track of the gasoline in each tank—the amount removed and the amount remaining, as a bank does accounting with its money. The software checks for a time when all the pumps attached to a given tank are closed down, and then measures the gasoline level in the tank. A leak shows up as a tank level lower than it ought to be.

In practice complicating factors intrude. A truck driving by will make waves in the tank and disturb the floating sensor, making an individual reading of the level inaccurate. Calculations must take the temperature into account and even the amount of gasoline vapor in the air above the liquid gasoline. Accuracy requires multiple readings and an application of a statistical analysis to the data (a regression analysis).

Using multiple readings of the level, the software can detect a leak of two-tenths of a gallon per hour in a week or so. In a month, the system can almost catch a leak rate of one-tenth of a gallon per hour. There are fancier sensors than a float that would increase accuracy and allow detection of even smaller leaks, but two-tenths of a gallon per hour is already a small rate. A larger leak, say, a gallon per hour or more, would show up immediately.

The U.S. federal government will require accurate reconciliation of gasoline amounts by 1998, but unfortunately, the method described above is just now being abandoned in favor of another that is simpler and less accurate. This other method sends pump readings and levels obtained with a dip stick off for processing and would only catch a

much larger leak after several months of leaking.

A profit-oriented oil company has reasons not to want the accurate leak-checking system in place. By one estimate, perhaps a quarter of all tanks have a slow leak, and digging up tanks or otherwise repairing leaks is expensive. A leak of one-tenth of a gallon per hour is about 900 gallons per year—a loss the company could ignore if it wished. Also, the system described here costs perhaps US$5000 to install, and there would be additional maintenance costs. One benefit to an oil company is early detection of gasoline theft. During the prototype experiments in San Antonio, a filling station manager filled his own truck's tank with sixteen gallons every Sunday afternoon when the station was closed. This theft was serious even though an unsophisticated manager stole a trivial amount, but the system would also catch important larger thefts.

The point for me is not this particular leak-detecting system, but the fact that such leak detection is feasible within a reasonable budget. This is an important social and environmental issue. Early detection of gasoline leaks is necessary to avoid later, more expensive problems with the water supply. If laws require all filling stations to detect these leaks, no station will be at a competitive disadvantage, and the loss in profits will be small, partly offset by the gain from not losing the gasoline.

Society should provide the world with monitors like those in a giant airliner, endless dials and gauges and warning lights, attended not by humans but by clever software agents, checking for all manner of problems and hazards.

Problems with Agents.

I am a fan of these agents and would like to see them widely used, but I realize that their utility depends on the application area. For the crimes of stealing or leaking gasoline, agents for leak detection seem like a good solution.

However, if society is not going to do anything about a problem uncovered by monitors and agents, there may be no reason to deploy them. For example, ozone and other pollutants in the air are often not effectively dealt with, and people may not need monitors to real-

ize the extent of the problem. Even here the monitoring is useful to pinpoint the exact areas affected, while research may help determine individual contributions to the problem and the best ways to reduce it.

The previous section passed quickly over problems of accuracy, reliability, and maintenance of the monitors and sensors and of the computers running software agents. Anyone with troubles keeping a personal computer working may not consider this a trivial issue, but there are ways to spend more money for improved reliability, including the use of multiple central processing units and other redundant hardware. Also, reliability problems often come from changing software, and systems used for monitoring should not need such frequent changes.

The expense of wiring up the world with monitors is another concern, and this chapter contains no careful cost accounting. Nevertheless, the prevention measures made available by more-vigilant monitoring are bound to pay for themselves. As with other issues in this book, society cannot afford *not* to monitor more extensively.

Finally, there is the danger that society may delegate to autonomous agents more than it intends. The New York Stock Exchange now has rules against automated stock-transacting agents after analysts blamed these agents for the severe 1987 market decline, when the computer-generated program trading agents issued huge buy and sell orders, faster than anyone could follow. The fear is of a future major crash—perhaps greater than the 22.6% drop in 1987. Thus human supervision is needed for agents that might quickly initiate a cascade of actions.

12. Planning
What Makes Us Human

In schools and through the media, people should be taught or reminded of the selective nature of their perceptual systems and their inadequacy for registering many ominous trends. People can be trained to have "slow reflexes" as well as quick ones; they can learn to react to the continual expansion of human numbers as adaptively as to a car swerving into their lane.

—P. R. and A. H. Ehrlich, *The Population Explosion,* Simon and Schuster, 1990, p. 189.

Planning is an essential part of the ideas in this book, which puts forward complex and interrelated suggestions for openness, privacy, and free speech, along with data gathering in public, all requiring plans. Especially important are long-term plans—a weak point of current society. Good planning is so difficult that it is not surprising society has often made a bad job of it. Yet the difficulty is no excuse: the form of society and even mankind's survival as a species will depend on the plans made and acted upon.

Humanity ought to plan and control its future. "No one has the wisdom for that," opponents say. But planning is a major factor distinguishing human beings from animals—the human ability to anticipate consequences. Humanity behaves like a blinded giant, staggering along without direction. Few modern countries have long-term plans in place. In wealthy countries like the United States or Germany, the politicians and planners can scarcely cope with problems as they arise; a city like Calcutta survives from day to day, from crisis to crisis. Even a hypothetical planning state (as Japan was once

thought to be) would be limited to local plans because it resides in an interrelated, unplanned world.

In many areas of the world the criminals seem to plan better than the governments in power, whether these criminals are engaged in petty crimes, organized crimes, or crimes committed by industries or governments—the full spectrum. To make crime impossible, society needs a technological lead on the criminals, including computer use and especially planning. People who want no planning, or no centralized planning, or no coordination of plans, put themselves in subjection to those brilliant, ruthless individuals who will plan for them. If society itself fails to plan, schemers will lay awake at night, seeking ways to take advantage, to exploit weaknesses, to improve their own lot. Society needs planning, interspersed with wide and open debate.

The Difficulty of Planning.

Planning may be humanity's most difficult activity, yet its most important. Everything depends on the quality of the plans and on their execution. Why is planning so hard?

Part of the planning activity is a prediction of the future, which is notoriously hard. Long-term planning requires long-term predictions, and these go beyond the simple extrapolations and trend analyses available for short-term predictions. Events in the real world involve a huge number of variables describing quantities often poorly understood. And unpredicted, unexpected events, even unique events, often occur. Thus predictions, and hence planning, are inherently difficult activities.

Modern chaos theory shows that the prediction of many aspects of the physical world, such as weather, will always prove impossible. The most minuscule influence on weather, the "beat of a butterfly's wings," will in months or years produce an arbitrarily large alteration. (Weather trends and patterns can be predicted, but details will remain hidden.)

Then there is the problem of bad plans. How can one recognize them, how avoid them? Some plans are bad for everyone, but other plans may favor one segment of society at the expense of another. This is often a critical problem: choosing from among plans

that have different goals, that favor different groups. It will always be difficult for people with different goals and philosophies to reach agreement. And effective long-term plans need global scope. Local implementations of plans may not be acceptable world-wide.

It is also difficult to follow actions dictated by plans. Particularly hard is formulating and following plans that lead to long-term benefit where the short-term performance is poor or even harmful. Capitalist companies have a "now" marketeering focus. What U.S. companies would build products to deliver long-term benefits? Employees of companies are usually evaluated on and rewarded according to short-term successes. Consumers are not conditioned to ask for "twenty-year products" and to invest in them. (Before its recent economic problems, Japan was regarded as a partial exception.)

The quote of Paul and Anna Ehrlich at the beginning of this chapter refers to a tendency of humans to worry about rapid changes and immediate threats while ignoring long-term problems. This is a tendency selected for by evolution: those who survived concerned themselves with immediate problems. Countering this tendency is precisely what long-term planning is for—to call attention to possible long-term consequences.

Finally, there is the problem of the bureaucracy of planning. What is to keep planning and others of this book's proposals from becoming another tool of Kafka's "Castle," a burgeoning but unassailable bureaucracy that individuals have no access to, let alone control of?

Lack of Planning.

Societies without planning leave themselves at the mercy of chance events; some such societies have been lucky and flourished, while others have gone through great suffering or have become extinct. I contend that openness, free speech, simulation, and predictive tools will allow the planning and consensus building needed to avoid many problems—new intractable problems, problems on a larger scale than anything in previous human history.

The remainder of this section discusses several problems partly created by a lack of planning. While these are admittedly difficult

problems, society absolutely must study them and similar ones—gather data, run simulations, formulate plans—the alternative of doing nothing guarantees future disaster. Each problem in this section contributes directly and indirectly to crime, makes control of crime more difficult; each problem makes people poorer and more unhappy and desperate, more willing or driven to commit crimes.

The number one problem on this list is overpopulation. As the Ehrlichs say, "Whatever your cause, it's a lost cause without population control." Many crimes can be traced to an excess of people. Overpopulation illustrates how hard it is to deal with a truly difficult problem: some will not agree it is a problem at all, while those in agreement will not agree on a course of action. The lack of scientific knowledge contributes to the intractability. As the Ehrlichs put it:

> And people of varied political persuasions who are unfamiliar with the magnitude of the population problem believe in a variety of far-fetched technological fixes—such as colonizing outer space—that they think will allow the need for regulating the size of the human population to be avoided forever.

These people may not be familiar with simple models of population growth, true for every species, from bacteria to humans. First there is an exponential growth phase, then either a decline in the growth rate as the size grows to the maximum level the environment can support, or a fall in the absolute size, due to problems created during the growth phase. Exponential growth would overwhelm any environment, even the entire universe—this growth is always self-limiting. Current society is still in its exponential growth phase, but the limit is in sight. Humankind will run up against it perhaps soon or perhaps late, but the growth rate *will* decline and stop.

Population biologists study fluctuations of animal populations—deer are one example. Suppose one kills the natural predators of a deer herd. During early exponential growth, the herd is in deer heaven. As the deer population nears the environmental limit value, the deer eat everything available, they reach as high as they can for leaves. In this case the growth is followed by a population *crash*, usually to a small size, sometimes to extinction, because all the easily

reached vegetation is gone. Humans are not deer, but as they "reach for" resources, they can reach far indeed. They search for oil under sea and under ice. If the world economy ever falls apart, many resources will be hard to obtain. There is a harsh logic here. As society uses its ingenuity to cope with increasing population, as it postpones the final reckoning, it makes the eventual problems worse. The worst scenarios get short-term productivity gains by exploiting non-renewable resources. Humanity is pursuing exactly this strategy. Many people now feel that such policies, avoiding long-term plans and ignoring long-term consequences, will lead to a deeper and more serious population crash.

Yet another dark side to the population crisis could lead to solutions as bad as the problem itself: the emergence of controlled societies that become "cultures of death" in their zeal to limit population. A focus on control, rather than on openness and free speech and privacy, could lead to such outcomes as population grows.

Greenhouse gas emissions give a second example of an intractable problem that planning should address. Here humanity is increasing the carbon dioxide content of the air without a clear idea or model of the consequences. Even current simulations fail because the effects of these emissions are so poorly understood. However, changes in weather patterns are likely to be harmful, whatever form they take. It is a hazardous undertaking to risk major changes in the world's climate.

As a third example, consider the problem of antibiotic-resistant strains of bacteria, such as forms of tuberculosis found in some AIDS patients and others. The World Health Organization said that three million people died of tuberculosis in 1995, and for drug-resistant strains it now takes a cocktail of four drugs to effect a cure. Despite these hazards, antibiotics are used on a vast scale, overprescribed to humans and routinely included in the feed of farm animals. The emergence of diseases resistant to the old cures is a result of terrible planning along with greed for short-term profits.

Energy policy worldwide, and especially in the United States, provides yet another example. Actually, there is a near absence of a reasonable and effective long-term U.S. energy policy. During the

1996 U.S. Presidential election, gasoline prices rose modestly, and both major candidates responded with questionable short-term measures to lower prices, while automakers pushed out new gas guzzling sport utility vehicles in response to public demand.

As a final example, consider the year 2000 software crisis, the difficulties computers will have in adapting to the new millennium. How is it possible that so few took the problem seriously until it rose up in front of society just short of the transition? At the least there will be widespread panic before the changeover, but no one knows how difficult the problem will be.

Those Who Predict.

The world is filled with plans and planners—numerous books about planning, from births to weddings to deaths. The plans for meals and holidays and countless other contingencies are mostly short-term. Long-term plans are rare except for personal affairs such as wills. Short-term planning can assume unchanging conditions, while long-term planning requires long-term prediction.

Who makes long-term predictions? A variety of groups have always made such prophesies: philosophers, novelists, scientists, futurists, science fiction writers, and scholars in many fields like religion or sociology. Consider the utopian books, from Plato's *Republic* and More's *Utopia* to B.F. Skinner's *Walden Two*, along with the anti-utopian *Erewhon* by Butler, and the modern anti-utopian classics *Brave New World* by Huxley and *1984* by Orwell. Many predictors have been Cassandras, prophesying disaster and ruin, while others made laughably optimistic predictions. Fundamentalist Christians see a Bible full of predictions about the future. Early science fiction writers like H.G. Wells and Jules Verne were succeeded by a modern host who have pursed endless possible visions of the future.

The sixties saw the entrance of futurists and even The Futurist magazine. These are similar to science fiction writers, but are taken more seriously by modern main-stream society, with their long-range plans, creative imaginations, and "what if" scenarios, looking for paradigm shifts. A large number of authors put forward proposals for fundamental changes to society.

Other long-range predictions come from scientists who talk of future volcano eruptions, earthquakes, unusual weather, and rising global temperatures. The earthquakes are taken seriously, in contrast to so many other predictions of problems, from environmental to political to economic. Thus the predictions are available, while most of the world chooses to ignore them, busy with current problems and hoping the larger long-term difficulties will not come to pass.

Among the myriad groups trying to be heard, trying to make a difference, is the Club of Rome, founded in 1968. The Club consists of one hundred diverse individuals united by a "common concern [for] the future of humankind." They identified three major needs: "To adopt a global perspective ... , to think holistically [seeking] a deeper understanding of interactions within the tangle of contemporary problems ... , and to take a longer term perspective in studies...." Their first important work was a book titled *The Limits to Growth*, which sold 12 million copies. Mainly concerned with the environment, population, and energy, the book was criticized as alarmist, even hysterical. This book was followed in 1974 by the excellent and important work *Mankind at the Turning Point*—a much more positive and forward-looking study, using computer simulations to help produce a detailed plan of action. In the ensuing twenty-five years, their recommendations, like those of other long-range planners, have been largely ignored. Since this early, ground-breaking work the Club has sponsored a number of additional reports, related to issues such as limits to growth (the topic revisited), conflict mediation, sustainable national income, and the environment.

Support for Planning.

This book's ideas do lend support to long-term planning. In order to plan, one needs information. And the results of planning must be available if society is to benefit. For this and other reasons, openness of access to information is a key to better planning and to addressing mankind's problems.

Openness and free speech are just what is needed for society to debate long-term goals and strive for agreement on long-term plans. Assuming the world shifts toward a global community or global or-

ganization, an outcome I sincerely hope for and expect, there will be more sharing of ideas and goals. Education is also part of the same picture—after all, sharing information is a form of education. It is interesting that one proposal to help alleviate the population crisis is better education for women of the world, particularly in lesser-developed countries.

As for Kafka's Castle mentioned earlier, the bureaucracy of planning, society needs to open up the castle, tear down its walls to let people see the plans in progress and the methodologies for creating plans.

There have always been those predicting disaster for the world, so what is new in the current era, not available before? New are the computer simulations that can make predictions more accurate, more vivid, more believable. These simulations can help people appreciate long-term consequences of actions and can help in setting goals and in planning for the distant future. Associated visualization software will help individuals understand implications, as with pictures of one's own future ravaged neighborhood helping to expose poor water management policies.

These simulation/visualization packages will supply a virtual reality environment of unprecedented realism and accuracy and usefulness.

Like a science fiction lens into the future, such systems will provide an array of possibilities for examination. Individuals and societies will better understand the implications of their choices and decisions. There is danger in lending mere simulations too much credence, but human beings are beset with dangers now, and my worries come from a dearth of plans, not from an over-reliance on the planners' tools.

13. The Future
Predictable yet Unknowable

There are two futures, the future of desire and the future of fate, and man's reason has never learnt to separate them.
—J.D. Bernal, *The World, the Flesh and the Devil*, 1969.

It is easier to invent the future than to predict it.
—Alan Kay (common attribution).

There are many visions of the future, but with respect to the areas of freedom, privacy, and control, I fear that mankind's choices will narrow to just two possibilities: one dominated by surveillance and control, and the other with openness, privacy, and free speech. But even the second possibility, the one I hope to see, includes a great deal of data-gathering in public in support of the openness—surveillance, in other words.

Why should there be all this surveillance? Would it not be better to have none at all? As I have repeatedly argued in this book, the gathering and logging of data about all public activities is a good idea if it is accompanied by open access to the data, and by free speech and support for privacy. Matters might be different if fewer people lived in a less dangerous and less technologically advanced world, if rational human beings were more willing to work for the common good. But modern society can no longer afford to leave people to their own devices without keeping track of their public activities. Society faces a range of threats from its members—the most extreme from those who might detonate a nuclear weapon in a city or might release sophisticated poisons or toxic biological agents. Just as worrisome is

the threat of computer attacks on financial or banking institutions, on services such as electric power, and on military systems. Hackers or terrorists or even governments might also coordinate their attacks for the transition to the year 2000, when computer systems may be in a turmoil anyway. Humanity is more vulnerable than ever before.

There is another, more-practical reason to expect widespread surveillance: It is already here. Nearly universal surveillance in public will come whether individuals want it or not. The main opportunity is to twist the course of events—to maintain or add openness and free speech and privacy to the surveillance—to get an optimal balance between security and privacy. Many current societies need only keep or enhance the openness and free speech and privacy they already have, while accepting the expansion of surveillance in public that is occurring on a wide scale, and while demanding open information about that surveillance.

The quotation at the start of this chapter comes from Bernal's remarkable book of predictions and seems at odds with the other two quotations, but in fact, all three of them have the same message: invent the future and make it happen. This is an activist, forward-looking viewpoint, the one promoted here. The problem is how to decide whose vision of the future to embrace, and how to make that future real. Bernal's view is cautionary: desire is not enough—the choices must be possible.

Another cautionary note comes from the history of eugenics, an optimistic program to improve the human species through science. In the late 19th and early 20th centuries foolish and eventually tragic policies promoted the betterment of humankind by breeding and sterilization and even euthanasia; these policies culminated in the eugenics of the Nazi Holocaust. But the new biotechnology now gives eugenics possibilities not imagined before, and scholars are engaging in a rational discussion about which techniques to use. The analogy with this book's suggestion of widespread surveillance may be helpful: Unrestricted and unenlightened use of surveillance could be as bad as the older eugenics programs, but open debate and access to information will allow society to embrace appropriate and reasonable surveillance technologies.

Some individuals may find the current book's surveillance proposals as dehumanizing as Henry David Thoreau found the society of his day, where people owned less and owed more than they used to, and where they tolerated slavery. But surveillance is not slavery—it will liberate society from crime and fear if combined with openness and free speech and privacy. These changes are part of the movement forward into the information age. Informed and empowered citizens will lead the way to the next level of open democracy, whose form one cannot now predict, and to some type of global organization that draws strength from local communities, yet supports activities that benefit all humanity.

Technology Growth.

Why is this future happening? Society is in the midst of a scientific and technological explosion that started with the Renaissance, adding to knowledge ever since. But one area is unique—one recent change differs from all others. Computer hardware capabilities have grown by about nine orders of magnitude in the past fifty years, a factor of 1 billion. Fifty years ago with a month's pay one could buy a mechanical calculator that would carry out one arithmetic operation per second. Pencil and paper calculations are at least ten times slower, while a fast computer at that time would do a few thousand operations per second. Today (in 1999) a month's salary will buy a machine good for perhaps 1 billion operations per second, while a large computer can do more than 1 trillion per second.

The speed of computers has doubled every 18 to 20 months for fifty years. This doubling continues as I write; it should go on for at least two more decades. The reliability of these computers, their size, their cost, their storage capacity, as well as data transmission rates and transmission reliability, have all improved in a similar way. These improvements make the information age possible. There has never been anything else like it. The doubling has continued until its incremental change has led to qualitative changes—transforming everything—intelligent wall switches, intelligent flashlights.

Other technologies have grown concurrently but have not kept pace. For example, advances in biotechnology, incredible as they are,

do not have the exponential growth seen in computer technology. In many areas there is progress every two years, but not a doubling of capabilities. The ratio of walking (5 kilometers per hour) to jet plane travel (1000 kilometers per hour) is only 200. A rate 1 billion times faster than walking is five times the speed of light. Another area of slower progress is computer software, which is notoriously difficult to create and to understand. If progress in computer hardware is the engine driving the information revolution, computer software is the governor, keeping progress in check in many areas. Still other areas of technology have hardly changed in fifty years: The microswitch of 1945 looks and functions just like the ones sold today, and a centrifuge in a laboratory is only modestly improved from far older models.

Here then is the answer to the question at the start of this section: Unprecedented technological advances in computer hardware are driving the onset of the information age.

Limits to Optimism.

I am assuming that surveillance in public is necessary. An optimist would instead assume that no such surveillance is or would be needed. Here is the scientific basis for my lack of optimism. At present, scientists tend to be pessimists about the future, while economists and others are often optimistic. Consider a typical optimistic statement from an editorial.

> … This [the failure of a prediction by Paul Ehrlich about the future price of minerals] adds one more to the long list of Erlich's [sic] predictions that have proven false, notably mass starvation in the 1970s and near-depletion of "many key minerals" before 1985. Yet Erlich retains his standing with the mass media as an authority on the planet's future.… Too often environmentalists' doomsday scenarios fail to allow for human ingenuity. Biologists think in terms of closed eco-systems. But market economies are responsive. The obvious truth is that resources are not static but depend on man's power to adapt and invent.

This editorial gives a common view of non-scientifically oriented in-

dividuals, presenting logical views based on past technological successes. The problem is that resources may not be static, but they are *limited*. This is such a small qualification, it is no wonder some economists and others fail to see any difficulty. And even if they agree with the word "limited," they expect to find new resources to exploit, ones not yet imagined, and such new resources *are* often found. Thus these non-technical individuals are firm believers that technological fixes of an unknown nature will come along to save them indefinitely.

In the same vein, but even more optimistic, are statements in a recent book by Francis Fukuyama, *The End of History and the Last Man*. It is hard to summarize his unusual book, but the book's prediction that liberal democracies will overwhelm other forms of government is based partly on expectations of what technology can deliver:

> Technology makes possible the limitless accumulation of wealth, and thus the satisfaction of an ever-expanding set of human desires. The process guarantees an increasing homogenization of all human societies....

Limitless wealth would indeed go a long way toward making crime impossible, removing the desperation motive of the poor. For example, part of the United States' strategy for reducing crime along its border with Mexico has been to strive for a rise in the Mexican standard of living. In the short term, however, economic and population problems have wiped out potential gains.

With no background in economics myself, I tend to see everything as a zero-sum game, a mathematical construct in which any gain by one person must be exactly offset with a loss by other people. But I know the world is more complicated, that it is possible for all to gain, for life to improve for each person. And information, along with its access, can expand for everyone at low cost. Nevertheless, extreme optimism of the sort described by Fukuyama is not scientifically justified in the world now. World resources will not remotely extend to raise everyone to an American standard of living, even if this were desirable. And many are struggling inside the U.S. Worldwide and with the current population, supplies of materials like iron ore and coal would in theory allow everyone to use as much

iron and energy as the American average, but many other materials would not remotely stretch that far. Meanwhile, food production, water resources, land management, pollution, ocean management and many other factors are heading so clearly toward disaster, that even moderate optimism seems inexplicable. Have these optimists seen no poverty or hunger?

More disturbing than the optimists are recent direct attacks on environmental pessimism. Profound scientific ignorance, exemplified by beliefs such as astrology, seems to be gaining ground, but now a group of intellectuals is promoting a backlash against concerns with the environment and overpopulation. Respected academics maintain that environmental problems have been overstated, that vast areas of world resources remain untouched and should be exploited, that better food production and distribution will solve mankind's overpopulation problem. The illogic of these positions is reminiscent of Joseph Goebbels' propaganda late in World War II claiming Germany was ready for a final push to win the war. In the end, one can only argue against these optimists as Paul and Anne Ehrlich have done with their book: *Betrayal of Science and Reason*. Argumentation continues unabated that there are no environmental problems and no population problem.

Anti-technology.

Anti-technologists have long been around; after all, the Luddite movement occurred early in the nineteenth century. The best-known recent anti-technologist is the so-called Unabomber, now identified as Theodore Kaczynski. At the beginning of his "Manifesto," Kaczynski wrote in part:

> The Industrial Revolution and its consequences have been a disaster for the human race. … they have destabilized society, have made life unfulfilling, have subjected human beings to indignities, have led to widespread psychological [and physical] suffering, and have inflicted severe damage on the natural world.

Kaczynski is a serial killer who, in the most charitable terms, has

severe mental problems. Yet his views were embraced by many, especially on the Internet.

Compare the above quotation with the following one:

> But now the machine era is coming to a rapid close. It has fouled the air, poisoned our waters, killed our rain forests, torn holes in the ozone layer, destroyed our soil and the art of family farming, rendered our young violent and self-destructive, dried up our souls, and sent adults wandering for meaning, bewildered and soulless. … The machine era has also managed to bankrupt itself. We cannot afford industrialism any more.

Though written independently of Kaczynski, these new words have a similar tone. Who is the second anti-technologist? No psychotic this time, but Matthew Fox, a deeply spiritual religious leader, former radical Catholic priest in the Dominican order, now an Episcopal priest. Fox's words come from his remarkable book, *The Reinvention of Work*, and the issue is not what Fox is against but what he is for: a view of work as a type of sacrament, where people will do their work as a ritual combined with the "great work of the universe," which for him is "the work of creation unfolding, the work of evolution or creativity in the universe."

Here then is the range of anti-technologists: from lethal lunatic to religious visionary. In between are lesser extremes, from Kirkpatrick Sale, a chronicler of the Luddite revolution with a profound distrust of technology, to Stephen Talbott, who challenges the assumption that computers automatically convey benefits on their users. Talbott has for years run a fascinating Internet discussion group that debates the utility of these machines, especially in education, where horror stories abound of clueless school districts adding computers and Internet connectivity without a clear idea of how they are to be used in the schools. He maintains that computers inevitably limit human consciousness and creativity. Talbott carries out his *NetFuture* discussion group using low-technology electronic mail.

Sale might dislike the term "anti-technologist" applied to him as too simple a label, but he would probably welcome the "Luddite" label, since he makes clear that Luddism (and the "neo-Luddites") are

not against all technology, but only against "technology … malevolent to the user, to the community around, to the culture, to the environment, to the future." Similarly, Talbott might also dislike the "anti-technologist" label, since it would be applied to a thoughtful man who *questions* the use of computer technology, who asks for an accounting. Fox might even welcome such a label, since he welcomes words like "radical" and "post-denominational" for his work as a priest.

The anti-technology movement is far larger and stronger than these four men might indicate. Worldwide, the fundamentalist religious movements are a fertile source of anti-technologists. Fundamentalist Christians in the U.S. are particularly strong, and their reliance on biblical literalism (the belief that every word of the canonical Christian Bible is literally true) leaves them completely at odds with most of modern science, though they dispute this assertion.

The transition to the next millennium, and the associated year 2000 problem, both loom very close now. There may be significant problems in the time running up to January 1, 2000 and in the months afterwards—economic and social problems, problems with technology, and especially problems with *computers*. These problems could lead to an anti-technology backlash.

Finally, there is a vocal group within the U.S. who would resist the technological support for crime reduction that this book discusses. These people are not exactly anti-technologists, but they certainly do not want technology monitoring their public activities or controlling their use of guns, and a program like national identification is unacceptable to them.

Justification.

Each of the four individuals mentioned in the previous section, Kaczynski, Sale, Talbott, and Fox, whether or not one calls them anti-technologists, represents a challenge to the author of a book about using computer technology—a challenge to justify this use. Even Kaczynski's writing deserves a response, but Fox's arguments are the most difficult to answer, since for Fox a great paradigm shift is now replacing the old "Machine Era" with a new "Green (or Sheen) Era."

I can think of four justifications for the continued use of computer technology in the face of these attacks. First, technology, and in particular computer technology, is needed to prevent a complete societal collapse. A primitive anti-technologist like Kaczynski wants society to abandon all technology, especially the computers—to return to a simple pre-industrial life style. But such a change would require a population reduction to a small fraction of the current level and would impose the most horrible hardships on the bulk of humanity. Society cannot go back; it must embrace much of the new technology or die. In fact, many new high-technology solutions have led to the abandonment of the lower-technology infrastructure, so that the old approaches are no longer possible. Most printing and publishing, for example, has become completely computerized, with no chance of returning to the old ways. And those who romanticize the pre-industrial, pre-technology times may not know of the great inequities in such eras, or even in the later American "Wild West."

Second, technology currently helps individuals get health, happiness, and security in many ways, large and small. Who would eliminate dentists in anti-technology zeal? Even Kaczynski used a bicycle and a typewriter. Who would want to type manuscripts with a carbon copy or to run a modern business with no computers? Much of modern technology, from power to communications to transportation, is now computer controlled.

Third, in the short term computers promise many improvements, particularly in applications where society develops good approaches to computer-mediated problem solutions. Computer technology holds out a long-term potential to transform lives completely, to give benefits now scarcely imagined. Society has only fifty years of experience with these machines; they are barely starting to come into their own. Hans Moravec, in his books *Mind Children* and *Robot*, speculates about a possible far future of mankind where machines would transform human beings into a new form of life.

The fourth and final justification is the most important. One does not need to choose between machine and green. In fact, because of all the world's problems, society will need the machines if it hopes to reach the green era. But many of the fruits of technology must

change. Picture a copper-smelting plant near the downtown area of a large city and next to a university, a smelter belching hundreds of tons of sulfur dioxide and other toxins into the air each day, choking nearby students, and laying down heavy metals to be ingested by the children of workers living at the smelter's foot; picture a blight on a large part of the city. Few would be enthusiastic about such an enterprise. It is reasonable to take a stand against much of technology, against many of the effects of industrialization. And the misuse of computer technology is of great concern. However, the answer is not to get rid of the computers; the answer lies in better utilization of these machines—use them to monitor all technology, to protect against abuse, to supply all of society with open information about technology use and abuse.

What to Do.

Analysts like to put forward *answers*, a single technique to solve humanity's problems. There is an alphabet soup of one-theory-for-everything answers. A is for abolitionism (or maybe absolutism or Anglicanism or atheism), B for Buddhism (or barbarism or Bolshevism), C stands for creationism (or perhaps Catholicism or Confucianism or conservatism), D for Darwinism (not to mention neo- and post-Darwinism), and so on to Z for Zionism or Zoroastrianism. It is no surprise that human beings want simple answers, single answers, but there are no simple, no single answers. Humanity needs different answers for different peoples, different regions, different times, different problems. Individuals as well as societies need to develop their own answers.

People also want the immediate solution, the quick fix. But quick solutions do not work well. Only the slow ways are effective. I meet naive computer students who want to learn to program, quickly—skip the unnecessary stuff, just get to the heart of it and not waste time. Programming skill takes time, though—an accumulation of techniques, learning from mistakes. In two plays by the German poet Goethe, a man named Faust resolves to change the world, seize knowledge, make a difference all by himself. The second play has an unformed man-like creature living in a bottle, the *homunculus*, who

wants to "become," to create himself. He finally decides to leap into the sea, to take the "slow" way. (And this was written half a century before Darwin.)

Physicians treating appendicitis know that they are not operating frequently enough unless half the appendixes are healthy, since diagnosis is difficult. You must make mistakes in life. Not just experiment and simulate, but *make mistakes*. Civilizations should take chances and make mistakes. John von Neumann, arguably the father of the modern computer age, urged society to push to the limit now and then, one time in a hundred. And individuals, nations, even whole civilizations must make their own mistakes. One can avoid many mistakes with study, simulation, and planning, but one is not experimenting enough if there are no mistakes.

A recent book by Edward Tenner reminds again that introducing technological solutions to problems may create new problems. The book's title is *Why Things Bite Back: Technology and the Revenge of Unintended Consequences,* and it uses examples to strike the right cautionary note without suggesting that society abandon technology. To avoid what he call "revenge effects," that is, effects seemingly designed by a malevolent and vindictive universe, Tenner suggests the "substitution of cunning for the frontal attack." Moreover, Tenner has my own passion for keeping track of all events and objects in the world:

> Technological optimism means in practice the ability to recognize bad surprises early enough to do something about them. And that demands constant monitoring of the globe, for everything from changes in mean temperatures and particulates to traffic in bacteria and viruses. It also requires a second level of vigilance at increasingly porous national borders against the world exchange of problems. But vigilance does not end there. It is everywhere.

The same interest in tracking events in the physical world extends to the data mining now carried out in the electronic realm, where agents will sift through the World Wide Web looking for evidence of terrorism or other wrongdoing.

Here is a list of activities to pursue in the future. The list takes Tenner's revenge effects into consideration, with the assumption that experiments may fail, that actions may give unexpected, even undesirable, results.

Openness, free speech, privacy: The foundations of this book, these proposals differ from those of other people in a desire to keep track of events in public, and to keep track of objects, especially objects that are valuable or dangerous. The tracking should be centralized and coordinated across the world, but with part of the information available only under court order. How else but by tracking will society know what the crazy people out there are doing? The alternative is to pay no attention.

Long-term planning, long-term goals, simulation, education: These are secondary goals of this book. Society cannot justify the current lack of planning, drifting where the wind dictates. The world is heading toward horrible and intractable problems, with too little thought of what is to be done or who might do it. Powerful simulation tools let one visualize many futures, to avoid obvious mistakes, to discover subtle possibilities. Computers and sensors, combined with surveillance and fingerprinting, can help keep track of the world so that planning is facilitated.

Traditional solutions: One should take advantage of old-fashioned methods that work. While effective "behavioral engineering" would be welcome, just as important are the traditional influences of family and friends, schools and teachers, places of worship and other community organizations.

Experiments, mistakes, risks: This is the opposite of using traditional approaches. Fruitful activities are too complex to simulate fully, so society must experiment boldly, and with this experimentation comes the chance of failure. Society must also not overemphasis security or the avoidance of risks. Francis Fukuyama's book mentioned in an earlier section predicts a future fate of mankind as Nietzsche's "last men": people obsessed with security and comfort, but devoid of ambition, lacking any higher purpose. That would be a bleak future for humanity.

The Future of Society.

I am at the end of a book on the use of computer technology in partial support of surveillance and control, to make crime impossible, and I maintain, as I have earlier, that society must move beyond this technology, that it must move beyond gadgets that keep people from carrying out the crimes they would like to commit. This may sound unusual or even contradictory in a book about technology, but the gadgets are for humankind's present crisis, for society's journey into the future, not for the final destination.

From the beginning I have insisted that openness of access to information is the key to society's future. Computers will support such open access in ways still imperfectly appreciated. Society stands at the *start* of the information revolution, not the middle or the end.

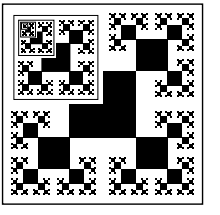
A hint of the world to come is revealed by the constraints that openness even now lays down upon people and companies and governments who would commit crimes—crimes against individuals or groups, or against humanity or the earth itself. From across the globe, the public can discern better than ever before what is happening, the good and the bad—and the crimes. Recent years have seen thousands of cases where a government, a company, or even an individual could not cover up a crime, where the laser-bright light of open access illuminated the activities and inhibited them—made those responsible fear for their own accountability. As just one example, Americans are now discovering the full extent of the deceptions by tobacco companies in pursuing profits, in pushing to sell to young people, in expanding into foreign markets, all the while knowing how addictive and harmful their products are.

Access to information about actions by the government, whether trials or meetings or law making, has always been and remains a cornerstone upholding the U.S. democracy. Imagine this access improved in the U.S. and extended worldwide—and including public actions by individuals and corporations. I foresee a future with the next level of open democracy, its detailed nature still unimagined. I foresee a future with an open global community. This can be humanity's future, a future where crime is impossible because the crime and

the criminal would immediately be revealed to everyone—and eventually because people have less need or desire to commit crimes.

WALDEN 3.0

Fiction



Contents[1]

Walden 3.0
(Fiction)

[1] Here is a fictional account of a small American town using technology described in the non-fiction part of the book. In fact, the town jokingly refers to itself as "Walden Three," after B.F. Skinner's novel *Walden Two*.

Topics in each chapter of the fiction correspond to those in the chapter with the same number in the non-fiction part. The page of each matching non-fiction chapter appears in parentheses at the right above.

Prologue

Sunday evening, March 22

From nearly a kilometer up, a bird's-eye view, the town was a spread of lights in the growing darkness—lights like Christmas strands along major roads, scattered points in residential areas—a typical smaller American town resting in the cool, still evening, bright stars overhead. Slowly the floating viewpoint shifted down to half a kilometer above. A dark river marked the eastern boundary, with lights along a highway spanning it. Barely visible railway tracks followed the west edge of the river; a freeway ran north and south a kilometer or so to the east, well outside the town proper, but a blaze of lights showed a satellite of development where the freeway met the road into town. The focus dropped further: to a quarter kilometer—then lower yet. This was Everytown, a stereotype of such places—cars, gas stations, grocery stores, a strip shopping center, bars, what looked like a college—nothing unusual, nothing special. The viewpoint purposefully moved west over the town to a range of cliffs and low hills on the western border. Down to fifty meters—still well above the tree tops. A camera lens adjusted, and the view zeroed in on strange silhouettes moving from bush to bush, hard for a person to see, but clear to the camera's CCD enhanced sensors. As three men reached the top of a hill and paused, the camera could resolve details of facial features. Two of the men carried tools; the other had a handgun ready.

One figure jerked away from shrubbery. A directional microphone picked up his voice. "Dammit, there are thorns here."

"Quiet!" whispered another figure. "And go slow—nothing sudden. You're almost to the camera I found two days ago. Up ahead and on the right, in that tall maple tree."

The lead figure, shorter than his two companions, awkwardly pulled himself into the tree and slipped a sack over the camera.

"Not much time now." He followed a wire from the tree into the ground. Frantic digging with collapsible army shovels uncovered a metal box.

"We're in luck. I would guess this is a relay station for cameras on the west side. We'll cut the wires and destroy this box. Get ready now. With a broken circuit they may send someone right away."

Another figure spat at the base of a tree. "I'm not scared. We've got their cameras spotted now, and we know which are fakes. Just go around them and take them out—it's easy. But when do we get our money. Tell Hoffmann to get out his checkbook."

"You're not to mention that name, or there may be no checkbook."

The third figure put in, "A fat checkbook—that weasel would push drugs to his sister if there was money in it."

At a gesture, one man cut several wires, while the third wrenched open the box with a crowbar. He jabbed the crowbar viciously into the electronic innards several times.

The leader remained calm, matter-of-fact, running his hand through close-cropped hair. "That's not repairable. Now make tracks, boys. You know the plan. And when we get to Mama Blue's, don't just sit together in a booth. Mingle, or nobody will remember us. Make people think we've been there all night."

"What about this damn crowbar? And the shovels?"

"Give them here," the leader said. "I'll stash them along the way to pick up later."

The three men half-slid, half-lowered themselves down a gully to a path. They jogged along the path and at its end dispersed in three directions.

Unseen and unsuspected over them hung a curious shape, partly hidden by trees. Three meters long and painted flat black, it drifted in the direction of one figure on the ground, with a hum of tiny fans and a whir of adjusting cameras, both apparently too faint to hear below. As the shape neared a road, it resolved against the sky into a blimp, some gas-filled balloon, like a child's remote-controlled toy.

Elsewhere, several men stared at two monitor screens showing scenery below the blimp. Too open, too exposed, they decided. After a brief discussion of the recorded voiceprints, they sent commands to discontinue this surveillance. The fans worked hard, turning the blimp from the figure below. Hanging video cameras retracted to a long-range view as the blimp headed after other prey that night.

1. Arrival

Sunday evening, March 22

Martin Davis was late getting to Ralph's house, driving too fast even for light Sunday traffic. He'd come 45 miles north from the nearest good air connection and had intended to arrive before dark, but the freeway was full of potholes made worst by a spring freeze. The cool air through an open window was a relief on his face. Finally a sign appeared: "Welcome to Rockcliff, Home of the Raccoons, Population 34,000." The highway continued north along a river, while an arrow pointed to an off-ramp and underpass for the town toward the west. He headed west over the river using an old-fashioned bridge and saw the last pale glow where the sun had set. The road went under north-south railroad tracks before entering the town. Ralph had sent a hand-drawn map. Three turns and he was in the driveway. The house stood off by itself, in the midst of evergreen trees. He crossed the lawn, missing the sidewalk in the dark, but found a faintly lit doorbell. The hallway light came on at once, a huge man threw open the door, and his friend Ralph Barnes gripped him in a bear hug.

"Martin, I'm so glad you're here." Ralph held him at arm's length. "How long has it been?"

He struggled free. "How long should it be? Five years, I think." Ralph looked older than Martin had remembered, his light-brown hair thinning on the top now. He'd always been large, but was larger yet, just shy of overweight—making a contrast with Martin. Ralph wore his standard khaki pants and white shirt. It was like a uniform; Martin had never seen him dressed any other way.

"Where's your luggage?" Ralph said as he ushered Martin into an entryway.

"In the car, where else? That and my little portable computer. I should have left it home; I've been paranoid about someone stealing it."

"It's probably safe now." Ralph backed up a step. "But let me get a good look at you. You're haven't changed at all. How do you keep from putting on weight?"

"It's the hectic life I lead, traveling so much."

They moved into the living room. "How about a drink? Cognac?"

"Sure." Ralph poured two small liqueur glasses, while Martin looked around. The room was stark, with simple furniture and bare white walls. Through a doorway he could see several computers on tables. He downed half his glass, then gasped.

"You're supposed to sip it," said Ralph.

Martin got back his breath and resolved to say what was required. He had steeled himself for this moment, but it was still hard when the time came. "Ralph, I just wanted to say how sorry I was about your daughter, little Kelsey. I didn't hear about her for six months, and then I never wrote like I should have." Ralph's daughter had died in a wreck with a drunk driver when she was a year old, but Martin didn't know any details.

Ralph's distress was plain to see. "I don't think about it much anymore. So long ago, nearly four years now—just part of life. The drunk who killed her did go to jail, but he may be out now. I don't even remember his name; I don't want to know it."

There was a long pause—Martin was not going to touch this subject again, but Ralph went on: "Did you know that I later divorced? Janet and I didn't have a strong marriage, and this was too much. She—she couldn't get over it—just sitting around staring at the wall, and I was no help to her. She's doing better now—remarried even."

Martin finished his cognac and decided to bring up a new topic. "Tell me, where's the fancy security system you bragged about. Everything and everybody looks asleep. I expected at least one checkpoint."

Ralph finished his drink, too. "It's a lot more subtle than that. Tomorrow I'll show you the log entries of your arrival. Parts of them anyway. I hope you weren't put off by my suggesting business *and*

pleasure with this trip. As I mentioned, we can pay you a small consultant's fee, but no big hourly rate."

"The pay isn't important, and besides, you'll get what you pay for. I'm no detective; I've never chased down any criminals. But the problem does sound interesting. If I understand it, you have a security breach, and you think it's an inside job."

"Someone leaked confidential health data to the newspaper and has spread misinformation using flyers he prints himself. It's about local issues and complaints, so very likely someone in the town is doing this. An outside hacker wouldn't care about this data. The data is protected, which indicates computer skills—not so common around here. That's why I thought of you: set a hacker to catch a hacker. I remember when *someone* crashed the whole campus network."

"Yeah, and *someone else* kept them from expelling the someone. I haven't forgotten your help."

Ralph smiled indulgently. "You didn't mean any harm—just playing games with your hacking—the best student of a young faculty member. I wanted to keep you around."

"Well, I managed to turn my hacking hobby into a profession. But what's so sensitive about your leaked health information? Why would someone bother with it? Does the town government have any secrets?"

"I started to explain on the phone, and I'll give you more detail tomorrow, but in brief we've been using computers to prevent crime and improve security for the town's citizens. A few of these citizens don't like our approach—they say we're taking away their 'freedom.' The leaks are meant to embarrass those of us running the town, to discredit our policies."

"And are you embarrassed? Can you defend your policies? Do they deserve to be discredited?"

"Of course they don't, I mean I can—of course I can defend our policies. I'll be showing you what we've accomplished in this town in just three years. It's impressive. I'm proud of it."

"I still don't understand the problem," Martin said.

Ralph explained that there was leaked data about individuals, data he himself couldn't access without subverting the controls. "Whoever

this is," Ralph said, "he's making it sound like we're misusing confidential data, when we're not. It's a bigger deal than you might think. You see, we consolidated the town's health records. All sorts of advantages, but people are worried about confidentiality. Then these leaks came along. We even held a town meeting about the issue. I saved one of the hacker's messages for you to examine." Ralph got up to fetch a bright yellow sheet from a table in the small dining room.

Large letters at the sheet's top shrieked in headline form: "Rockcliff Invades Privacy, Shuts Down Freedom!" Martin read through the rest, a tirade against the surveillance used by the town. The pamphlet went on, "Do you really want constant monitoring of your personal and private activities?" At the end it revealed details about the health records of four local people, one of them Ralph himself.

"Ralph, I didn't know you had high cholesterol levels."

"That's bad enough," Ralph said, "but at least the hacker has avoided truly sensitive data, like sexually-transmitted diseases."

"You don't mean … ," Martin started.

"No, no, not *me*," said Ralph indignantly. "I just meant that he hadn't destroyed any careers, as he likely could have done."

"So you want me to install traps, snoopers, that kind of stuff," Martin said.

"Exactly. I hope you brought the software we talked about."

"I brought some software. I can fetch the rest over the net. But right now I need a toilet." Ralph directed him down the hall. Above the commode was a neatly-lettered sign: *To operate this device, please follow these simple instructions: 1. Pull chain gently, but firmly. 2. Hold down for exactly 5 seconds. 3. Then release. Thanx. –The management.*

Back in the living room, Martin sat down on a short couch. A gray cat jumped into his lap, and he started idly petting it. "Cheeky cat here, but they all are. OK, can you give me more of an overview, more background about this town? How did you get started working here? With your credentials, your Ph.D., I expected you in a fancier position." Martin thought maybe he was going too far. "Uh, sorry. I'm not even sure *what* your position is."

Ralph leaned back with his feet on a cushion. "No apology

needed. I know this is a small town. But not a hick town—that's a big difference. I'm in charge of data processing for the city. It's a unique situation, because I work closely with the Police Chief—Rollins is his name. Paul Jordan under me handles the payroll and routine matters. It was just a lucky break that I interviewed for the job. A friend from college, Becky Phillips, referred me, but I didn't see how far they wanted to go till the interview."

"And who are 'they'?" Martin said.

"The City Manager, the Mayor, the Police Chief, two councilmen, two other influential citizens, and my friend Becky, who is still working here as an education consultant. They interviewed me as a group. They had rough high-tech plans, rough ideas of what they wanted. But *I* put it all together—well, with help from Becky. I know this may sound silly, but some ten years ago a phrase came up in a course. I don't remember the course, who said the phrase, or how the discussion proceeded, but that one short phrase is burned into my brain, like non-erasable memory. Whoever it was, student or professor, said this: 'What if crime were impossible?' All through graduate school I couldn't let it go. What if we could arrange our technical society so that crimes were physically impossible? I thought of all sorts of ways one could take a crime and just make that crime into an impossible event, a non-crime. With no crime there's no search for a criminal, no incarceration, no trial, no punishment. The city manager actually had much less in mind, but he and the others got excited along with me at the interview."

Martin thought the idea of impossible crime sounded typical for his friend—always chasing some obscure, elusive goal. "I hate to rain on your picnic, but are you going to make it impossible for me to pull out a gun and kill you right here?"

"Of course not, though mind you, we could do that sometime if we wanted to. We can't make all crimes impossible, but we can get rid of many, and we can fix it so people get caught for most of the others. Don't misunderstand, we use the old methods here too: police on bicycles, for example, and dogs. But even there we have high-tech bicycles with computer links. And the dogs have computerized collars to give their position. Are you a science fiction fan?"

"Not a fan, but I've read some. Why?"

"Do you remember van Vogt and his 'Weapon Shops'?"

"Sure," Martin said. "He put guns in his books that could only be used in self-defense. I see where you're heading. I enjoyed the books, but the ideas behind them were far-fetched—not remotely reasonable."

"I agree, but I think we can get the same results. All the mechanical widgits around us are getting more complicated and more computerized, more intelligent. You name it—from VCRs to washing machines. We should be able to keep tighter control over just what can be done with them. Fix them so they only work where we want, and how we want."

"Hold it," Martin said. "Who's the 'we' here? An elite deciding for the rest of 'us'?"

"Why, there's no special 'we' in this case. Companies will manufacture electronic goods that won't work when stolen, and consumers may elect to buy them, if they think the crime-proof features are worthwhile. Then you could stop worrying about your laptop being stolen.

"But it'll take more than one chat to tell you what we're doing," Ralph continued, "and you look tired right now. Tomorrow I'll show you our setup."

Ralph led the way to a spare bedroom. After a few explanations, towels and blankets placed on the bed, Martin settled down alone. No matter how tired, he always had trouble falling asleep in a new setting. He mulled over what Ralph had said. Even if society could make crime impossible, should it really do so? A "Do Not Pick the Flowers" sign—you bend to pick one anyway and get a violent electric shock. What manner of world would that be? It sounded like slavery, total control. But should you let people pick flowers if they're not supposed to? Maybe you could let them pick a flower and make them pay a fine later. Maybe you could keep them away from the flowers. He slept restlessly. All night long, it seemed, shadowy individuals in dreams watched him, told him what to do, told him where to go.

2. Monitor Traffic

Monday morning, March 23

A lone car drove into town through light mid-morning rain. In Ralph Barnes's office at City Hall, Ralph stared with his friend, Martin Davis, at a yellow icon of a car moving on a glowing computer map of part of the city.

Even without a good night's sleep, Martin had gotten up for his usual three-mile run, only to confront a dreary, cold morning. He gave up the run after fifteen minutes when it started to sprinkle. At least he'd seen part of the town—so small, so many trees, so rustic—houses spread so far apart. On returning to the house Martin found a redbird in formal combat with his rental car—flying to the outside mirror, attacking, retreating. He and Ralph had finished coffee and doughnuts while they drove the short way to the new four-story city building. Now they were in Ralph's cluttered office, where Ralph was showing off the town's vehicle tracking system.

"We had one heck of a time getting all this in place, I can tell you." Ralph pointed to the screen. "You see that car? It would have gone through several sensors if it stayed on the main highway and skirted the town—we even track cars that bypass us. For those coming in, we blocked and rerouted roads so that there aren't many ways to get in or out. Key roads have speed bumps on them—hardly noticeable at 20 miles per hour and tolerable at 30, but terrible to go through at 50. The sensors get the license plate number as well as the speed and the other data. See the tick mark there? That means the state site is searching for the number right now. No answer yet. We also have the car's weight, an image of the driver, a silhouette of the car, and the paint color. See there on the screen?"

"You mean you have software that retrieves the plate number from a digitized image?" Martin was impressed. "I figured you would just get a picture and read the number by hand. How do you do it? And what's your error rate?"

"The error rate is less than five percent for the first scan even in rain like this. But we get later scans that reduce it below two percent. Most of the rest are covered with mud, or missing, or maybe pulling a trailer. For those we get the number by hand from the image or even by going to the car.

"This is state-of-the-art stuff," Ralph continued. "Few local communities have it. Video cameras grab the image, and the software first assumes the plate comes from this state. If that doesn't work, we compare the plate with stored images of plates of all other states, along with Mexico and Canada. Keeping up with new plate designs is a bother, though, and after that comes the hard part of determining the number."

The yellow car stopped, then jumped to a new position. "What happened there?" Martin asked. "It's hopping like a rabbit."

"The software keeps a probability distribution for the car's location, like quantum probabilities for the location of a particle. The screen is showing the last-known certain location given by an actual sensor reading."

"How many sensors do you have?"

"A whole lot of them," said Ralph. "I shouldn't tell you just where or how many, but we use traffic lights when we can—up to four cameras perched above a light. Then we installed decoys for the boys to shoot at."

"Decoys?"

"Yeah, that was my idea. I thought some of the locals would try to knock out our cameras. So we made a big deal about putting up these iron boxes—a target for them to shoot. The real cameras we put up quietly at night or by pretending to repair traffic signals. The locals just filled those empty boxes with lead, and we picked up most of the good old boys who were liable to try for a camera. I thought things had settled down, but there are still problems. We lost equipment on the west side just last night, and I'm afraid it's not an

isolated incident." He interrupted himself. "There, the ID on the car just came in."

"Who is it? Where is the driver from?"

"That's not on the screen," he said. "It's logged into the system, but it takes a court order, or at least strong probable cause, for me or a police officer to fetch the information. And I can't prevent a log of the fetch itself. They audit once a month and they're real fussy. Now watch—he's stopped for gas."

"OK," Martin said. "But why are some cars green and some yellow?"

"The green ones are locals who volunteered to put a special transponder on their car. We're up to seventy-eight percent now. We talked them into it using the auto theft angle."

"Sure, you 'talked them into it'—with a gun to their head. At the very least it sounds like manipulation without full disclosure."

"I don't see it that way," said Ralph. "They know that we'll be able to track their car, and they don't care. There's nothing else to disclose."

"What about the other cars?" said Martin.

"Oh, we can track them pretty well, too. Look. The car we've been following has finished getting gas, and it'll go over another weight sensor. See, now we can tell how much gas the car took on."

Martin shifted in his chair. "That's almost scary. What if someone wanted to come here and dump a body, or toxic waste?"

"I wouldn't recommend it. After we found the body or the waste or whatever, a court order would let us pinpoint the car and driver right away. The software might notice the actual dumping and call our attention to it, or if they acted suspiciously, we could even flush them out as they did it." Ralph started to get wound up. "There's a lot more going on than you see from this display. We're using military software that we adapted. And surplus military hardware, including special infrared and CCD scanners. The software keeps track of every car, and we almost never mistake one car for another. It's one of those knowledge-bases, with deductions about the cargo and passengers—where they were dropped off or where picked up, based on weight. It's got fuzzy logic built in, and special rules that fit our application.

Most of the locals don't realize the system's full extent. Outsiders never know how closely we track them."

Martin was more concerned than he was letting on. Where did freedom come into all this? "I don't like that at all. Close surveillance, and you admit people don't know all the implications. Shouldn't people be free to go where they want?"

"They *are* free to travel as they like. We're not getting anything that we couldn't have gotten the old way by following a car around. Well, maybe the weight. Mostly now we're just doing a better job—not missing a tick."

"But you know everything about each car in town? An innocent tourist comes in and you know everything about him? I don't like it. I can see you guys now: 'There, he stopped to pee beside the road, and ran over Mrs. Whats-her-name's trash can.' I don't like it."

"*I* don't know everything about the cars," Ralph said in defense of his system. "It's just logged into the computer. It takes a *crime* or at least good suspicion of a crime to get the data out. Since we got fully operational, we've had *no* cars stolen that weren't recovered. We used to have wild driving by young people, and they've calmed down. Much of the semi-wild driving we tolerate. Our drunk-driving problem has gone way down. We pick them up right away from the weaving, before they kill anybody. There are good people out there alive now who would be dead without this system. And we mostly don't have to deal with a big-time trial for a drunk killing someone. Instead they sober up overnight in jail or get probation for DWI.

" 'Driving while intoxicated,' " Ralph explained further. "I think you call it DUI in California, 'driving under the influence.' "

Martin didn't say anything, and Ralph went on more soberly. "I know what you're thinking; I can tell by your look—that I'm not objective about the issue of drunk driving because my daughter was killed by a drunk. It may influence me. But Kelsey's seatbelt wasn't properly fastened to her car seat, so maybe we were partly at fault. I don't know. I will say this: People get much more law-and-order oriented if they suffer a personal tragedy. They worry a lot less about intrusion and loss of privacy, and think more about security."

Ralph's phone rang abruptly. The ensuing conversation was

obscure—talk of replacing, rerouting, using wireless connections. Martin looked for something to hold his attention in a large office filled with technical books, manuals, even hardware components—on bookshelves, chairs, on the floor. Martin was browsing through a book on networking when the call finally ended.

"That was Steve Ribak, my best hardware technician. He's repairing broken lines on the town's west side. But where were we?"

Martin tossed his book back on the floor. "Intrusion. We were talking about how intrusive your system is."

"Intrusion means to interfere with someone, to force yourself on them. We're not bothering them. We're just keeping track of their *outside* movements the same way a nosy neighbor might. We're not peeking inside their houses. We're not listening to their conversations, not even on the phone. We're not recording these conversations. I've often wondered what people are so worried about. What are they planning that might be compromised if we can later fish out where their car was? Are they having an affair? We'd just never let on where they'd been, even if we found it out, unless there was a crime at the same time. And then the affair would likely come out without our monitoring. Do these good old boys think it's their *right* to break the law selectively?"

"Calm down," Martin said. "As you admitted, you'd intrude if they did something you disapproved of. Anyway, I'm not the one you need to convince, but the townspeople, and I guess you did that, except maybe for your hacker who's leaking data."

"No, we didn't convince everyone. There's still a lot of hostility from a few folks—a minority, but a vocal one, and with many different views. Our opponents could never agree with one another, except for hating our efforts. All the resistance has been frustrating—there's no appeasing these people."

"What are they hostile about? Maybe they have a legitimate concern. Maybe you should ease up in that area."

"Oh, different people are upset about different issues. Townspeople complained from the start about 'loss of freedom,' about 'invasion of privacy.' I expected that, and I expected potshots at our cameras. Lately, though, events have taken an ominous turn. A hard-core of

militants has been destroying equipment. We lost cameras and a relay box last night. That phone call was about repairing them. This group has gone out armed, and so far we've avoided a confrontation, even though we usually know where they are. We don't want anyone killed." Ralph paused, then went on. "On a bad day this bothers me. We're trying to eliminate crime, but in some cases our tactics seem to be *creating* crime, inspiring a few to commit crimes." Another pause. "One person has been particularly disturbing. Patrick Hoffmann—as nasty as his German-Irish name sounds. He owns a good-sized chunk of the town, and his intrigues and schemes reach everywhere."

"Could he be your hacker?" Martin asked.

"Well, probably not by himself. Hoffmann's an old man now, and wouldn't know the latest computer techniques. But he might be working with someone. That's his style—to get others to do his dirty work. He likes to talk people into filing lawsuits against his 'enemies.' I wouldn't put anything past him. I'm convinced he once had someone deliberately crash into the car of another enemy. They paid for the damage, but the enemy was so preoccupied with the wreck that he was distracted from his opposition. It was an effective strategy. There have also been rumors about Hoffmann carrying on affairs. And I have, um, personal reasons to dislike him; I'll tell you sometime. I think he's scared the surveillance could uncover his own activities.

"Ideological opposition has continued as well," Ralph continued. "Now more pointed, more refined, especially from one other thorn in our side—the 'Reverend' Bob Laherty. I call the pair of them, Laherty and Hoffmann, our 'pusillanimous preacher and publisher.' "

"What does 'pusillanimous' mean?"

"Full of pus," Ralph said with a straight face. "Don't get me going about them. You see, Hoffmann owns the town's newspaper, and he often prints a column by Laherty, who's a minister in a local fundamentalist group. In one column, Laherty started calling this place 'Walden Three,' and others picked up on it as a nickname. They even posted a 'Walden Three' sign outside town, along with a backwards swastika. Ignorant scum—they don't even know how to draw a proper swastika. Myself, I take the name as a compliment."

"I don't understand. 'Walden'—that was Thoreau's pond?"

"Yeah," said Ralph. "And his book. But later a psychologist named Skinner wrote a book called *Walden Two.* "

"I sort of remember that, but I don't think I ever read it."

"Well, it's about one of these utopian societies. I did read it after the fuss, and I see similarities. Skinner wanted to control people's behavior—to make crime impossible that way, I guess. In Skinner's little Walden Two community, everyone was happy because they were conditioned to be that way. He had some weird ideas, but I thought the book made a fair amount of sense, though I didn't think all the ideas would work. Much of what we tried didn't work the first time either, or didn't work at all. Since then I've read other Skinner books. There was even an article about Walden-type communities, where they tried to put these ideas into practice."

"And why did they draw a swastika?" Martin asked.

"They're claiming the town's now a Nazi concentration camp. What rot." Ralph started to dig beside his desk. "I've got a copy of Skinner's *Walden Two* book here somewhere, or if not here, at home. Want to borrow it?"

"Sure, I'll look at it tonight."

3. Identify People

Tuesday noon, March 24

The next day, Ralph Barnes and Martin Davis were finishing lunch at a downtown "homestyle" restaurant. They sat at a quiet table toward the rear of a long, narrow dining area with a tiny kitchen at the back. Martin had eaten chicken fried steak.

"It tastes OK, but they shouldn't call it 'chicken,' " he said.

Ralph looked up with astonishment. "It's *prepared* like fried chicken. Have you been living off-planet?"

Ralph, never one to pass up food, ordered a piece of apple pie for dessert. Martin watched in fascination as the waitress measured and then carefully cut a fresh pie into seven equal pieces.

"Did you see that?" Martin said. "Seven pieces, all the same. That's hard to do."

"Sure. Clair always cuts sevens."

"Why? Is that a Walden Three specialty? Evidence of a superior civilization?"

"Hardly," said Ralph. "I asked her once. They look the size of a sixth of a pie, but she can sell one more piece."

"Ah-ha. A crime," said Martin. "Cheating customers who think they're getting a sixth. Just wait—you'll all get your just deserts."

Ralph winced, but before he could answer, a woman and teenage boy walked to their table. Ralph stood up for them abruptly, with Martin belatedly rising also. Ralph seemed awkward, almost embarrassed, in introducing her as "my friend, Susan Pierce, and her son, Kevin." Ralph continued with an introduction of his "former student, Martin Davis, from San Francisco."

Ralph convinced Susan and her son to sit down even though he and Martin were clearly almost finished with lunch. Susan was short,

with brownish-red hair and a pale complexion. Martin wondered if Ralph had anything going with her. Martin didn't think her very attractive, and she seemed old for Ralph—then he felt the opinion was unworthy of him—it was Ralph's business, after all.

The boy was thin and small, perhaps fourteen or fifteen. His jeans and tee shirt were topped off with glasses and curly black hair, a narrow, prominent nose, the face drawn and serious—Martin thought it looked like a suffering poet's face.

When Susan asked what he did in San Francisco, Martin replied that he went for long walks along the beach, attended plays, and then more responsively said that he worked with computers. "Consulting work with various companies—network and access problems, security problems."

Martin tried to engage the boy Kevin in conversation, with limited success, and Ralph had to take up Kevin's cause himself: "Kevin's good at everything academic—a good writer and a clever computer user. Tell Martin about your work with the library's web page."

Kevin reluctantly described how he had created a library homepage. Martin understood his reticence; the server was already there—it was just a bit of simple HTML programming, though he had managed to put a hook into the card catalog.

Ralph had long since finished his pie, and he decided they should leave the newcomers to their lunch. There were still subtle tensions as the two of them left after saying good by.

It was just a short way to Ralph's office, diagonally across the street to City Hall. As they walked, Ralph evidently felt an explanation was needed. He told Martin that Susan Pierce was a single parent, divorced long ago, and that he had been seeing her "off and on." Kevin lived with his mother, though he spent some holidays and a month or so during the summer with his father in Seattle. "Susan's had a rough time," Ralph said. "When I got here, she was finishing a nursing degree part-time and was working at Patrick Hoffmann's car dealership. You know, the guy I talked about, the sty in my eye. He subjected her to the most amazing abuse—emotional and physical—even following her around at night, lurking outside her apartment, phoning late to see where she was. I was worried for my own safety,

as well as her's."

Martin wondered about the topics Ralph had left untouched. Kevin seemed either shy or resentful, maybe both, trying to get along with Ralph, his mother's friend—and Ralph could be so dogmatic and authoritarian—not easy to deal with in the role of unofficial stepfather. Also, Ralph's story about Hoffmann was so incomplete. Had there been a simple rivalry of two men for the same woman? Or something deeper? The questions would have to wait for now.

At his office, Ralph threw himself down in the chair. "I'm really tired. I let you sleep last night, but I had to get up to restore the system. Took two hours. Those deputies don't know how to be ordinary law officers any more. They go crazy without their computers. Luckily we don't have a crash very often, and I can repair and reboot from home. I'm real proud of setting it up so I don't have to physically go to the computer to restart."

"What about the town's data logging—all your surveillance data—during the down time?" Martin asked.

"Those computers didn't go down. But if one had and the data logs were missing, the software would synchronize with reality quickly—in hours or days everything would be located again."

Martin was sitting beside a window on the second floor of City Hall. Cars went back and forth below, evidently followed by software, carefully identified and kept track of. He didn't like the idea of so much surveillance, but it wasn't worth an argument with Ralph. "And who pays for all this?" He'd wanted to ask that from the start.

"It's not as expensive as you might think. We've used secondhand equipment—some of it military surplus—and a lot of free software, not to mention volunteers who help. The town is financially healthy, and finally, we *are* on a tight budget."

Ralph cleared his throat. "Martin, I want to log you into the system so the town knows who you are. We don't usually do this with tourists, but you'll be in out-of-the-way places with me, and it'll be easier with your ID on file."

"You want my fingerprints?" Martin moved to a seat opposite the desk. "I've been fingerprinted by the feds, of course—you knew I did classified work—but never by a civilian agency."

"Nah," said Ralph. "We don't use fingerprints here in the city. If someone leaves a fingerprint at a crime scene, or if there's a booking, we send the print out for state and federal searches, but otherwise no prints."

"Now that I think about it, I've never heard of a city with its own ID system. What do you use? And how do you get away with it?"

"The climate's gotten easier with tort reform, and we get by because our system is non-intrusive, non-invasive. For individuals we use primarily voice, and then also profile, weight, and a picture of the face. We can get these without asking."

"But you just asked *me*."

"For your *permission*. We already have the data. We've gotten it many times while you wandered around."

"I actually didn't know that." Martin suddenly felt nettled. They weren't just following the cars. The software knew who he was, knew where he was, all the time. Was there a camera pointed at him right now? He had a flash of self-consciousness. Were they filming him in the toilet? Did they have footage showing him scratching his rear end?

Ralph could see from Martin's expression that he didn't like this new disclosure. "Don't get upset. We could get so much more, all kinds of biometric data—iris patterns or fingerprints—but we don't. And the system has you logged as an unknown, with a tentative ID, of course your real name, since you were matched to the car. But all that is inaccessible without a court order. With your permission, we can make your name available locally and openly to the computers."

"Do you really think that the ability to collect even more data justifies what your town is already gathering? But OK, I'll go along. What do I do?"

"Just sign on the screen here," Ralph said, after typing a few commands. "See, we still use ordinary signatures for legal matters. What we really need is a national ID card, but I don't expect that anytime soon."

"An old debate," Martin said. "But I'd just as soon leave it alone for now.... "

Ralph ignored the attempt to drop this subject. "I don't under-

stand all these people opposed to effective, coordinated national identification."

"Come on, you understand a little." Martin couldn't help getting drawn in. "They're scared. Scared of losing autonomy, of being controlled. They're worried about a future when they have to show the card to take a walk in the woods."

"Is that better than what we have now—worrying about getting killed by an anonymous thug during their walk in the woods?"

"Nice rhetoric, Ralph, but it doesn't alter the fear of control."

"I think it does, to the ordinary citizen. We'll be controlling the people they fear, not them."

"We're caught in a loop, you and I."

"Then here's a new thought." Ralph stood and started pacing. "I think the strongest opponents of ID cards have done things now and then on the sly. Activities they call *technically* illegal—that others would call just illegal. They want to preserve that 'right.' Most of these people have a valid driver's license, have never had any fake ID, wouldn't know how to get a fake driver's license if they needed one. It's crazy. They want to preserve weak, insecure ID cards, when such cards will never do them any good and might do them harm, say if someone with a fake ID assaults them, or if someone impersonates them."

"You're still repeating yourself. It all *starts* with perfect ID cards and goes on from there. Until we have no freedom left."

"There's our difference. I don't want people going wherever they like anonymously. I can do without that 'freedom.' I'll have other freedoms to replace it."

Ralph paused in his pacing, glared at Martin. "Someday you may be accused of a crime," Ralph went on, "one you didn't commit—a crime committed by someone impersonating you. It happens all the time. They'll use your name to steal, perhaps even steal your own money and property. Then you'd need national identification badly—you'd be grateful for it."

Martin broke the loop by letting Ralph have the last word this time, but he didn't agree.

4. Track Data

Wednesday afternoon, March 25

That next afternoon Ralph Barnes was at his office, sitting in a well broken in, overstuffed chair, while his visitor Martin Davis typed at a keyboard. Ralph had tried to straighten up the mess of books and computer parts in the office, but with limited success. Martin's software was searching through processes running on the town's computer system. Unusual activity. He pulled up the executable, copied it and disassembled it. "You see this?" he asked, triumphantly pointing to the screen.

"What about it?" Ralph said.

"This is your intruder. I'm sure. It's one of his agents. He's maybe not very good, because he just adapted a standard worm program. See this section? The program clones itself every five minutes and the son process kills the parent. An everyday hacker approach, I used to do it all the time."

Ralph ground his teeth. "Kill the worm. Chop it into segments. Feed it to birds."

"No, I don't want to kill it. Our quarry might suspect he was spotted. I'll leave it and hope he mucks around. Don't you have any intrusion detection software running?"

"No," said Ralph. "That's an area I always meant to get to. We haven't had problems with network attacks, and I was hoping for the best."

"Well, you've got a problem now. Your system's practically wide open—what they call 'the embodiment of the freedom of information act.' Later we need to talk about security measures you should take, extensive ones, but for now I think I'll leave your system alone and

let my little PC here snoop on the network without responding to anything. It'll just listen and record."

"You'll connect it where?" Ralph said.

"Right here in your office, I think. How good is the *physical* security of this office? Remember, we're assuming an insider. Maybe he works for you. Maybe he has keys."

"Of course I remember," Ralph said. He paused. "Can we mount a video camera around here somewhere? I've never done it in the offices before. If it's one of my programmers, perhaps he won't expect it."

Martin examined the sparsely-furnished office with its tall ceiling. "Only if this were a movie or a spy novel. You've no place for a camera. Just re-key your lock."

Martin then peered back at the screen. A second worm. "I also checked your hacker's yellow flyers that blanketed the town. It's all health information that came from a specific database. We should concentrate on the users of that database. What about usage logs? And other logs?"

"Yeah, we keep a log file of all users of that database. With the username and the access times."

Martin was disappointed. "But not a log of the specific data items accessed?"

"The database has that information, but we don't save it."

Martin finished typing and turned to Ralph. "It's too bad we can't fingerprint the health data. I could put nasty little fingerprints on each version a user gets."

"And get the data dirty?" said Ralph.

"Come on, you know what I mean: *data* fingerprints. Tiny alterations to the content. If he tried to use this information, we'd pinpoint him right away."

"Sounds great," said Ralph. "Let's do it."

Martin stared out the window at cars and people below. "We could in principle. In practice it's another story. Your health database is one of the standard versions my company's worked on. We extended it to provide fingerprints on the data—our value added. But it would take weeks to install. And cooperation from the various em-

ployees. And official permission. A big project, expensive for your town, unless I did it all for free. Even free it's a big project."

"What else can we do—in a shorter time-frame?"

"The database itself keeps a log of all accesses to data items. I'm sure I can get it to copy this log file so it will be around later. Then with the next leak we can sift through all that data, looking for everyone who accessed the specific leaked items. It will be a lot of data, but I'll throw together a few filters. It's not definitive like a fingerprint would be, but it may narrow the field. Also this hacker may access his worm in the next week or so. If he does, I should get a report of that."

"I hope it works, but I don't expect it to. Sounds too easy. Are you going to finish up soon, though? I have to stop by my house, and then there's a party this evening at the Mayor's place. Lots of movers and shakers will be there. And I already told them I was bringing a guest. I should have told you earlier."

"Do I have to dress up?"

"Nah. It's informal." Ralph pointed to his shirt. "I'm wearing what I have on, not even a tie."

"What happens to this guy if we catch him?"

"You always were a softie," said Ralph. "We'll fire him, if he works for us, but nothing else, I swear. It would be hard anyway to get a conviction for what he's been doing. We might even have trouble firing him. Now let's get going—first home, a snack, and then the party."

Ralph parked on the street nearly a block from a large, brightly-lit house. There were cars everywhere. Somewhere would be a screen with green and yellow cars; their's would be green. A huge oak tree dominated the front yard of the mayor's mansion. As one of the perks of the job, the mayor got the use of this official residence—a white Greek revival with four tall columns forming a front porch.

They were late, the party well under way, as Ralph pushed in, with Martin in tow. People were spread throughout the downstairs, even spilling into the kitchen.

"Jeez, everyone has on a suit coat," Martin muttered.

"Relax. *I* don't have one; you're not alone." Ralph greeted people left and right, grabbed food. A short, odd-looking, older man pointedly addressed Ralph as "Doctor" Barnes. Ralph just as noticeably said "Mister" Hoffmann, and Martin recalled the name—so this was Patrick Hoffmann, the person Ralph disliked so much, perhaps a rival for Ralph's friend, Susan Pierce. Hoffmann didn't look formidable, a small, well-dressed man with wiry gray and black hair, a sharp nose, and glasses; Martin thought he looked a bit like Kevin. If Martin hadn't known better, he might not have noticed the undercurrent of tension and hostility in the words Ralph exchanged with Hoffmann. It was also awkward that Ralph didn't introduce them, and Martin was glad when they moved on.

After several quickly-forgotten introductions, they faced a older heavy-set man in a clerical collar. He was bald, with a thick dark beard.

"Martin, I'd like you to meet Father Joseph Phillips. He's Rector at Grace Episcopal Church. Joseph, this is my good friend and former student, Martin Davis, visiting from California to help me with software problems."

"Pleased to meet you, Martin," he said, using the firm handshake that all ministers have. Ralph drifted away as Joseph struck up a conversation. They wandered through several topics, until Martin said:

"Ralph told me the nickname of this town was 'Walden Three.' Have you heard that?"

"Yes, a name bequeathed by my friend Robert Laherty," Joseph answered. "You'd have trouble finding anyone here who hadn't heard the name."

"So what do you think of B.F. Skinner?"

Father Joseph smiled. "A trick question. What answer do you expect?"

"I don't know. But I asked you first."

"Oh, I know what you expect," said Joseph. "Skinner the famous materialist, the atheist, and I the priest. You expect me to say Skinner was the tool of Satan—the world would have been better off without him. Something like that?"

"Ahh … yes."

"Or how about a silly answer? 'He's part of God's Great Plan,' in capitals, 'even as a poor misguided unhappy man.' Well claptrap. Skinner was an important thinker, with fabulous originality. He introduced precision and science into psychology. He taught us to think before we use words like 'freedom,' or 'justice,' or 'dignity.' Do we know what they mean? Do they mean anything?"

"I seem to have pushed a button. You like him then."

An older woman came through with drinks, and Joseph scooped one off the tray. "Skinner talked about Jesus in his 'Walden Two' book. Did you know?"

"Ralph lent me a copy, and I'm supposed to be reading it. I guess I haven't gotten that far." Martin sipped guiltily from his glass.

"Skinner dwelt on the 'Love your enemies' message. He truly was a materialist, of course, but even from his point of view he had only admiration for Jesus."

"As a moral thinker? A teacher?"

"Not at all. As someone presenting remarkably effective techniques of self-control. Mind you, I'm just relating Skinner's view here, and though I share it, I put it into a larger framework. Anyway, Skinner said that oppressed people like Jesus and his followers might let the oppression lead them to rage, and the rage would make them suffer. By displaying the opposite emotion, love, to their enemies, they comfort themselves, they rid themselves of their suffering." He held up his hand as Martin started to respond. "But there's more. According to Skinner, Jesus discovered that love of his enemies gave him power over them, eventually to control them. I wouldn't myself use a word like 'discover,' but that's Skinner's way."

A young woman joined them quietly. Martin tried to look at her without obviously staring. She had dark hair and clean features, an easy smile.

"I must admit I'm pretty much a materialist myself," he said, keeping an eye on any reaction she might have.

"That's one of Skinner's contributions—providing a link between materialism and religion. I talk to young people like you all the time. Even you must admit that there truly was a *historical* person Jesus of

Nazareth, who lived and taught and was crucified."

"That much of course."

Martin found the conversation interesting enough, but Joseph was lapsing into a sermon. "This historical person, Jesus, introduced a remarkable new way of thinking, a 'paradigm shift' we call it now: 'Love your enemies'—the most important shift in human history. Were you brought up as a Christian, Martin?"

"Yes," he said uneasily.

"There you have it. Your whole outlook, your fundamental assumptions, all are shaped by this paradigm, 'Love your enemies.' Renounce your religion if you will, the paradigm remains. Other cultures are bewildered by it. They say, 'If we are to love our enemies, what will we do for our friends?' They don't understand it, but Skinner helped us see it in a new light." He paused, as if he thought he was talking too much. "You see, it's a paradox. He who loves his enemies has no enemies."

Martin felt strangely moved. "That's odd. Ralph was telling me something similar—he wants to make it impossible for anyone to commit a crime—his Walden Three. Now you're saying Jesus made it impossible for anyone to be his enemy. Isn't that interesting?"

Joseph wasn't impressed. "I know about Ralph's plans, and I approve. We've often talked about them. But that's a short-term, stopgap approach, based on technological gadgetry. The real solution's elsewhere. Based on faith and morals, on family and community, and especially on love."

He looked a little sheepish that he'd run on so. The young woman slipped into the pause.

"Ah, father, you always have the same message."

"But it's nice to have a new audience. Martin, meet Becky," he said as introduction. "Please excuse me, they just set out little desserts." He handed Martin a card. "If you're in town on Sunday, this shows the times of our services. You'd be very welcome."

Martin stood alone with Becky, a conversation island in a swaying sea of people. Her hair was dark, and a rounded face framed beautiful dark eyes. She was of medium height and thin, conservatively dressed in a black turtleneck sweater and simple skirt. A plain

silver cross hung on a chain around her neck. He'd taken her at first for a teen-ager but decided she was much older; there were lines of experience around her eyes, a scar on her chin. He tried a random stab at conversation. "Where do you know Father Joseph from?"

"He's my father," she said with a smile. Then when he looked confused, "My *biological* father."

"Ah, I was thinking of a Catholic priest. I guess Episcopal priests can marry."

"I hope so," she said.

This was not going well. "What's it like, being the daughter of a priest?"

"The standard question."

"OK. How often do people ask what it's like being the daughter of a priest?"

"Too often."

He was getting desperate. "Has anybody ever asked how often people ask about being a priest's daughter?"

She blinked. "Maybe. I'm not sure."

"I've got you now." Martin took a deep breath. "Has anybody before *asked* if anybody asked how often people ask you if you like being a priest's daughter?"

She forced the smile of someone used to dealing with computer crazies. Martin felt like a comedian whose act had just died.

5. Track People

Thursday afternoon, March 26

On the day after the party, a warm and sunny afternoon, Ralph was forcing Martin to stare at a computer screen in his office, despite the nice weather outside. They watched a simple screen world that mirrored part of the true world of places and events.

"Now look at this display," Ralph said. "What do you think it's showing?"

Martin studied it carefully, scrolling around a map of the town overlaid with green and yellow tick marks. "My God, these must be people—each spot is an individual! How do you do that?"

Ralph gestured toward the watch on his wrist. "Each of the green spots is wearing one of these, a personal monitor."

"That's it! That's really going too far," Martin said. He was himself surprised at the strength of his outrage—everyone in the town linked to the computers like robots! Martin thought of bad science fiction movies, as when the hero discovers he's the only human being left on an earth full of aliens. Had everyone in the town taken leave of their good sense?

"You have each of these people wired up?" he continued. "Monitored? That's disgraceful, demeaning. How can you possibly justify this?"

"Are you going to listen to an explanation, or just keep babbling?"

Never, never would he wear such a device, Martin said to himself. Aloud he said, "OK, I'm listening, but I can't imagine a satisfactory explanation."

"First off," Ralph said, "these watches are *not* recording or relaying what the person is saying or doing. They're just responding with location and heart rate. The use of these little gadgets is strictly

voluntary—we're only up to 63 percent right now. They serve many useful purposes."

"Yeah, I'm sure. Many useful purposes."

"Will you just hear me out? I can even show you the fancy explanation we sent out when we introduced the watches. 'Propaganda' you would call it. But let me summarize. The watch keeps track of where its owner is and that he or she is in reasonable health. For example, if they have a major heart attack or cardiac arrest, the watch will signal that, and we can dispatch EMS. We may already have saved several lives that way. The watches have two 'panic' buttons on them—one a personal health or injury notification, requesting emergency EMS, and the other a crime or danger notice, asking for immediate help from the police. The buttons are hard to push by accident, though I admit we've had a number of false alarms and a few cases of people pushing the wrong button. Of course we don't get a true false alarm, since each watch identifies the user."

"You're not making this sound good—just tidy and efficient, smooth running," said Martin. "It sounds like a terrible threat to privacy and personal freedom."

"We *are* keeping track of their location. But an individual can push a third 'abort' button at any time to turn off the watch's monitoring functions. It's all voluntary. As for 'freedom,' the citizens who choose to use this watch and even the others who live here and don't use the watches, are mostly free from crime, free from anxiety about crime, free from worry about an unreported accident or illness. They have many 'personal freedoms' that you're not counting."

"I don't care. You'll never convince me this is anything but a terrible idea. You can use sugar-coated logic to make it sound nice, but it still stinks. One day it won't be voluntary anymore, and your prized abort button will stop working."

"The watches come in different sizes and styles," said Ralph. "Men's and women's, and different colors, different bands."

"You're making me sick. I mean physically ill."

"Come on, it's just not that bad." Ralph was wringing his hands, the way he did when he got worked up. "I know you have this picture of me following people around though the monitor, keeping track of

an affair they're having, and later blackmailing them. First of all, remember that the *system* knows who these people are and where they are, but *I* don't know that, and can't find out without good cause, like suspicion of a crime, or a button pushed. And even then there's a log of any information I might obtain—the log's reviewed monthly to see if the law officer's actions were justified. If *I* were having an affair, I'd leave the watch on—it'd be much safer. If I wanted to kill, I guess I'd take the watch off. I suppose I should tell you the rest, though I know you're not going to like this: Even without the watch, our software keeps track of most individuals in real-time."

"Yes, I concluded that. The yellow dots on the screen. And did you explain that to the good citizens of Walden Three?"

"Perhaps not completely, but it was implicit. Maybe we should have explained it better. Some of the good old boys and kids don't realize that we often know where they are. Most of the others, and all the town leaders understand the implications of what we're doing. And approve of it. It's taken two years to get the majority used to this, but now most are convinced, all except the several groups I've mentioned, the different hostile citizens. And we can't track everyone—the yellow dots are either educated guesses, or they are the last-known certain location, whatever display option you choose."

"You said people have gotten 'used' to your surveillance. Humans can get used to almost anything—no matter how horrible. Stick in another phrase for 'surveillance,' like maybe 'neutering the mentally defective' and you'll see where you can get. Even the Holocaust didn't happen overnight; people got 'used' to it, with gradually deadening nerves. I don't like the way your citizens are 'sold' on your controlling mechanisms; you always present them as a snow job or maybe a marketing scheme, but not a revelation of the whole truth. Where's your open access to information?"

"Give me a break," said Ralph. "Nothing is hidden here; the townspeople have had full disclosure. Some don't care about the implications or can't understand them, that's all. And yes, we've been selling the citizens on these mechanisms, convincing them that it's in their interest to go this way. That's how a free society is supposed to work. Those with strong new ideas try to persuade the others."

Ralph grumbled a little more, growling like an old grizzly bear, and then turned to show Martin additional display features, zooming in on the west side. He continued in a more subdued tone: "We also use infrared detectors and CCD scanners at night, along with dish phones. We're lucky how Rockcliff is laid out, with natural barriers on two sides. See here on the screen—there are just a few ways to get into or out of town along this whole western boundary—we did a little digging to make it harder. You should picture a room holding hundreds of screens showing night views around the city. What we have is much better—infrared scanners with automated scene analysis and special attention to movement. The important parts are not the surveillance cameras, but the *agents* analyzing the images in real-time. It's like the early days of the personal computer revolution, when people thought a PC in everyone's hands would make the difference. But only the *connection,* the network of all these PCs really mattered. Now it's not just the network, but the agents at network nodes."

Once again Martin was upset. "You have autonomous agents, pieces of software, outside the control of human beings. Do you know for sure what these agents will do? Just as in all the old myths, such creatures will turn on their masters."

"You keep trying to pick a fight," Ralph complained. "The agents are just logging data—sometimes calling it to the attention of law enforcement, for possible action. And our software agents that do the scene analysis never sleep or get tired; they do a great job identifying what's in their view, especially people—the specific individual—and cars and animals and UFOs."

"You've got UFOs, too?"

"Just kidding. We do regularly get unidentified objects—not flying ones, though. I'll also admit to *you* that for the watches, the heart rate monitor has been erratic—we've had to lower the threshold, to zero for some, because of lost beats." He held up his watch. "The Singapore firm that made these babies oversold them. They've been disappointing. They work fine in a lab with just the right tension in the band, but reception's intermittent at best in the field, and we had to loosen some bands to promote user acceptance. The bottom line is,

we get a steady beat from about half the wearers. Of course the system factors this information into its decisions—any truly anomalous responses still get flagged."

"What about batteries?" said Martin.

"A big problem. Actually, these watches don't continuously broadcast, but instead respond to transmitted pages. Arrival times of the response at different places give us a location estimate. The intermittent broadcasting saves enormously on the batteries."

Martin was idly scrolling through the display, when something caught his eye. "What the … ? *Red* tick marks?"

"Well, what do you think they are?" Ralph asked.

"Um. Maybe important people? The mayor and other big shots."

"No," Ralph said with a short, nervous laugh, "not even close. These are folks on probation—some of them for a serious offense. *They* have no choice. They must wear a leg monitor. And we make sure to get a heart beat from it."

"Can you force them to wear a monitor?"

"I know you'll dislike this answer, but yes. Usually it's a condition of probation. They do have a choice: jail or the monitor."

"How horrible. I'd prefer jail to constant monitoring."

"Well, you're wrong. You've never been in jail. The convicted carry out a normal life with the monitor, and save the town a huge sum compared with jail. Actually, we have several kinds of monitors, from ones that are beefed up versions of the wrist band, and ones that provide audio links, to waist bands that will deliver a disabling shock."

"Oh, God, this just goes on and on: 'A disabling shock.' "

"We have none of the shockers in use right now. And I don't understand your complaint. It's better than shackling a person up, like a turkey ready for roasting. In fact, that's been an issue at trials: no matter how dangerous they might be, our defendants don't have to prejudice a jury with restraints that show."

"These shockers are easily the grossest device you've mentioned yet. Don't you think they could be misused? Set off by accident? Do you have medical studies to show the effects on 'victims'?"

"Well, Martin, I don't want to defend them; I'd use them spar-

ingly, for sure." Then as an afterthought: "If at all. As I said, we're not using any now."

There was an awkward pause. Then Martin said, "One more question. On the display with the cars—I saw it yesterday morning. Are there red cars too?"

"Yeah, good guess. I didn't write this software, but it's well-designed, especially the visual interface. Green for monitored, yellow for neutral, red for trouble. We can tag a car red with the software, say, if we are suspicious. The program automatically tags others red, for example if there's data returned by the state or federal searches. We can also slap a special monitor on a car, by court order, and those show up red too.

"Oh, and I must not forget, we put special hardware on the cars of 'driving while intoxicated' offenders. We get elaborate and accurate data about their car. We can also disable the car remotely if we need to—turn off its electrical system."

Martin had been looking at the display again. His attention snapped back to Ralph. "What? Remotely turn off the car? Like at the top of a hill? That would solve your problem with them."

"Martin, these are convicted, DWI offenders. Just by luck they didn't kill anyone when they were drunk and driving. Whose side are you on here? Would you rather see one of these drunks race all over town with no controls? As for your hill, the brakes would still work—just have to push harder. In fact, after nine months of use, I don't think we've once used this feature.

"There's also a keyboard activation unit," Ralph went on, while Martin rolled his eyes. "They have trouble satisfying it when they're drunk. In fact, there've been proposals for tests in the workplace to check for impairment. We don't use them here, though."

Another day had passed, and Martin decided to stay home Friday while Ralph worked at City Hall. Martin had neglected his consulting and e-mail for nearly a week and needed to catch up. The security report to the Penza Group would take hours to finish, and a furniture

company still had computerized voicemail problems. Ralph used one of the new ISDN phone lines, and he had all the latest equipment. For Martin it was like time spent on an uninhabited Pacific island—well, one with a data link, but no noise or distractions, no annoying phone calls or door-to-door sales people, just Ralph's pushy grey cat and five goldfish. After awhile the silence itself was distracting. And stranded on an island, he probably would have had more food—two rooms full of computer equipment, but an empty refrigerator. How did Ralph survive with no food? He finally found junkfood snacks.

He and Ralph hadn't discussed the evening, but Ralph generally got home at five-thirty. Six o'clock came and then seven, with no Ralph. By eight o'clock, Martin felt like a stranded housewife, but he was a bit concerned. Probably something just came up, an unexpected problem. But wouldn't Ralph call if that were the case? Martin had long since logged off the computer to make sure both phone lines were free, but now he stopped work entirely and paced the house, not wanting to call Ralph at work, but irritated that the evening was wasted.

At nearly nine, Ralph came in and collapsed in a chair. "Sorry I'm so late," he said.

"That's all right." Martin had resolved not to start complaining.

Ralph heaved a sigh, then said, "No, no, it isn't all right. Big trouble at work, and I owe you an explanation—can't tell you, though."

Not sounding sincere, Martin muttered that no explanation was needed.

"Oh, rats, Martin. You must not hint about this to anybody, but I'll feel better telling you. Those damn police! Chief Rollins even approved it. What idiocy—and a waste of money, when we don't have that much money."

"Slow down," Martin said. "Start at the beginning."

"OK." Ralph took a deep breath. "I need a drink." He poured himself half a glass of cognac, while Martin declined a drink. Ralph sipped carefully. "The police bought a new toy, an expensive toy, without consulting me. A surveillance blimp. I'd never heard of such a thing, and no wonder—the world's stupidest platform for a video camera. A ten-foot blimp, with little electric propellers to move it

around, and several infrared-sensitive video cameras and CCD sensors. There's a directional microphone on it too, one of those sound cannons."

"That might not be very effective," Martin ventured.

"Not effective!" Martin had never heard Ralph like this. "They gave me a demonstration. Painted it black—might as well have made it florescent—a huge black floating hippopotamus, it stands out like the full moon. Did they think no one would notice? They've deployed it several times, and so far they've been lucky. They can only send it up when there's almost no wind; a top speed of ten miles per hour, so what did they think it would do in a twelve-mile wind? You could shoot it down with a BB gun or a slingshot; you need an unobstructed view from above. Unless it's very high, it sounds like a washing machine in the same room with you. And be careful of power lines; watch out for airplanes. Oh, Lord, how stupid." He stared at his glass, drank more cognac.

Martin tried to calm him. "A silly toy all right. They can paint it red, white and blue, fly it around on Independence Day. Money spent to no purpose, maybe, and a toy *I* would dislike, but I'm surprised *you* 're so upset."

"You don't understand this small-town culture. Try to picture it. The people see a black blimp videotaping them? They'll go berserk. And not just the few paranoids. Half the town would flip out. We'd be on the national news." Another sip of cognac. "I found out about it today from the budget printout. At least Rollins didn't directly lie to me.

"Especially now," Ralph continued, "anything we buy like this, anything we deploy, we have to publicize it—everything out in the open. If a blimp had any real utility, we might put it over by letting everybody know, stressing some idiotic use—find Jimmy Hoffa's body, say. Even if it weren't a disaster, we still wouldn't need it. The fixed surveillance cameras we have are fine. And the fixed microphones. If we ever want an aerial platform, I'd go with one of the tiny stealth helicopters, but again, we'd have to promote it."

Ralph started pacing again. "The worst of it is, they bought the blimp through Patrick Hoffmann—you know, the newspaper owner

we met at the Mayor's party. Whenever I find something strange going on, he's always behind it."

"I thought you said he was against surveillance, against all your ideas for the town."

"He is, but he often plays a subtle game of intrigue. I think he wanted the blimp used so that we would all be discredited."

"So what's to happen?" Martin asked. "Do they keep using the blimp?"

"I won that battle, but I don't like the implications. I can't threaten to resign every time something like this comes along. I told Rollins that. I'm part of the team; I have to take part in the decisions."

"You trusted the police before?" Martin asked.

"No, dammit, of course not. We need surveillance of the police, too. People must know what the police are doing. Shine the light of public scrutiny on all these activities, keep track of government agencies and their actions.

"I've also changed my ideas about cameras in public. We should spread the word about where they are, and make all the images available publicly. After all, each image just shows what citizens could see for themselves by walking to the camera location. Our citizens could help keep areas secure by watching."

"You'd make all the surveillance images available on-line, to anybody?"

"Yeah," said Ralph. "It makes sense to me right now. But I should consider the idea again when I'm not so tired."

Martin wouldn't let up. "What if an individual misused the video images, say, for blackmail?"

"Remember what I said. These cameras are in *public* locations. You can always go to the camera and watch what it records. Or take your own camera."

"What if a company misused your images? A private firm could try to keep track of everyone just as your town does."

"We wouldn't give them unlimited access to the camera images. And they're missing much of the data the town's computers have, anyway. But like I said—I'll have to think this over carefully."

6. Private Lives

Sunday morning, March 29

Saturday had been a beautiful day, but Sunday was cold and gray again. After sleeping late, Martin confronted Ralph, following him to the small back bathroom where Ralph started to lather his face.

"The girl I met at the mayor's party, your friend Becky, Becky Phillips, well, I talked with her on the phone yesterday," Martin said. "She said she wouldn't have been at the party, that she doesn't usually go to those affairs, except that you'd made a special point to ask her father to bring her."

Ralph grunted and kept shaving. "Ouch," he said. "I need a new blade."

"You remember that personality profile you had me fill out? 'Just for fun,' you said."

Ralph grunted again.

"You used that to computer match me with her. You fed in the data, her name popped out, and you asked her to the party."

Ralph finished up, rinsed and wiped his face. "You've got it mostly wrong. You see, I knew her before I knew her father, Joseph, before I came to this town. In fact, she's the reason I'm here at all."

"Then why'd you invite her?" Martin was still nursing a grudge. "You shouldn't match people up without asking if they want it."

"I'll admit I thought you two might like talking to one another. But I didn't try to line you up. I didn't drag her over to you."

Martin glared at him, and he stared back with open-faced innocence. "I'm still suspicious," said Martin. "OK, then, how did she bring you to this town?"

"It's another one of those long stories. I met her at school, after you left; she was the student of a colleague. I was still teaching

computer science. She came back here partly because of her parents and partly for health reasons—she's a diabetic, with a serious form of the disease. She started consulting for the schools—introducing computers, adding tricks. She has a weird background that includes experimental psychology. And she was always interested in improving education—it was the Dark Ages around here with the schools. Anyway, she wanted to do a better job with school records, like test scores—make them centralized, not to mention records of vaccinations and such."

"So she hired you."

"Darn near. They wanted to hire someone to straighten out their computer system, which believe me was a big mess. She tossed my name around and here I am. In fact the hardest step was convincing me to interview at all. This was a year after you'd finished your degree. I was getting tired of teaching, tired of the politics in academia. And my personal life had gone down the toilet. Now for me this has become an experiment in social engineering—to see if I can make a small town work better."

Martin wasn't in a good mood. "I know how to make the town work better, to make crime impossible. Just take away all privacy. Everybody wired up all the time—not even Orwell's 'thought crimes.' Think about it, no family violence, no child or wife abuse. There'd be no guns, not even sharp knives. You can tattoo a bar-code onto everyone's arm—no, their forehead, for easier scanning. Eventually embed control circuitry under the skin, maybe in the chest cavity."

"You're just baiting me, but I'll take your statements seriously anyway. Removing all privacy would be a bigger crime, a crime committed by our town, by society. Of course I have other goals besides just making everyday crimes impossible."

"So what's the big deal about privacy?" Martin said. "Why is privacy important? Why not just give it up?"

"You don't believe this. You want to know how I'll react. I don't know—why is privacy important? Um. I like my privacy. All alone, if I want to march around my bedroom singing skinhead hate songs, I think I should be able to."

"A weak justification there. What if someone overheard you and

misunderstood? Shouldn't society protect you from making yourself unhappy with your songs?"

"I don't propose to protect people from themselves, though I do want to help them conquer any personal demons."

"A daemon is just an autonomous agent," Martin muttered.

"You're really grumpy today. I didn't mean that kind of demon, of course. But I'm fuzzy-brained—I need coffee. Why privacy? This country has always valued privacy. Isn't it some big Fourth Amendment issue? Gee, I don't know if I can justify it on abstract principles. Privacy promotes individuality, and thus promotes individual creativity and individual contributions. Is that a good enough answer?"

"No," said Martin. "People living with no privacy could still make large individual contributions. I took a history class once where the prof talked about the Middle Ages, with its lack of privacy, its anonymity, and how liberating it could be—even inspiring creativity. Like the cathedral builders who worked only for the glory of God. He said privacy and individualism were overrated in the West, had been since the Renaissance. Before then we didn't have much privacy."

Martin paused for several seconds. "Anyway, I'm like you, I guess. It would really bother me if I knew I had no privacy anywhere."

"We have a lot of privacy here," Ralph countered. "I'm proud of that. Because we *officially* do all kinds of tracking and surveillance in public, we're prepared to know about public activities by companies and individuals. A company can put up a surveillance camera in their own private space—we encourage it, but in every case we've been able to talk them into sharing the images. We don't allow business surveillance of public space. A big corporation or wealthy individual can't have you followed around here with no one knowing about it. We're committed to evening the disparity of power between individuals and corporations or government. I want to log data about public activities, for use at need, but I don't want *anyone*, especially not any mega-corporation, snooping around after private citizens, though anyone can make their own videotapes. The result is we have less private and surreptitious tracking than in similar towns."

"How do you know that? Do you have published data? And

what company would want to track an individual in this small town anyway?"

Martin followed Ralph into the den, where they both sat down. "You might be surprised," Ralph said. "Surveillance of individuals occurs all the time, for insurance reasons, or by private detectives, say, related to marital difficulties.

"Oh, I forgot to tell you," continued Ralph. "Somebody messed up the town's official homepage. Before I disabled it, instead of 'Rockcliff,' it read 'Walden Three Labor Kamp,' with a swastika, not drawn backwards like the one outside town. I think it was probably the same hacker. Dammit, that makes me mad."

"Who handles security for you?" Martin asked.

"Me. I handle it. I'm the Security Officer, such as it is."

"And what about the regular security alerts, the patches, all the precautions?"

"I admitted earlier. I haven't been doing it—just been whistling in the dark."

"That's almost encouraging," Martin said. "This afternoon I'll go down a current list of standard security holes. Stick the patches on. This hacker is probably just using a simple hole that he'll find plugged tomorrow. I'll stay up as late as needed today looking around, seeing what I can figure out. I have several expert friends who are often on the net at odd times; they'll have advice. This development doesn't surprise me, though. I said it before: your system's wide open to the sophisticated hacker.

"Another question," Martin went on. "Why haven't you managed to track your hacker? If he's spreading his flyers all over town, can't you see him on your monitors if you're doing so much surveillance?"

"We've been trying," said Ralph. "The guy is clever—he keeps changing tactics on us. First he sent data to the newspaper. The owner, Patrick Hoffmann, my 'friend' who sold us the blimp, published that set, and we raised hell. Because of our complaints, or maybe in spite of them, Hoffmann said in an editorial he wouldn't do it again. The second and third sets were distributed by hand. We got permission to retrieve data near the distribution time, but the software couldn't get anything. Since then the hacker's mailed his leaked

data, sending it to enough people that it's gotten out—he sends me a personal copy. Such arrogance. Our mail system's anonymous, like anyone else's. We're not even scanning most mailboxes, and of course we can't paw through boxes looking for suspicious letters."

"Speaking of Hoffmann I have one other item to show you." Martin pulled a folded sheet from his pocket, handed it over. "Recognize it?"

"Yeah." Ralph made his just-sucked-a-lemon face. "The Walden Three editorial that Hoffmann published—written by Bob Laherty. Where did you get it, and why would you want to look at it?"

"Father Joseph dropped me a copy in the mail. We'd talked about it, and perhaps he thought I'd be interested."

Ralph handed it back.

"I was looking for a smoking gun," Martin continued. "Falsehoods, distortions, ignorant comments. They weren't there. Instead, I find a long quote from Joseph Wood Krutch."

"Yeah. Instead of making ignorant comments himself, Laherty quoted an ignoramus. Please don't recite it again."

Martin paid no attention to his request. "Krutch was not ignorant, whatever he was. He was trashing Skinner here. First Laherty quoted Krutch as saying that human nature no longer existed at all for Skinner—just something changeable, as much or in whatever direction you wish. Here's the rest of the quote from Krutch. 'Since no human nature capable of revolting against anything is now presumed to exist, then some other experimenter—conditioned perhaps as the son of the commandant of a Nazi labor camp—might decide to develop a race of men who found nothing more delightful than inflicting suffering, and to establish a colony to be called Walden Three.' Well there's your Walden Three, a Nazi concentration camp."

"What loathsome debating strategy—call someone you don't agree with a Nazi. Krutch did it to Skinner, and Laherty by implication to me."

"You're not being fair. Right afterward Laherty admits this town is no Nazi labor camp. He's worried about dark possibilities, about loss of privacy rights, about control of individuals—what you and I keep discussing. In fact, this just occurs to me. He calls on the

townspeople to follow carefully what you are doing in the town. Isn't that ironic? That's what *you* want to do—keep track of what's going on."

"Yeah, Laherty is devious, just like his buddy Hoffmann."

"You know, Father Joseph seems to respect Laherty; he called him a friend."

Ralph snorted, almost choking. "Yeah, Laherty can also be charming. Even that swine Hoffmann can be charming when he works at it. Did I say 'swine'? Hoffmann's a toad—a giant, fat toad with warts and poison skin."

In the early afternoon the cloudy weather cleared. Martin was relaxing with the newspaper, mustering ambition to work on security problems, as he had promised Ralph.

The phone rang, and after a short delay Ralph announced: "We're going to have company. Kevin—you know, Susan's son, you met him at lunch—is coming over, and he's bringing Becky's little brother, Michael. Let's see, he must be eleven now, and Kevin just turned sixteen. Susan works this afternoon and into the evening, until eight, at the health clinic." Ralph ran on, giving Martin more information than he wanted to know about the clinic and about the two young computer nerds who were coming. They liked to play some new distributed game at Ralph's because he had such a good phone line.

Martin worried that tying up the phone lines would keep him from starting his work. But there were two lines; maybe they could share.

Susan soon dropped off the two boys without stopping in. Kevin looked younger than Martin remembered—certainly not sixteen, while Michael was a two-thirds-size near-clone of Kevin: straight dark brown hair instead of Kevin's curly black, but the same small, skinny frame and glasses—a poster child for the computer generation.

Martin decided to intercept them before they started their game. "Do you guys know about SATAN?" he asked.

Ralph had been working with seedlings for his garden, tomatoes and beans, getting them ready to plant outside. He stuck his head around the corner of the kitchen door. "What? What did you say?"

"Relax," Martin said. "SATAN, in all caps, is software, related to computer security. I promised you I'd get to work on the town's network this afternoon."

To Martin's surprise, not just Kevin, but also Michael knew all about SATAN, the software that checked networked computer systems for vulnerabilities. "Here's my plan," Martin said. "I'm going to fetch the SATAN software from one of the mirror sites and use it to probe the town's computers. Do you want to watch?"

They both answered yes—the first bit of enthusiasm he'd seen from Kevin about anything. Michael looked like a religious convert getting ready for paradise.

Martin sat down at one of Ralph's computers, after having the boys pull up chairs on either side. Martin first connected to the town's server. "I don't know off the top of my head where SATAN is. I have that information on some computers in San Francisco, but it's easier to use an Internet search engine."

Martin typed "SATAN" to an engine and had the downloading information in less than two minutes. He was glad the Internet was responding so fast that afternoon.

He continued typing quickly. "Ralph already has PERL on the computer, so that will speed things up. You guys look the other way while I type the root password." Ralph had reluctantly given him "privileged" access the day before. Martin retrieved several megabytes of code using anonymous ftp. He explained to the boys how to use the "MD5 message-digest fingerprint" to ensure they had uncorrupted software. Then it was a matter of compiling the code and invoking it through the web browser. Michael giggled at the picture of an actual satan, complete with red skin and horns, that appeared on the screen.

"Cool," Michael said. "Wait till I tell my dad."

Martin groaned inwardly. He'd forgotten that Michael's father was a priest. Michael's family would think they were exposing him to some devil-worshiping cult. Michael was all impatience when Martin explained that the satan image and even the name were mostly a gag by the inventor. "Dan Farmer, who came up with SATAN, is about as weird an Internet guru as you'll ever hear of, but he has high ethical

standards. I actually know him."

Kevin asked a question unexpectedly: "Are you a member of any of the privacy-oriented organizations, like the EFF or CPSR?"

Kevin seemed impressed when Martin explained the he helped maintain the CPSR website. Then Martin turned back to SATAN. The Prince of Darkness was producing a huge problem list, as Martin expected. The boys seemed fascinated by Martin's explanations of the various vulnerabilities. "If the town had installed a firewall," Martin explained, "we'd have had to breach it, but of course there's none."

Ralph interrupted with an offer to get pizzas for dinner. Martin expected protracted negotiations about ingredients, but they always used a standard order which he went along with: cheese and mushrooms for Kevin, who didn't eat meat, and two elaborate combinations for the others.

After the group had gorged on pizza, Martin started the tedious process of installing patches and fixes for the various problems, with the boys hanging onto every keystroke.

7. Conversations

Tuesday evening, March 31

Martin Davis had spent much of a boring Monday and part of Tuesday installing security patches. It all seemed to take longer than he'd expected. Tuesday afternoon was wasted with other maintenance. After a late dinner, Martin went with Ralph Barnes back to Ralph's house. Ralph led the way through his unlocked front door to the study. He fetched Martin a database manual and muttered about "reading his mail." Soon Ralph was hooked into the town's mail server, skimming items.

Martin had stocked the refrigerator himself, since Ralph always ate out. Ralph had explained that if there was food available, he would just eat it, so Martin bought only low-calorie items. Martin fixed iced teas for the two of them and returned to the study.

"What's this?" Ralph said as Martin came into the room. Then, "Good grief!"

Martin got up and stood behind him. Ralph had a mail message on his screen.

"I think it's from our hacker," Ralph said, "but what does the header refer to?"

Martin pulled up a chair. "Just an anonymous server. I thought they'd closed down the one in Sealand."

Glowing letters filled the screen.

```
From daemon@anon.sealand.secure Tue Mar 31 22:43 CDT
To: ralph@services.rockcliff.com
From: an236584@anon.sealand.secure (_A_Turing_Too_)
X-Anonymously-To: ralph@services.rockcliff.com
Reply-To: an236584@anon.sealand.secure
Date: Tue, 31 Mar 04:11.42 UTC
```

```
Subject: You brain-damaged vermin

    You bastard wasps sit in your comfortable chairs,
telling _us_ what to do.  We know what you're up to.
You want to control everything and everybody.  And
you don't have a _clue_ in your tiny brains about
what kind of people you are.  Privileged white males
who have never known any hardships.  You want to
preserve your power and status, to fight the
emergence of a new multi-cultural society.  First you
will get us all registered.  Who has guns and where
they are.  Who are the "trouble-makers" (= those
capable of independent thought).  Then you'll clamp
down.
    Who are you to tell us that safety and security
are more important than freedom, more important than
change?  Your machines and your technology are
destroying society.
:
```

The colon at the screen's bottom meant there was more of the message.

"How does this anonymous server work?" asked Ralph.

"First you register with the server—send them a message. They assign you an anonymous identifier, the 'an236584' in the message. You can also specify a nickname, like a handle that the CB radio people use. This guy is calling himself 'A Turing Too,' with underscores."

"What's his handle mean?"

"It must be a reference to Alan Turing—you know, *the* Alan Turing."

"The name sounds familiar," said Ralph. "Who is he?"

"Are you serious? He *started* the whole field of computer science in the 1930s by finding unsolvable problems. He helped break the German Enigma code during World War II. I think our hacker wants to be Turing's successor."

"Yeah, I sort of remember now, but I never liked theory much." Ralph was staring at the screen. "Can we send a message back to him?"

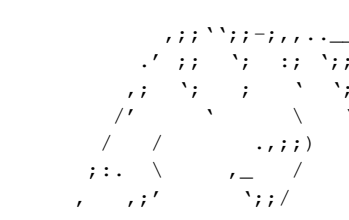
"Sure. We just use the name 'an236584.' Any new message from him will have the same anonymous name, so we'll know that it came from the same person."

"All right," said Ralph, "how about cracking this system and figuring out who it is. Can't we send mail to Sealand saying that we need to know this guy's identity?"

"They aren't going to tell you his name. Or *her* name, it occurs to me. Nothing short of a really major crime—serial killer stuff—would get the name out of the people in Sealand. Well, or serious political pressure. You could conceivably monitor all the traffic from this end, looking for anything going to Sealand. My guess though is that he uses a remote mail server. Unless he's got a death wish, he's not using your city's server. Let's see the rest of his message."

Ralph hit "return," and the next screen popped into place.

```
    For three years now we watched you put up your
surveillance cameras, install your monitors and
microphones and recorders.  Somebody's got to stop
it.  Mr. Hoffmann and Mr. Laherty say you're
destroying the town.  This is our town too.  You
newcomers blow in and take away our freedom.  You've
seen nothing yet.  You know your mysterious crash
three nights ago?  That was us.  We can crash your
silly system any time we want.  Now check your health
database.  We trashed it for you, and that's just for
starters.  Turn off your cameras or we'll destroy
your whole f-f-fing system.  We might destroy it
anyway just for fun.
    We're not waiting any longer.  At noontime this
coming Sunday, if you haven't turned off the cameras,
we're going to stop playing games -- we'll cut loose
on you, and you'll see what we can _really_ do.
Don't forget your deadline:  Sunday noon, April 5th.
```



```
      ;:.  /____  ..-'--.     /-'     ..---. ._._/ ---.
      |    ;' ;'|         \--/;' ,' /       \   ,       \
      `.fL__;,__/-..__)_)/  `--'--'`-._)_)/ --\..)_)/
      _A_Turing_Too_, an3236584@anon.sealand.secure

--***ATTENTION***--***ATTENTION***--***ATTENTION***--
Your e-mail reply WILL be *automatically* ANONYMIZED.
Report inappropriate use:   abuse@anon.sealand.secure
For info or non-anon reply:  help@anon.sealand.secure
For problems:               admin@anon.sealand.secure
```

"He's a friend of Hoffmann?" Martin said, scanning down the message.

"That doesn't surprise me; I always thought Hoffmann was behind this. The skunk. Useless to ask him, though."

"Have you noticed," Martin said absently, "that you always use an animal name when you refer to Hoffmann?"

"Yeah, how else? I see that the hacker is mentioning Laherty, too."

Then Ralph read further in the message. "Jeez. He crashed me the other night—Oh, my God! He's messed up our database."

Ralph pulled up another display window and connected to the health records server. He poked around for a bit, then said, "He's right. It's completely trashed. The clinic's closed tonight, or I'd have heard about it already. Nothing to do but restore the system. I hope you have ideas to help, Martin. He crashed it just a while ago, so he can again after I get it back up."

Martin felt discouraged. He'd just finished beefing up the security of these computers, and the hacker still crashed one he had worked on. What was going on here? The hacker had only moderate skills; this network and the attached computers formed a fairly simple system, so how did he break in again so easily? Martin then had an idea he decided not to share with Ralph. After a bit more thinking, he said to Ralph: "As soon as we get to your server, get there physically, I mean, I want you to reboot and change the root password. Then I'm going to make a number of other changes, mostly disabling services you haven't been using anyway. We may have to announce password

changes to a number of users. Another thing: we have a short time span during which this hacker crashed your health system. My little PC is still snooping on the network, and it should have saved some data. The hacker has no way to know about my snooper. But for now let's send a reply back to him."

"A reply?" Ralph turned to stare. He had the database server in single-user mode and was loading backups from tape. "I'm busy now. But why would we want to reply to this creep?"

"To get more information. Maybe to reason with him. Whatever. Keeping them talking is a often a good strategy—one used by the FBI against the Unabomber."

"Won't it take forever? To Sealand and then back near here? Then his reply to Sealand and back to us?"

"It might be quick, at night like this. And it's even later in Sealand. Maybe just half an hour. You've got another machine here. Let me get to work answering him while you carry on with your backup. I'll draft a message to send in your name."

"You go ahead. What I'd have to say wouldn't be pretty."

Martin set to work composing a reply, first looking over a copy of the hacker's message. The "fL" in the picture stood out, so he asked Ralph if it could be a clue.

"I doubt it," said Ralph. "He probably lifted the picture off the net for his sig. Surely he wouldn't make a mistake like that."

Martin also noticed the use of "we" throughout, but when queried, Ralph thought it was just the same way the Unabomber always used "we" in his communications—a loner trying to sound like part of a larger, more powerful organization.

After Martin finished the message, Ralph looked it over and said, "That's dull. You want to put him to sleep? Anyway, it's a waste of time to send anything to this criminal. If he's willing to crash a computer system, he's not going to listen to you."

"That's the idea—say nothing controversial, just keep him talking."

They sent Martin's dull message off to Sealand. It only asked for more dialog, more discussion of free speech.

Ralph continued his restoring work while Martin thought about

the holes he might have left for the hacker to exploit. Then Ralph got a mail reply from Sealand, from the hacker. After the header, it went on:

```
    You make me sick.  Are you really so blind that
you don't know you're just tools of the establishment
-- big business and government?  You didn't even
address the issue, do you know?  You want to
_control_ us.  That's the issue.  We want to be free.
That's practically the only issue.  CONTROL. You got
that?  Lots of people want to control, and others
don't want to be controlled.  Is that simple enough
for you?  You'll create a controlling society, and
the new technology is giving you the means.

Here's the letter we're circulating on the net:


>                       ================
>                       A CALL TO ACTION
>                       ================
>     A police officer stops a car for a minor infraction.
> Before issuing a warning the officer measures the car's air
> with a sensor to check for drugs, inhalants, or open
> containers of alcohol.
>     The electric company and law enforcement jointly monitor
> power levels of homes for abnormal electricity use.  A police
> van with the latest infra-red monitoring equipment goes to any
> suspicious residence looking for an unusual heat "fingerprint"
> to target indoor marijuana growers.
>     Even disguises can't deceive current face recognition
> software, and voice recognition software lets interested
> parties wiretap as they want.  Electronic money will be
> traceable because governments have scared people into
> believing that only child molesters, terrorists, drug-dealers
> and blackmailers are interested in untraceable money.  Soon
> we will live in a world of constant surveillance.
>     People commit crimes.  Does that mean preemptively
> imprisoning everyone?  People will use electronic money for
> illegal activities.  Does that mean monitoring everybody's
> spending patterns?  Cars are used for criminal activities
> every day. Shouldn't we ban cars?  Criminals send letters.
> Should the state monitor and censor all letters?
>     Criminals are monitored and controlled with leg
> bracelets.  Why not surgically implant them at birth, as we do
```

```
> now with livestock.  Then send physical data in one direction
> and punishments and rewards in the other.  Just think of it:
> no more crime.  No more troublemakers.  No more dissenters.
> No need for courts, or prisons, or laws, or privacy, or bills
> of rights.  Just legions of obedient people doing and thinking
> exactly what they are told by their all-wise leaders.
>     Get involved. Get angry. Do something about it. It would
> be better to destroy this system and this society than to live
> without freedom.
> ************************************************************
> *  "These [United] States need one grand national Vigilance  *
> *   committee, composed of the body of the people."          *
> *        -- Walt Whitman, 1856                               *
> ************************************************************
an236584@anon.sealand.secure (_A_Turing_Too_)
```

"We should keep him talking," Martin said. "And maybe I'm sympathetic with him. Why don't you answer this time? I want to see what you say."

"You're sympathetic with this nasty creature?" Ralph crafted a reply. He was muttering and grumbling to himself as he wrote.

```
I see.  You want no control of anyone, especially no
control of what _you_ do.  You are a common criminal,
and should be locked up like one.  You filthy
hypocrite, _you_'re trying to control _me_.  We've
always had interference -- what you call control --
by schools and churches and parents and friends, but
less now than before.  The free world you want is a
world with people free to suffer, and all you can do
is whine about _control_.
----------------------------------------
Zuerst müßt ihr uns was zu fressen geben.
Dann könnt ihr reden:  damit fängt es an.
(First you must give us something to eat.
Then you can talk:  that's how it starts.)
--                      Bertolt Brecht
----------------------------------------
ralph@services.rockcliff.com
```

"Ralph, what are you doing? That's not going to influence him but just make him mad."

"I don't care. I'm tired tonight. He screwed up my system; then he cries about how he's controlled. To hell with him."

"You just see this guy as an obstacle to overcome," Martin said. "As a 'problem' to solve. I see something different. I see a person with passion, with beliefs, who cares about the world he lives in. I don't mean to co-opt him, but to redirect, to channel, to make use of his abilities."

"Garbage! Excuse me. But this is a criminal. OK, not *just* a criminal—a little more than that, but not much."

"Well, I hope we can find him for rehabilitation. You see, you're in an adult mindset, whereas your tormentor may be high school age. He's computer sophisticated, and I picture a minority, perhaps black, perhaps a woman. He has good English usage. Maybe we can find him this way. Think about a younger minority or woman you might know in town—someone who's always seemed clean-cut and docile, but intelligent, well-spoken."

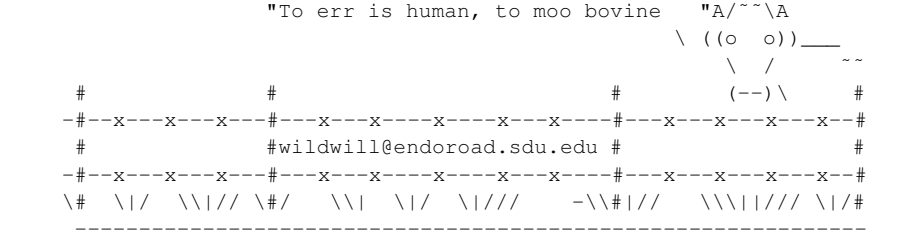
Late that night Ralph and Martin were still working when huge amounts of electronic mail started arriving at Ralph's internet address.

"Look at this," said Ralph. "They're spamming us—over twenty megabytes and more still coming in. Only a few dozen separate messages, though. Here's a small one. Let's see what it says."

He pulled up a message from Arizona on the screen.

```
                                                    late wed 1 april
hi guys maybe you know all about this but I figured
i would drop a line_________________just kidding       :-)  ahhhh
anyway i was hanging out at captain sting's bbs when
i got a call for vurors virtual jurors you know
well i decided to be one cybertrials are such a gas
they were trying four people and one town but one of
them was for sure you ralph whoever you are
the trial is still in progress never stops
people just come and go slows down at night
i really did not agree with the way it was going
besides before they were hardly started they were
posting your names as enemies of cyberspace saying
```

```
get these people spam them destroy their credit       :-(  ummmm
they posted 14 credit card numbers for four people
ralph barnes martin davis paul jordan david rollins   :-@  ohhhh
you all might want to cancel these cards cause
there sure will be a shit load of charges now
anyway good luck just thought you would want to know  ;-)  haaaa
```



Ralph's face turned beet-red; his already huge bulk expanded as he sucked in an air supply. Then he provided a list of synonyms for human excrement. "This is electronic vandalism, cyber terrorism." Ralph took several more breaths to calm himself. "We need to cancel the credit cards right now. I think I'll call Jordan and Rollins tonight even though it's so late. It's scary how easily they can get hold of card numbers. Our credit card system stinks—so stupid—just charge to a number, any number, no authentication at all."

"Well, not any *random* number," said Martin. "The numbers for a given company start a certain way, and there's a check digit, so only ten percent of random account numbers would be valid."

"Oh, give me a break. All they have to do is construct or steal a valid number." Ralph was starting to call his co-workers. "They can paw through trash for receipts or hack into credit reporting companies. Without an effective ID of the individual, there's no check that a stranger isn't using the card."

"Still pushing national IDs? You never give up, Ralph. But it's irritating that *my* name was on the list. I haven't exactly been introduced all over town. How many people know me here, anyway? I *need* my credit cards—they're my only source of money."

In the background a display showed a continuing flood of arriving electronic mail, at a steadily increasing rate. Ralph was still visibly disturbed. "We've got to take action. If the e-mail gets worse, it

could slow our computer to a crawl and clog our network. What will be next? Sabotage? And I just remembered—the hacker gave us an ultimatum, with noon Sunday as the deadline."

8. A School Visit

Wednesday afternoon, April 1

Martin left the house about twelve-thirty. He'd promised to meet Becky at one o'clock and had decided to walk. He had time enough—the town was so small you could walk to most parts in thirty minutes. He tried to recall the town's size—were there really thirty-four thousand people? It didn't seem possible. There was just one high school, just one hospital, though at least two middle schools. True, the downtown area was eight blocks long, with a central square and the four-story city hall. And the town had its own small college, its own historical museum.

Martin was still tired from staying up half the night. By three in the morning, he and Ralph had changed passwords and canceled credit cards, and had eaten at an all-night diner before staggering off to bed.

Martin walked through beautiful trees that loomed over the streets, with bright dappled sections where the sun was shining through. There were sidewalks made from actual stones. As Martin passed an alley, two little boys and a girl, looking like they should be in a pre-school, were poking at a pigeon on the ground. "Is it dead?" he heard one say. He resisted the temptation to intervene. It wasn't his town; these weren't his kids.

He arrived early at Alf Landon middle school, an undistinguished single-story brick building. Becky hadn't said exactly where to meet her, so he was stuck just looking around. Did they have a computer laboratory? His first impressions of the interior were of an open floor plan with diverse facilities stretching into the distance. Students carried out equally diverse activities, some singly or in small groups, with several larger groups. Overhead, the lights flashed to signal

some transition of activities. Assuming they used lights to cut down on noise, it was only partially successful—there was confusion and talking as the larger groups broke up. In the midst of the milling students, Becky appeared and greeted him almost shyly.

"A few things came up that I have to do," she said. "Why don't you observe the discussion group over here." She talked with a young male teacher, then introduced the two men and left.

Martin was seated to one side as a dozen students began discussing an article they had evidently studied—an unusual mixture of Lewis Carroll's Alice with relativity theory. The comments were spirited, with hardly any intervention by the teacher. Soon simple comments gave way to heated arguments: Was the image of Alice really smaller if you observed it from farther away? The final five minutes were occupied with a strange "debriefing" session in which students candidly critiqued their own and others' participation.

Martin felt almost disoriented from all the activity around him when Becky came to his rescue.

"Where's your computer lab?" he asked.

"Distributed. There's no actual *lab.* Just computers where they are needed. From the beginning I wanted educational needs to drive computer use, not the other way around. The biggest and most effective changes haven't involved computers at all: a more open setting, more self-paced work, and more individual initiative about what activity to pursue at any given moment. We wanted to de-emphasize conventional lecture-type teaching, to favor recitation, analytical thinking, critical reading, problem-solving. Actual computer skills are way down on the list."

Martin wandered through the school with Becky. In spite of what she had said, there were computers everywhere, most of them in use. Martin looked at the activities of several students and asked Becky if they were taking exams.

"These are intelligent tutoring programs. As students work along, the program assesses their progress, examines them, if you like. The program also keeps a time log of the amount of effort, so it's not feasible to cheat. For these subject areas there's no worry at all about plagiarism, or cooperation, or cheating on exams. The software doesn't

bore better students with endless repetition, either. It adapts to their progress and gives immediate feedback. And we can get a summary of each student's progress. We use these for mathematics especially, and for segments from other areas—structured areas that involve rote learning. The computer-based education frees teachers to work one-on-one or with small groups. The other type of subject area we have is project-oriented—specific projects crossing subject boundaries that the students work on for weeks, often in teams. Computer use is not yet so relevant for these."

It became evident to Martin that there were far more computers than he'd thought at first; many were tucked away so students could work without interruption.

"How'd you afford all this hardware?" Martin asked.

"A grant from the phone company started it up. Then money from two other companies. And you'd be surprised what industry calls obsolete and will give away. The hardest part was getting computers for the teachers and getting release time for training. Oh, and getting money for software. The board thought hardware was all you needed. We use volunteers, too. Kevin, uh, I guess you met him, right—he even comes by on his bike three afternoons a week. He's old enough to drive but insists on biking. He helped get the network going, and he helps with repairs, with software installation."

They watched students weighing small fluffy chicks in an area obviously used for biology topics. "This is Mr. McAndrews' famous chick experiment," Becky said. "Each year when he teaches nutrition, he has each student raise a chick. They feed it whatever they want, whatever they eat themselves. Meanwhile McAndrews feeds *his* chicks commercial chick food, Purina Chicken Chow or the like. It really gets the kids' attention. Their chicks eat spaghetti and potato chips, and they soon lose their feathers, drop in weight. They look awful, especially compared with McAndrews' chicks."

"Oh, gross," Martin said. "Weren't there complaints?"

"Whatever we do, there are always complaints. We've been getting results, though, and the griping has gone down."

"So you've got the standard modern education tricks here—ones that schools have used for years. What are you doing that's new?"

"Actually, there are even more 'tricks' than you see right away. We have incentive programs for good behavior, a student court for discipline. And as I said before, we're using the computers for major course segments, and to support projects. Just as an example, most students learn a whole year's worth of the 'Algebra One' curriculum with no teacher intervention at all—well, almost none. That's not common yet in most schools. And all records, across the whole town, are computerized and coordinated.

"We have connections to the outside world, too," she went on. "Internet access, of course, where students have their own homepage on the web. We just have a few exceptions; in those cases the parents objected. And we also have access to a variety of special courses we don't have the resources to offer. And access to formal educational materials, like libraries and museums. Much of this is just now getting under way. It's more important at the high school level."

She started sounding like Ralph at his most enthusiastic. "I expect computers to revolutionize teaching at all levels. Much of the drudgery that teachers face should be shifted to the computers. Then there will be time for effective individual tutoring. Software created using hundreds of man-years of effort will support subject areas that have clearly-defined goals. World-wide access to information will be the environment where our students do larger, more ambitious projects."

Martin had to admit, everything at her school seemed smooth, even if a bit manic. "So you're conditioning them—a scene right from *Brave New World:* 'I like being a Beta. The Alphas have to think all the time. And the Gammas work so hard. It is fun being a Beta.' Repeat a thousand times in their sleep."

"You don't like conditioning?" she said.

"Well, no. Who does? Who wants little robots saying just what they're supposed to, what they're programmed to say?"

"I take it you had no younger siblings or contact with younger children?"

"That's right. Just an older sister."

"So you never tried to take care of children, to bring them up. We always condition children, all the time. Sometimes we do a bad job

of it, that's all. What does it mean to guide children, nurture them, raise them? It's all just conditioning."

"I suppose you have an easier time here than in a school with 'big city' problems."

"We do," she said. "But this town has most of the problems of society in general and these problems are mirrored in the schools: divorce, drugs, gang activity, abusive parents, abandoned or unwanted children, needless health problems, AIDS."

"You have all that in such a small town? Here in your 'River City'?"

"Don't assume that smaller rural areas are spared. But in the four years I've been here, I can see substantial change. When I came, there were gangs out of control, lots of drugs—mostly in the high school and above, but spilling down into the middle schools. I can claim only a little of the credit; the problems galvanized the whole town into action."

After another hour, school ended. When they left, a number of students stayed to finish work. Martin thought some of these children should be out playing baseball, but he didn't say anything.

"I shouldn't have made fun of you yesterday," Becky said as they walked to a parking lot, "when you thought a priest couldn't have a daughter. I get that reaction all the time."

"The chances seemed so low, I didn't consider it."

"Chances! So you're one of those people who thinks in terms of numbers, of probabilities."

"Yes. Yes I do. How else?"

"Yours isn't a bad method, just not the only way. It didn't work this time, and how often will such a situation come up for you? How else? Just live your own unique life and forget the numbers, at least most of the time."

They stood beside her car, parked behind the school. "I've got several errands to run," she said. "Later, would you like to get together for dinner?"

Martin agreed to the plan, while wondering if this would be a date. He'd solemnly assured Ralph earlier that he wasn't going on a date. He turned down an offer of a ride and watched her drive

off. They were to meet in two hours at the Summit Street Cafe—guaranteed home cooking.

Martin spent a boring time at Ralph's and went out to his rental car before Ralph got back from work. Martin's redbird friend was still there, a beautiful scarlet male cardinal who loved to admire himself in the car's rear view mirror. Or did this frantic little creature think he was competing with another male? The redbird flew off as Martin started the car to leave.

For Martin, Becky's choice of a restaurant was dull. Fried chicken, mashed potatoes. He was used to such unusual places to eat, every type of ethnic food, that it was hard adjusting to this town. At least Becky was interesting to talk with.

She had studied in England for a year, and Martin had spent time in England, too, so they stuck with England through history, literature, and geography. They must nearly have run into one another at an *Othello* performance in London. "Why didn't you say hello?" she asked.

After dinner, she excused herself to go to the ladies room. "I'm a diabetic," she said. "I must check if I need medicine. It'll just be a few minutes."

Martin felt awkward when she came back. The mention of an illness had let the mood slip. "They've made progress in treating diabetics," she said, "with simple strips to check for glucose levels and get the right amount of medicine or insulin. If you're careful, there's much less chance of complications."

"My sister often talked about diabetes. About its treatment and prognosis." Becky said nothing. Stupid, stupid, Martin said to himself. Why mention prognosis? He hurried on aloud. "Not about these glucose strips, though. She was a doctor, uh, a *real* doctor as she would say—a physician."

" 'She was,' you said. Is she deceased?"

"Yes. She died years ago. I'll always miss her, but it's not such a big issue with me any more."

Martin changed the subject. "Do you buy into what you're doing at your school? The controlling strategies? Shouldn't kids have a chance to develop naturally, to be what they want?"

"Let them be what they want? Don't you believe in original sin? They all *want* to be criminals, sociopaths."

Martin stared at her over the candle on the table. "You're joking, right? Pulling my leg."

"Maybe a little. After all, even the high school mascot is a burglar: a raccoon. But I would guide them to become what *we* want them to be. We shouldn't 'let them be.' Help them choose to be the kind of person we would want in our society."

Martin was horrified, but tried not to show it. "Ralph's been talking about making crime impossible, sort of a running theme with him. His proposals sound very controlling: technological gadgets force adults and children to toe the line. You're saying much worse: Condition children so they do what you want. Now we've moved to Orwell's *1984*. Remember the 'Newspeak' language, with no words for activities they don't want citizens to think about? You asked me about original sin. Don't *you* believe in free will?"

"Yes, I believe in free will, and a lot of other things, too. Eventually, the children must freely choose; we can only help them, prepare them. But you, what do you believe in? Where do you stand? You seem like a computer person who doesn't like computers, who doesn't want to see them used."

"I don't want the computers dictating policy, or taking away our privacy rights, or destroying our freedom."

Becky shifted her chair out from the table and leaned forward. "Tell me this. What do you think a school is? What's the *definition* of a school? A place to baby sit children so the adults can go to work? Well, it is partly that. A place to bring out the creative abilities of each child, to make them think independently, to foster their development? Sure. A place for children to develop however they want? No! Guide them, mold them, prepare them, and yes, even control them. For me a school is also a place where we can make crime impossible."

"Oh, damn!" Martin said suddenly. And he'd promised himself not to swear, not in front of this preacher's daughter, practicing darn and drat and rats that afternoon.

Becky started. "What? That's your response?"

"No, no, I just remembered I promised Ralph to see him early

this evening. It's not exactly early any more. Ralph's hacker struck again yesterday—bombarding Ralph with e-mail, retrieving credit card numbers, including my own. I had to cancel them all. There's nothing like personal involvement. Anyway, back to your school, I think you're over-simplifying. Even if you wanted to, you couldn't make perfect little citizens out of these children."

"No, but it's a worthy goal. We can get part-way there. We *are* getting good partial results."

"Frankly, it all sounds naive. You called me a computer person who doesn't want to use computers. You sound like a computer fanatic who thinks the computers will easily solve all your problems."

"It hasn't been easy, and I'm not that naive. The computers are helping, that's all—just a tool, one of many tools we will use."

Martin was becoming his normal argumentative self. "And you're following the recommended psychological routine? Only positive reinforcement? Don't bruise their little egos."

Becky looked offended. "You must be reading too much B.F. Skinner. We use whatever methods are effective, including negative reinforcement—aversive techniques. We've had to be tough with our more difficult students. Small as we are, we have a special school setting for the disruptive and uncooperative. ADHD students, though, have to go sixty miles south for a school." At Martin's raised eyebrows, she said, "Attention Deficit Hyperactivity Disorder. And there are other learning disorders we don't have the resources to handle. As I mentioned before, we also use remote virtual classes for unusual subject areas and for special students."

Martin felt the conversation had gotten too negative. He deliberately shifted to a favorite topic: simulation, and how it might be used in their environment. Becky was interested in his work with real-time simulations, and they discussed the educational possibilities of ever cheaper and more capable hardware.

They each had driven separately to the restaurant, so they said good-by across the top of her car. Not exactly romantic. Martin thought the evening had sagged at the end. He resolved to be less argumentative the next time—if there was a next time.

9. Evil Influences

Friday evening, April 3

Careful over the ears," Ralph was saying, as Martin eased on the VR helmet. Ralph had been called in for a late-evening session, and after an hour had phoned, suggesting Martin come to the city hall for an interesting display. He'd taken Martin to the basement, where he and his technicians worked on computer hardware. Furnace and water pipes loomed above, while wires and computers covered two rows of tables against the walls. Ralph had equipment jury-rigged on a table in the center of the room. "Have you ever seen, uh, 'experienced,' I guess you say, virtual-reality pornography before?"

"The virtual reality of course, but not the pornography. I saw hard-core porno in college, though. I don't expect this to shock me." Ralph helped Martin slip into a special jacket and gloves.

"Stand and relax." Ralph adjusted straps, plugged in connectors. "You'll be viewing a replay of the last VR session of the person we pulled in—a twenty-four-year-old who lives outside town. *He* participated in the session, so that when he raised his arm, he saw an arm in just the right place. When he slashed with a knife, the image reacted correctly—blood flowing or whatever. But you'll just be watching. As an active participant, his experience was more realistic than yours will be. Why don't you carry on a running commentary about your impressions after I turn it on?"

"OK. Yeah, here it goes.... A remarkably beautiful little girl here, maybe eight years old. I assume you viewed this, so I don't need to describe everything." Martin said nothing as the action unfolded. "She's acting like a prostitute, coming on to him, and he's already, um, 'engaging her,' you might say. Can we break off for a second. I have questions."

The scene froze with a pause command, and Martin said, "Does he have extra widgits, apparatus, like maybe a doll to play with?"

"You got it," said Ralph. "Along with the software, they sell inflatable models that one can actually grab and fondle. Soon they'll have full-sized rubberized dolls hooked into the system that will respond appropriately. That's only feeling. What he sees and hears and smells comes from the VR helmet. Our boy had such an inflatable toy, but you're just experiencing the replay. I've been talking around the real question. During this session, the, uh, gentleman we have locked up probably, ummm, got himself off with his toy, but I'm not sure. Finally, no, I only watched the start of this one. I didn't need to see it. Does that answer everything?"

"Yes, let's go on." Ralph started it up, and Martin continued his commentary, after a delay: "OK, now he seems done with her." Martin had to pause. "Now he's hitting her around, and she begs for more." Another pause. "He's slashing at her with something, I guess a knife.... That's really gross.... He's cutting her all over the place, and she keeps saying how much she likes it.... Now it looks like he'll simulate sex with her again." Martin paused longer. "She's missing one arm!" He paused and watched, horrified. "Oh, jeez. That's just...." Words failed him. Finally he signaled frantically, and Ralph turned off the machine.

"I had no idea this existed," Martin said, taking off the helmet. "The sickest, nastiest images I ever saw. Do you know what he was doing at the end? No, I can't say it. What does it do to a person who takes part in these VR sessions? He must have been off the scale to want to watch them."

Ralph settled back in a wooden chair, put his feet on the table before him. "No, I think that's a common misconception. Child molesters can appear to be normal—stalwart types, pillars of the community. I've known several such. They don't see much of a problem with themselves; they rationalize it. They can lose track of reality. Certainly our boy was suggesting unusual activities with the girl he picked up, though he didn't do anything."

"What will happen to him?"

"If he stays here he may get sent to 'sensitivity' sessions. I hear

it can work well over time, but even at best it takes awhile. That's for the health people, the police, the courts. I'm glad I don't have to deal with all that, but I hope he can be treated."

"I see those pictures now wherever I look," Martin grimaced. "Are these systems illegal here?"

"Not the helmet, but this particular software is illegal. It's child pornography, after all. They just download it off the net. I hate to see censorship, but we've got to try to keep this out of our kids' hands, not to mention our adults'."

"Ralph, as a serious question, why is child pornography illegal?"

Ralph paused. "Umm, it promotes the exploitation of children. That's bad, that's really bad."

"But this was a virtual session. They started with a real image, I guess, but worked from there using computer graphics, without an actual child actress. Suppose the images were entirely digital, no children involved, no one exploited. Is it still child pornography? Is it illegal? Should it be illegal?"

"Yes … well, maybe." Ralph said. "Oh, I don't know. I'd have to think about it."

"At least, there's no further they could go."

"That shows your lack of imagination. As I said before, there'll soon be motorized, rubberized attachments. Right now there are multi-user versions—say, two people participate. They can actually touch one another. If one 'cuts' the other with a dull plastic sword, there's blood. They can have group sex—actual sex with one another, and virtual sex with various VR objects. And even that isn't all …"

Martin interrupted. "Don't tell me. It's nice to know we're breaking new ground in pornography. Thinking thoughts more disgusting than ever before."

"That's not true," said Ralph. "Haven't your read de Sade?"

"Well, I've heard of him, but I've never read him."

"He wrote pornography—in the previous century I think or maybe earlier. He was a sick man, and he wrote truly sick stories—nothing worse has ever been written."

"But *you* read him."

Ralph sounded defensive. “I had a roommate in college with several of his books, but I didn’t read much from them.”

“Yeah, sure.” Martin ignored Ralph’s glare. “So the VR session I just viewed is not a big deal after all? Kids could read de Sade and get the same kicks.”

“The same *subject matter*,” corrected Ralph. “But virtual reality is a new and dangerous development, near-life in realism. The average person will be entranced, captivated, where he would be bored with words on a page. Someone can try out new activities he wouldn’t normally meet up with. I tell you, I’m scared of this new pornography. Anyone can be desensitized to violence, to brutal, antisocial, deviant behavior, and that’s what happens. I think our society will face whole new classes of ‘schizophrenic’ behavior we’re ill-prepared to deal with.”

“Well, I’ve used virtual reality for network visualization. We look for anomalous activity on the net, to ferret out hackers. The visualizations help. I’d hate to give up the technology.”

“Who wants to give it up,” said Ralph. “Just not the inventive pornography you saw, and its ever-more inventive descendants. Do you remember a movie from years ago, where a vehicle with passengers was ‘miniaturized’ and injected into a person? They were the size of a blood cell. Traveled all over the body.”

“I saw it as a thrill ride at a theme park.”

“Soon we’ll be able to do that.” Ralph finished packing up equipment, then crossed the room to an old coffee machine he’d fired up an hour before. “Coffee?”

“Yeah, black.”

“The premise of converting a ship and several people to microscopic size is idiotic—scientific nonsense. But we’ll get the same effect with a micromachine, one with sensors and communication channels leading back to VR controls. You’ll *be* right there in the body.”

Martin sipped coffee. “And not just microscopic trips. Magnify me and I’ll take a trip through the universe. That’s what I want. See black holes and distant galaxies.”

“A *virtual* universe,” Ralph said. “At least in your lifetime.”

"Just a mockup, I know. We could get the real thing within the solar system. Not in real-time, though." Martin paused. "Back to the subject of pornography, here's another thought. Maybe we shouldn't have any censorship, no matter how ugly it gets. Think about it in your terms. Censorship creates a 'crime'—with no censorship the corresponding crime is impossible. Just what you want." Martin leaned back triumphantly.

Ralph was shaking his head. "I agree that we want as little censorship as possible, but that's not the same as *no* censorship. Did you ever hear of Lenny Bruce?"

"Just barely. A foul-mouthed comedian. Died of a drug overdose. But that was long ago."

"He was famous for his 'colorful' language, all right, and his willingness to bring up any subject. A reporter once asked for his views on censorship, expecting total opposition to any form. I think he said something like this: 'We must have censorship. Otherwise people will pay to see children run down in the streets.' "

"Your standard way to argue. Running down children isn't a free speech issue."

"Maybe not. But there are still limits, and not just with pornography. Like actually *inciting* violence, instead of advocating it, or teaching children how to kill with kitchen tools."

"Yeah, yeah, the standard 'yell fire in a crowded theater.' But don't take away my free speech."

"You've got to have free speech, huh? Have you seen 'The Terrorist's Handbook'?" Ralph asked.

"Sure, everybody's seen that. Directions on how to make bombs. Even practical advice. At least they advise you not to build them."

"Well, I confiscated a how-to-do-it book from Michael, Becky's little brother, a book that makes 'Terrorist' look like nursery rhymes. I can't believe he'd printed his own copy and was reading it; it's just science fiction to him, I guess. Here, I'll show you a copy on the net."

Ralph connected to a web site and pulled up a nicely-formatted page. He slid back to give Martin access to the computer.

" 'Destroy the World—A Practical Guide,' " Martin read aloud. "They're not settling for half measures, are they?" After reading a few

chapter titles, like "Nerve Agents and Other Goodies," and "Attack the Food Supply," Martin said, "This is a joke, right?"

"The distinction between humor and seriousness gets blurred on the net. But I don't think their ideas would work."

Martin skimmed around in the document, moving back and forth from the table of contents to individual chapters. At one point the book was recommending purchase of a particular commercial farm insecticide—really a type of nerve poison—many, many barrels, and giving directions for distilling the active ingredient, the poison itself, into one barrel. A whole section dealt with exploding the barrel to get the correct "droplet size." "Dress like a maintenance worker," the text continued, "clean shaven, clean uniform. You should be able to kill everyone in a large building, say an airport, or museum, or office."

A section in the "Biologicals" chapter told how to get plague bacteria ("you must play the role of a research bacteriologist—use a fake letterhead and a history of harmless orders to allay suspicion"), how to raise antibiotic-resistant strains ("best to steal the antibiotics from a hospital—they mainly worry about theft of hard drugs"), how to grow large quantities of the bacteria ("lyophilize (freeze-dry) it for use as an aerosol"). Martin shuddered as he read suggestions for eliciting the pneumonic form, for spraying it at international airports. ("A once for all worldwide spread of plague.")

The chapter "Attack the Food Supply" talked of obtaining a plant pathogen called "wheat rust," and spreading it by scattering from an airplane or by dumping into wheat shipments abroad. ("Wheat's not the only food? Let's move on to 'rice blight.' ") Martin skipped past chapters titled "Nukes: Buy or Steal, Don't Try to Build" and "Get Them to Destroy Themselves," to the "Cyber Terrorism" chapter. He read for long minutes while Ralph puttered around.

"Ralph, under cyber sabotage, they've got sections with practical-sounding methods for knocking out the electric power grid, the air traffic control system, the phone system, the electronic banking system, the stock market—it goes on and on. They even write about military control systems for nuclear-tipped missiles."

"Just fiction," Ralph said. "Those computers are all hardened."

"They suggest getting a job as a programmer in the particular

industry you want to take out. But there's more: they recommend a coordinated attack on the evening of December 31, 1999. Diabolical."

"Ah, relax," muttered Ralph. "I understand your worry: chaos anyway on the first day of the year 2000, so that if too much fails, people might totally panic. It's not going to happen."

Martin was still squinting at the book. "Does anybody read this stuff."

"Who knows? But that is not the original; there are many copies out there."

And why, Martin wondered to himself, did someone write this? The book didn't give the usual weak initial justifications—"for information only," "to better understand terrorists," and so forth—"don't try this at home, folks." Did they really want people killed? An obsession with overpopulation, an assumption that a huge die-off would help? Were they showing off, demonstrating how clever and knowledgeable they were? Of was the idea to protect society by calling these possibilities to people's attention?

Ralph interrupted Martin's reverie. "I'll say this: they may end up suggesting actions to disturbed people who might not otherwise come up with such clever ideas. These methods won't work to destroy civilization, but some of them could cause terrible problems for society."

"The 'disturbed' people will think of these anyway," Martin said. "The remainder of society, those are the ones who need to be aware of the possibilities. Take a child like Michael, for instance. He was reading this, of course just for entertainment, but even if he were serious, he couldn't take advantage of the techniques in the book. A child can't buy fifty-five gallon drums of insecticide."

10. Dinner Time

Sunday afternoon, April 5

They were sitting in Becky's car at one-thirty. Martin had returned his rental car days ago, and she'd insisted he drive hers—an old-fashioned touch.

"I don't like admitting this," Martin said, "but I'm scared, really scared."

"Oh, there's nothing to be afraid of."

"Look at my hands shake. I'm terrified."

She took hold of both his hands—maybe he was onto something. "It's just dinner with my folks. They're nice. They're easygoing."

"Dinner with a girl's parents is the most frightening ordeal a guy ever has. And your father's a *priest*. Just wait. He's going to ask if I believe in God, or maybe ask me worse."

"What could be worse than that, you coward?"

"Asking me to say grace before dinner, that's what. 'Martin, will you please give thanks?' I want to go home and curl up with my computer."

"Out!" she ordered. "Out of the car. Think of yourself as a soldier in a foxhole, ready to assault a hill. Leap out before your courage fails."

Martin followed her advice, opening the car door quickly, then going up the walkway with her. The house before them was an interesting older Queen Anne with a beautiful widow's watch tower on the right and a wrap-around porch. The house needed repairs and a good paint job.

"What's your mother like?" he asked.

"Just relax," Becky started to open the door.

"Aren't you going to ring the doorbell?" Martin said anxiously.

"I *live* here. I don't have to announce myself."

They walked into a dark entry room, with a larger living room to the left and what looked to be a kitchen straight ahead—all fitted out with old furniture that suited it. Martin had expected neatness and order, but here instead was disorder—lots of bookcases and even stacks of books on the floor.

Becky's mother, Margaret, was bustling and fussing around, looking harassed, putting final touches on a formal meal. He'd gone to church with Becky that morning—a trial, but at least she had coached him well: stand up, sit down, kneel, repeat. Calisthenics, aerobics. Joseph had of course run the service, while Becky's mother had been occupied elsewhere with mysterious organizing roles—whether cooking or child care or what, he hadn't found out.

Joseph came hurrying in, evidently from his church, and asked if Michael, Becky's little brother, was there yet. In response to a negative answer, Joseph and his wife looked at one another and decided somehow, perhaps by telepathy, to start dinner without him.

After small talk, after sitting down to dinner, after a short simple prayer by Joseph, came—more small talk: the weather (nice) and peas (hard to eat). Martin thought he might survive.

Ten minutes into the meal, Michael arrived breathless.

"Mom, I couldn't help it. I got stuck at George and Kate's car wash. It's for the Club." Don't ask, Martin told himself silently, what "the Club" is.

Michael was surprised but happy to see his friend Martin. As he ladled food, he asked pointedly why Martin had come to dinner. Becky's mother explained that Becky had invited him.

A light seemed to dawn, and Michael said quietly, as if to himself: "Thank goodness. You know, it's embarrassing to have an old maid for a sister."

Becky actually blushed, while her mother told Michael to hold his tongue. She went on to say they'd gotten a letter from their middle child. To Martin she said, "Sarah's in Basel, Switzerland, singing in the opera there. I wish she had a job in America, but there are so few chances here."

Michael, on his home territory, was much more open and ar-

gumentative and opinionated than he'd been a week ago Sunday at Ralph's house. "Are all eleven-year-olds like this," Martin muttered to Becky, "or is this one just precocious?"

To change the subject, Joseph held up his fork for attention, getting into a college lecture mode. "I've been thinking about Skinner's Walden Two. The town was a group of like-minded volunteers, an artificial community created by assembling these volunteers, with no dissension in evidence and no diversity. That may give stability, but it doesn't solve our problems with existing communities." The others were busy eating, but he sped on anyway to forestall any interruption. "I don't just want people who agree with me. A healthy community needs diversity—ethnic, cultural, religious, you name it."

Martin was glad for a chance to speak. "I finished the book a few days ago. Interesting ideas, but a one-dimensional society, except for the main characters. And having all volunteers would make agreement easier, as with a Mennonite community."

"If you want a static, dead community, you can drive out diversity. To me, Walden Two seemed dull. A few hundred or a few thousand people interacting, all voting the same way, more like a cult community than a town full of Mennonites. No connections with the outside world, at least not that he mentioned."

"What about this town? It looks like all WASPs?"

"Well, not as much ethnic diversity as a large city, though partly because of the college we have minority ethnic groups here—there's more variation than might appear. Three weeks ago there was an altercation involving two Muslims living here. Local toughs were making fun of their clothes and then followed them to their mosque, walked in and ridiculed it, too. Not very fancy, but it's their place of worship. Our Committee intervened forcefully for a change."

"Your committee?" asked Martin.

"An anti-defamation group," said Becky. "Dad is practically 'Mr. Ecumenicalism' around here. He's involved in several groups to promote tolerance."

"Yes, we have the standard mix of ethnic and religious groups," Joseph said. "Just a normal smaller American town, with a few high-tech touches."

"And the high-tech touches?" Martin said.

"You've been working with Ralph, so you should know. The plan is to spread technology through the town's infrastructure."

"How will you do that? Can you give an example?"

"Margaret," with a gesture to his wife, "is Chairman—er, Chair*person*—of the Hospital Control Board. Can you tell him about it, dear?"

Becky's mother put down her fork and turned to Martin. "It's been a great deal of work, but rewarding to see progress. We first resolved to coordinate health data across the town.Ralph helped get the data computerized and centralized, and we're doing well with that. The children can't escape their immunizations—even the transients get caught and vaccinated quickly. Most towns like this have records scattered, in every doctor's office and hospital.

"The next project—we're still working on it—tries to identify those at risk for health problems. It's computerized, and it's already doing a good job notifying people that they need a checkup or should change their lifestyle."

Martin felt invisible hackles rise at the mention of "changing their lifestyle," but he kept quiet.

"We have many other plans. The big limitation is money—how to pay for it all."

Somehow Martin made it though the meal and the obligatory conversation afterwards. Becky's mother fetched ice cream and then cleaned up while they solved the world's problems, or at least the town's.

When she returned to the living room, Martin asked if he could look at the widow's watch upstairs. "I rent an apartment in an 1870s house in San Francisco," he said, "and I'm fascinated by these old houses."

He felt miffed when she wouldn't let him go upstairs. "It's not cleaned up," she muttered. His asking and being so pointedly refused made for an awkward moment.

Martin was then trapped for a time by Michael—dragged over to Michael's computer to look at his web homepage and at some of the work he was carrying out with Kevin.

Later, alone with Becky, Martin said, "Your mom looks sort of stretched out—nervous, tired, I don't know."

"It's that obvious, then," said Becky. "I need to talk with Dad. You see, he's what they call a workaholic. Well, maybe that's too negative a term. Anyway, he's on call all the time, works constantly. But it's his show; he gets the credit and doesn't notice the hours. Meanwhile Mom's stuck with all manner of scut work, people in the church watching her constantly." She started thinking out loud, no longer talking for his consumption. "Mom needs recognition *and* a break, and it has to be subtle—I can't arrange for an appreciation plaque."

She turned to him. "Did you notice any eyes on us in church?"

"I was working at my invisibility spell. Too busy to notice."

"They were there, watching our every move, especially the L-O-Ls, the little old ladies. It's nothing bad, but there's always interest in a minister's family. And if I were to show up in a low-cut dress or with a tattooed biker, the gossip would fly."

"It'll take a day or so, but I can get tattoos."

That Sunday evening Becky and Martin were meeting Ralph for dinner at the town's only Mexican restaurant—at least Ralph claimed it was the only one worth considering. He was already there, working on a margarita.

"Ah, here's Rebecca," Ralph said, standing up.

She made a face. "You know I don't like my name."

"What's the matter with it?" Martin put in.

"It's the nickname. I can't get rid of it. Sounds like someone cute and trivial."

Martin proceeded to order what Ralph was drinking, without the salt, while Becky got a diet coke. Colorful papier-mâché fish hung from the ceiling. The waitress looked like a fresh-faced high school kid, rather than the hardened criminals Martin was used to. Ralph, who seemed to know everyone, knew her too. When polled for advice, she recommended the chile rellenos, stuffed with an eclectic mixture unheard of in Mexico.

"I'm worried that our hacker's deadline has passed," Ralph said during the lag time before the food came. "You remember noon Sunday, *this* Sunday, was his time to cut loose on us. I keep wanting to access the computers, to check for vandalism."

Martin was nervous, even feeling his own heart in his chest and throat, as he said: "I wanted to mention. I have an odd suspicion about the hacker. Could it be, do you think it's possible that it's Kevin?"

Both Becky and Ralph looked surprised.

"No," said Ralph promptly. "I'd suspect Becky here before Kevin. He's a really good kid; also he doesn't know enough to be the hacker. And you said yourself it's probably a minority."

They were interrupted by the waitress bringing food. Between mouthfuls, Martin started in on another track. "Michael has his own plan for making crime impossible. Maybe you've heard it. First he said, 'Do away with money, all money. Crimes involving money won't be possible with no money.' So I asked how people would pay for items they wanted. 'Anything, everything they want is free. Just given to them. No reason to steal anything, because you get things free.' Without any prodding from me he went on to say, 'Each person will work as he is able, on what he does best.' "

"Communism," muttered Ralph. Then more loudly, "And did you ask what he would do about those who won't work?"

"Yes, I asked about slackers. There was no delay in his answer. 'We kill them.' Finally, I asked, 'And who decides which slackers are bad enough that they need killing?' He said firmly, 'Me, I'll decide.' "

Martin turned to Ralph. "I've been thinking about making things impossible. You ought to make back trouble impossible, and nearsightedness. And how about boredom?"

"There are many things we could make impossible," said Ralph. "I have a list in mind that I'll be working on."

"I was just kidding, OK? My little joke."

"Well, I'm not joking. First, I don't want to see death during law enforcement—make it impossible. You know, like the British police, the bobbies in the past—without guns. A police officer with no gun isn't going to kill anyone."

"And what do they use instead of guns?" Martin said. "Sling-

shots?"

Becky set her drink down. "Men always want to fight. We even see it with boys in kindergarten. And when not fighting, they're analyzing, endlessly. But go ahead, you already told me about your non-lethal weapons."

"Becky gave the punch line, but that's the idea: weapons that don't kill given to law officers. I think they hold great promise, but it's been hard to get the professionals to use them."

"Why?" Martin said. "I'd expect them to welcome a way to keep from killing people, even law breakers."

"They don't trust new weapons," Ralph went on. "We've had electric shocking devices—tasers and the like—for a long time. The police worry that they'll get killed while they're trying to sort out the wires and send a shock to the bad guy. A high-tech weapon they like is the stun bomb. You lob one into a room before going in yourself. After the bomb goes off, people inside are disoriented. Those entering get an extra edge, though they mustn't delay going in. They also distrust the new pepper spray, and no one wants my sticky bombs."

"Sticky bombs?" Martin said.

"Yeah," said Ralph. "Many of these weapons rely on stickiness. They stick a car to the road or make the road so slick the car can't move. But the bombs just came out. You throw one, and it explodes as a mass of sticky gunk, all over anything nearby. It's fixed so the gunk doesn't go too far. Often the person is immobilized. You need a special solvent to get it off—water's no good. The bad guy will stick to everything he touches. Unfortunately, I got them to use it, and they're still talking about what a mess it was to deal with the guy afterwards.

"But not just death during law enforcement, I want to make accidents impossible—and make unhealthy lifestyles impossible."

"This would be hilarious," Martin said, "if you didn't sound serious. Becky's mother was talking earlier about 'changing people's lifestyles.' The two of you'll have everyone so pre-programmed and controlled they can't hurt themselves."

"You don't listen to me," Ralph said. "I don't want to *control*. I don't want to arrange the world so people feel controlled, or are

subtly controlled. Take accidents, for example."

"No thanks. I'll pass," Martin said.

Ignoring him, Ralph said. "Society has worked hard to create environments and products that don't hurt people, but there's much yet to do. Consider the bathroom." Ralph glared, daring Martin to interrupt. "It's an accident waiting to happen. Hard, slick floors and tub or shower bottoms, hard protruding metal objects, scalding water on tap. The surfaces you walk on should not be slick. The objects you might fall against should be soft or padded—no burning hot water, either. And don't forget the water-polluting toilet. The bathroom is a mess. They once were a type of home electric chair, regularly frying people, but we've fixed that in new construction with special circuits.

"And picture the typical suburban or urban environment, where children play in the streets and get hit by cars. Our master plan for this town calls for clustered houses connected by pathways to local parks where children can play. I'd like to promote more biking and walking, less driving. I have a dozen other proposals like these, all designed to prevent accidents, improve lives."

"And unhealthy lifestyles?" Martin grabbed Becky's coke, held it up. "This drink isn't healthy. No nutritional value. Ban it."

"You should talk," said Becky. "Look at you two—you're guzzling alcohol."

Martin used his most pompous, academic tone. "Medical studies show that one or two drinks a day decrease the incidence of heart disease. But only for men."

"Whose studies?" she said. "Sounds like male-sponsored research to me. And *you*." She pointed to Ralph. "Mister sits-in-front-of-a-video-screen-all-day. You should talk about unhealthy lifestyles."

"I exercise. I go skiing. And not the sissy downhill skiing. Cross country."

"You go twice a year," she said. "You need *regular* exercise."

"Anyway, back to unhealthy lifestyles." Martin handed Becky her coke and turned to Ralph. "You'll follow people around, yanking fried food out of their hands, force-feeding them fresh vegetables?"

"You keep forgetting," said Ralph, "that I'm serious. No, I won't

force anything on adults. But I do want to encourage them—help them achieve a healthy lifestyle. I had eight aunts and uncles who all smoked, and they're dead, every one, from their smoking, from diseases related to smoking. I would discourage smoking, but I'd also decriminalize the less-dangerous drugs. You know, marijuana never directly killed anybody, unlike cigarettes, though of course a stoned driver might kill or be killed. Many of these people who are set on making all drug use illegal are big users themselves of alcohol, or caffeine, or nicotine, or even prescription drugs.

"My auto mechanic has computerized record-keeping," Ralph continued, "with complete data about my car. I get reminder notes when the car needs service, and when I take it in, he knows exactly what to do: 'Let's see, it's been ten thousand miles. You need an oil change for sure and . . . blah, blah.' "

"They just use reminders to suck money out of you," Martin interrupted.

"Oh, maybe some mechanics remind for profit, but mainly it's good, and you can always decide for yourself—take your car elsewhere or ignore the reminder. Anyway, we should do the same for people—complete records coordinated with reminders and incentives, even monetary incentives, insurance incentives. Most people can use a bit of a push now and then. My relatives sure could have."

"So you'll interfere with their lives," Martin said.

"Damned right! Excuse me, Becky. A bit of interference. Constructive interference. Other places do it already—but not a good job, not coordinated, not thorough. I want to reach out a helping hand to everyone, the young and the old, those with emotional problems, too."

"And if they don't want help?" Martin asked.

"The reminders, the offers, the incentives will be there, year after year. And the records, so when they really need help and ask for it or permit it, we can be effective."

As if in perfect synchronization, to punctuate Ralph's last remark, the lights in the restaurant flickered, then failed completely. After a brief time, conversations started up more loudly, while the restaurant manager and help brought candles to the tables. Ralph looked outside

and found no lights, no power within view.

"He did it," Ralph said distractedly. "It was the hacker. He managed to knock out the power grid, maybe by crashing their computers."

Ralph was dancing with impatience, so they quickly finished their food and headed for their two cars. Becky convinced them that she would get home fine even with the power outage. Ralph had checked that the phones were still working in the restaurant, so he headed home with Martin.

"I have one of those uninterruptable power supplies," Ralph said, "so I should still be able to get on-line. Maybe I can tell what's happened."

Soon after they reached Ralph's house, the power came back, and right away the phone rang. One of Ralph's technicians advised Ralph to check his answering machine message. Sure enough, it was a tirade against surveillance technology and further warnings that the deadline had passed.

"He broke in and changed my phone's message."

"Well," said Martin, "not much of a trick to do that. I'll bet your phone is 'protected' by a two-digit code. Fifty calls on the average and he's broken it."

"It's pretty clear anyway that the power failure was this hacker; my altered message was his signature."

11. Catch a Hacker

Tuesday morning, April 7

A day and a half after the power outage, Martin wandered into the kitchen, where Ralph was eating a doughnut and reading the paper.

"I had a weird dream last night," Martin said.

"Martin, you know I'm not a psychiatrist."

"Come on, listen." Martin looked around for food. Doughnuts, that was all there was. "I was teaching college classes again, but with a twist. I had a *mobile* office that I *drove* to the classroom."

"You mean drove down the hallways, like a golf cart?"

"No, no. It was self-contained—more like a bookmobile. I drove it around outside, through this strange desert landscape, swerving around tall cactuses, over small hills and through sandy gullies. I drove halfway around the campus to the proper door, where I plugged my office into the classroom like the people-mover bus at Dallas Airport. There was hidden machinery that assembled the classroom itself, the right size for that class and with the right equipment. In the dream I didn't know how the students got to the class."

"You're a sick man," Ralph said.

"There's more. Just before class I'd made up visual aids for my lecture—multi-colored 3-dimensional constructions designed by me and spit out of an odd machine, as a picture would come out of a laser printer, only these were solid. I finished the lecture, and drove to the departmental office to pick up my mail—a high-tech dream, and I'm still getting snail-mail. Then I drove off to a meeting with other faculty."

"Well," said Ralph. "Your subconscious is telling you something."

"Ah, psycho-babble. You just admitted you're no psychiatrist."

"I'm serious," said Ralph. "You were just doing physically what we'll all be doing better and easier electronically. You want to meet with students in a classroom? But you also want the resources of an office right there? You and each student will create a virtual classroom, with you all together, interacting. You want visual aids—a rock, or an airplane, or Hoover dam? We already have crude 3-d constructors like the one you described, but who wants a physical object when you can fetch a virtual copy into the classroom. You can all take an excursion to North Africa to check out the pyramids. You can have any kind of learning environment you want. Eventually it will be crazy to spend millions of dollars and years of time building fixed structures for education. We'll 'build' whatever we want in next to no time."

"You're reading quite a bit into a dream that probably started with the extra onions on last night's burger."

"Enough of that," said Ralph, more seriously now. "Look at the story in this morning's newspaper."

The article reported on Sunday night's electric power failure, which lasted thirty-one minutes over an extended region containing the town. The story quoted a power company spokesman as suggesting that someone might have deliberately crashed the computer controlling local power distribution. The article closed with the mention of "yet another computer problem affecting the town."

"The publisher, that louse Hoffmann, wants to blame me personally for everything that goes wrong," groused Ralph. "But anyway, Martin, we've got to take action. The hacker gave his noon Sunday deadline, and I'm sure he followed through with the power failure. Each success will just lead him to a new, more-dangerous step. Soon we'll need to tell the local authorities about our suspicions. What if there's another attack? Other industries should protect themselves. Have you made any headway with the logged data or with your snooper?"

"I have a theory," said Martin. "But I'll need more time today, preferably at your office so I can poke around in your backup tapes, even ones from months ago. Give me just one more day."

As they drove into town, Martin explained that the hacker had

deleted entries in several log files dating from a week ago, after he crashed the health records database. He couldn't know that Martin's snooper computer was keeping its own log file, and in some cases the backed-up log files also still contained deleted entries. Unfortunately, there had been no further leaked health information. Martin said that instead he was analyzing all computer usage data over the past several months. "A bit more filtering and comparison today, and I think I'll have results to show you," Martin said as they walked up the steps into the city building.

Ralph had pushed aside books on the floor of his office—it looked like he'd used a shovel—to make room for a small desk, with a computer on it, where Martin could work.

Martin was certain he knew the hacker's identity now, but he needed evidence to convince Ralph, and maybe to convince others. As with many amateur detectives, Martin was later to find that he'd uncovered only part of the truth.

He soon lost himself in files of data and comparisons between access times. He was using a hand-drawn time line chart to keep track of events and dates. The work was feasible because he was only gathering data in support of a specific hypothesis; he had long since discarded the bulk of the logged data as irrelevant. By late morning Martin was ready with his charts and diagrams and conclusions for a presentation to Ralph.

Ralph had often been on the phone and often out of the office. Martin waited through another call and indicated that he wanted to show his data.

Martin felt nervous when he started, as if from too much caffeine. "The hacker initially got in through a regular account, nearly three months ago. These early accesses are in the log files, but later he deleted logged entries." Pointing to entries as he continued, Martin explained that a professional would have deleted each log entry immediately, but the hacker waited, sometimes leaving a discrepancy between the backup tapes and the on-line entries.

"Since I arrived, I have my own log entries, and they show further discrepancies. These are like flares on a runway, guiding me to this hacker, since only he was deleting entries."

Ralph was having trouble restraining himself. "Get to the meat—tell me who it is."

"All in good time," Martin said. "After I modified your network and secured the machines, the hacker got on again immediately. That really bothered me. The log entries show him logging on as 'root,' with all privileges. He didn't enter through some backdoor; he knew the root password. Then after we changed the passwords, he hasn't been on at all. For me, this was decisive."

"Martin, you're driving me crazy." Ralph was wringing his hands.

"Let's go back and look at the original accesses. The hacker shouldn't have belatedly deleted their log entries—his biggest mistake, calling them to my attention. They represent a usage anomaly: a user accessing the system all day, and then the same user on the system for three and four hours at night. Here's the username; you've surely guessed it." Martin showed Ralph the entry "spierce."

"Susan!" exclaimed Ralph. "You're back to Kevin as the hacker. We already went over that. It's not Kevin. He wouldn't do it. And he couldn't—he doesn't know enough."

"He did, he does," said Martin calmly. "I'll go over all the entries if you like—do you really think Susan used the system for hours on two successive nights, in the middle of the night? But for right now just recall the Sunday afternoon a little over a week ago, when Kevin and Michael came to play computer games. I let them watch as I worked on the network. I typed the root password right in front of Kevin. Real smart. You were using "susan-p" as password—a bad choice, by the way—and Kevin could tell what I typed. Maybe he had to try a few guesses where the hyphen is. After we changed the password and I disabled a few utilities, he was locked out again."

"Kevin!" said Ralph, with clear anguish. He got up and paced the path to the door and back. "Oh, Christ! What am I going to do?"

It was evidently a rhetorical question. "If it was just the hacking," Ralph continued, sounding distracted and stressed. "But knocking out the power, that's really serious. Didn't he know?" Ralph paused for a long while, not a sound in the room. "There were conflicts, resentments, but I thought we were doing better. I never dreamed he had all this anger and hostility bottled up. I don't know what to do."

Another pause. “He’ll finish his classes early this afternoon and then should be over at the Landon middle school. I’m going to talk with him there.”

“Don’t do anything hasty,” Martin said quietly. “That’s basic Ethics 101: gather data, get the facts straight, consider alternative actions—then proceed. And what will you do if he denies everything?”

“It’s not his style to deny this when confronted; I give him that credit. He never directly lies—one of his strong points. Martin, I’m … irritated. The past four years I’ve gone out of my way for Kevin. I taught him much of what he knows about computers. And I don’t like his e-mail mention of Patrick Hoffmann. Hoffmann may have put him up to this.”

“What’s the deal with Hoffmann,” Martin asked. “Is there something special about Kevin and Hoffmann?”

“Oh, sort of,” Ralph said, still distracted. “It’s … complicated. I’ll tell you about it later—sometime. I’m going to leave now. Slam the door shut as you go. Do you want a ride home?”

Martin replied that he would grab lunch and walk home, only about twenty minutes of walking.

After Ralph left, Martin sat thinking. From the start he’d thought Kevin looked like Hoffmann. Could Kevin be Hoffmann’s son? That didn’t seem to make much sense. Hoffmann was so old, and paternity was easy to establish now. They wouldn’t let a wealthy person avoid his responsibilities.

Martin pushed these thoughts aside and began admitting to himself how worried he was about Kevin. What would happen to the boy? Ralph was so hard-line and uncompromising—almost the opposite of what Kevin needed. Martin thought how much he and Kevin were alike—except that Kevin was the precocious one. Martin wondered where his own loyalties lay. He’d never before experienced such mixed feelings—sympathy for a hacker so similar to a young version of himself, opposition to all the prying electronic eyes in this town, dismay at the crime of a crashed electric power grid.

The longer Martin waited, the more agitated he became. The Phillips family, especially Becky and Joseph, knew Kevin well. Mar-

tin decided he should call Father Joseph. Joseph answered right away—as Becky had said, always on call. Martin told him everything, all the details. Joseph was concerned, as one would expect, and he knew all about Kevin's problems with Ralph. Weren't there any secrets in this town? It seemed that Ralph had understated Kevin's resentment—particularly his resentment of a relationship between Ralph and his mother.

Martin promoted the idea of community service for Kevin—maybe they could let Kevin spend time in a police car or at the hospital. "Let him see the town's real problems," Martin said. "At the end he writes an essay, like a term paper, giving his views—what should be done, how this society should change."

Joseph wasn't overly optimistic. It would be up to law enforcement, up to the legal system. He thought that Becky was also at the Landon school and promised to call her. "Perhaps she can mediate between Ralph and Kevin."

Martin walked back to Ralph's place with hot afternoon sun beating on his back. Ralph still wasn't locking his house—an affectation, it seemed to Martin, proclaiming the town's lack of crime. Martin dropped into a chair to think. It was all over, wasn't it? He'd found Ralph's hacker. But he had a sick sense of foreboding that there was always an aftermath, consequences to sort out.

Ralph was gone all afternoon. Finally he called to give Martin an update. He'd talked at length with Kevin, more briefly with Becky, and then at Joseph's house with Joseph and his family.

"At least Kevin admitted it," Ralph said on the phone. "As I expected. He never lies. But I had a … hard time this afternoon. Kevin is unrepentant—and more openly hostile to me personally than before, if that's possible. But there's … more. Kevin didn't act alone, the way we'd thought; he had a partner."

"Ah," said Martin. "Your nemesis, Patrick Hoffmann, was involved. You expected him behind this all along."

"No—well, Hoffmann might have made suggestions—Kevin acknowledged talking with him, but it's worse than that. Michael, Michael Phillips, Becky's brother, was Kevin's partner in all this. I find it hard to believe."

"Oh, I can believe it," Martin replied quickly. "I can see how it might be true. Michael likes to follow Kevin around. It would be just another exciting activity, like watching Kevin play an elaborate computer game."

"We might be able to sell it that way to the courts. In fact, that's the story Kevin wants to go with, that Michael just watched him a few times. Or if possible, Kevin would like to keep Michael out of the story altogether. Kevin really feels sorry about Michael's involvement. But I talked with Michael a long while this afternoon. True, Michael lacks much of Kevin's ideology. While he believes in Kevin's viewpoint, the whole business was a lark for Michael, a diversion. Still, Michael was the one who suggested knocking out the power grid, after finding directions in that 'Destroy the World' book. Kevin managed to hack into the electric company's computers, but then they just followed the book's recipe, steps one, two, three, and darkness on the face of the earth. The people who wrote that book should bear part of the responsibility."

Ralph went on to say that he'd talked with Joseph and Margaret. She was especially upset, and they hadn't decided what to do. "The boys will be in the juvenile court system, and Michael is only eleven. I think we should let both boys face whatever consequences fall out over this; it may already be too late to take a different course. And Martin, why have *you* been so involved in all this? Kevin's just a criminal, after all."

"He's underage, and he's not *just* a criminal. Of course you know that."

"Yeah, I should say not." Ralph sounded more upset on the phone. "He's ideologically motivated. I had no idea. That's scarier than an ordinary criminal. What's to become of him? At worst it's a personality disorder, like a borderline personality. Not a psychosis, but not curable either, in his own fixation area."

"Spare me the psychological doublespeak. Kevin's no borderline personality, whatever that might mean. I have reasons for wanting to help him—hard to explain to you. I was Kevin's duplicate eight or nine years ago, but I was lucky, and maybe I didn't have Kevin's strong beliefs. I hate to see a young and talented person get into

trouble."

"Well, maybe you should talk with him. He doesn't seem mad at *you*, maybe just curious as to how you caught him."

"And now there's Michael to worry about, too," Martin reminded.

Sounding tired, Ralph said that he, Susan, Joseph, and Margaret were going to have an executive session and make a decision.

Hours later Martin was still at the house and thinking of sleep when Ralph came in with Kevin. He and Ralph were arguing.

" … disappointed in you," Ralph was saying. "How could you do this? How could you do this to *me?* To *Michael?*

Martin thought perhaps he should quietly leave, but he felt a compulsion to stay, to intervene if necessary. Martin was aware of his trait to want to help, to interfere, to give advice, but he had to stay and listen. The other two paid no attention to him.

"What bullshit!" Kevin said. "You're screwing up the *world* with your machines, and you give me this crap about 'disappointment.' Listen to this—I know it by heart: 'The Industrial Revolution and its consequences have been a disaster for the human race. They have destabilized society, have made life unfulfilling, have subjected human beings to indignities, have led to widespread psychological and physical suffering, and have inflicted severe damage on the natural world.' "

"That's the Unabomber," said Ralph. "A psychotic serial killer; thank goodness he's no longer loose. That's going to be your source of inspiration and wisdom? You commit crimes and start quoting a maniac about the Industrial Revolution." Martin thought he could hear Ralph actually grinding his teeth.

"Here's another quote, then." Kevin pulled out a sheet of paper. "I don't have this one memorized." Kevin read on in a shaky voice. " 'But now the machine era is coming to a rapid close. It has fouled the air, poisoned our waters, killed our rain forests, torn holes in the ozone layer, destroyed our soil and the art of family farming, rendered our young violent and self-destructive, dried up our souls, and sent

adults wandering for meaning, bewildered and soulless.' Later it goes on: 'The machine era has also managed to bankrupt itself. We cannot afford industrialism any more.' "

"More of the Unabomber," Ralph said, "though I admit those are real problems. Of course I don't like such consequences of industrialization. Nobody does. They're partly a result of things out of control. I want to restore a measure of control."

"It's not the Unabomber. That was Matthew Fox, a Catholic *priest.* A theologian."

"So you quote people I've never heard of. What else does this guy Fox say? I'll take a chance here; I'll go out on a limb. I'll bet this *priest* Fox doesn't suggest killing people, doesn't propose to destroy civilization like the Unabomber advocated. I'll bet Fox wants to *replace* industrial society with something better, or wants to *refine* it. That's what I want, too."

Kevin wasn't going to give a finger's width. "Fox wants what the Unabomber wanted: a return to nature, a renewed respect for nature. In a crisis you need extreme measures to get attention. The Unabomber killed maybe three people. Two thousand civilians per *month* are killed by land mines left around from wars. At least two hundred *million* people died over the past twenty years who should have lived—overpopulation."

"This is ridiculous. You make no sense. How many people was it acceptable for the Unabomber to kill? You can't solve problems by killing people, any more than by causing a power failure."

"You talked about community service. Send me to jail instead. 'Under a government which imprisons any unjustly, the true place for a just man is also a prison.' Who said that? I'll bet you don't know."

"I'm tired of your quotes. Who cares who said it. We're not imprisoning anyone unjustly."

"How little you know. You probably believe what the newspapers say. The 'free' world has always had political prisoners. Like Alan Turing."

"Turing?" said Ralph. "Oh, yeah, your handle. What about him?"

"He was crucial in helping the English in World War Two. And

they paid him back by convicting him as a homosexual, using England's horrible anti-gay laws. He killed himself after he was sentenced to 'chemical castration,' whatever that is—it sounds nasty as hell. The greatest computer scientist ever—they push him to suicide.

"And my quote?" Kevin continued. "I knew you wouldn't recognize it. You guys always talk about 'Walden Two' and 'Walden Three.' What about 'Walden'? Thoreau's 'Walden,' his book, and his other writings. I'll bet you haven't read any."

"I read 'Walden' in college. He went and lived beside his pond. Lived by himself, like the Unabomber, but only for two years."

"You're frozen in your own way of thinking, your love affair with these machines. No room for new ideas. You ought to read Thoreau again—and Fox, and others. Load new information into your brain. Realize that computers and machines are never going to solve our problems. The computers just let us screw up the world more quickly, more efficiently."

"The sad thing is," Ralph said, "there's nothing new in what *you're* saying. The world has always seen anti-technologists. The Luddites in England wanted to throw away all technology. So you and the Unabomber will return to basic nature. What do you really know about 'nature'? At least Thoreau lived out in the woods. You've hardly ever gone camping. Your idea of fun is to be glued to the front of a monitor. Fine—rave on about a return to nature, abandon technology. Wait until you have something as simple, as trivial, as a toothache, say, a *bad* toothache. Your tooth will take over your life, drive you crazy, and you'll have sent the dentists packing. What kind of population level do you think the world could support without technology? What creature comforts? What quality of life?"

"Things will collapse sooner or later anyway. Better sooner than later. For a short time, you and your like, the white, Christian males in power, you who've always been in charge, will keep your control, that's all. The world is changing to something undreamed of by you, a multitude of lifestyles and beliefs, of practices and possibilities that you don't want to understand, that you see as threats. It's useless talking with you, you stupid old man. I know nothing will change your mind."

Ralph stood over him with clenched fists. "You worthless little criminal. I ought to … "

"Yeah, beat me up," Kevin interrupted. "That would make sense."

Martin couldn't stand it any more. He walked over next to them. "Stop it. Stop it, both of you. Let's have respect for each other. You're neither one listening. Kevin, messing with computers, knocking out power, is completely unacceptable. What if someone had been hurt because of the power outage? And we haven't mentioned your worst activity—I'll go ahead and say it—involving an eleven-year-old in all this. We can't tolerate behavior like that, but you, Ralph, should listen to him, hear what he's saying."

Martin's voice nearly cracked. "I'll be honest—I'll admit to you both—I'm enamored with this technology, these computers and the devices attached to them. But I know, I *know* the final answer involves much more. And I *hate* what is happening to our world. I'm not optimistic about our future, facing overpopulation, environment degradation, terrorism, and all the rest, as we are. You, Ralph, would just keep adding gadgets, looking for technological solutions. And you, Kevin, would substitute chaos, the absence of technology and control. We no longer live in an underpopulated frontier land, the Wild West. And people love to romanticize those older, more primitive times. The 'Cowboy and Indian' era contained terrible injustices. Abandoning technology and control, that won't get us through the next fifty years—it will all fall apart, unimaginably horrible conditions. There are too many people now, too dependent on technology."

Martin pointed to Ralph. "Admit it, the technology's not the final answer."

"Of course not," said Ralph more quietly. "I know that. But it will help."

Martin ignored the last and turned to Kevin. "Don't you see what you are? You have a conscience, and you feel pushed into a corner by technology. You use technology to undermine technology. You even use anonymous services. You *like* these computers."

"Sure, I like them," Kevin said, also quieter. "They're seductive. And I see the irony here. So what?"

"Kevin," Martin said reasonably, "the computers can help us get

to the world you want, with respect for nature, a world in balance. We won't get there now without technology. It's never possible to go back, only forward. We can't become native Americans, living off the land. And Ralph is right—you'd hate such a life. The computers are not the problem. *People* are the problem: greedy people, ignorant people, people deceiving themselves, lazy people ignoring problems."

Martin pointed to Kevin, surprised at himself. "I want to talk about all that matters here and now: It's time for strong decisions, for a change in your life, in your approach to life. Instead of attacking computers, or attacking a computerized society, instead of focusing hatred on technology, on Ralph, you need to focus on the real problems. Maybe you could make a difference."

12. To Stay or Not

Wednesday evening, April 8

At 8 pm Martin entered Ralph's house in good spirits considering how stressful that morning and the previous Tuesday evening had been. Kevin was still hostile, but he had given a reasonable and accurate-sounding report to the police. Michael's report was what one would expect from an eleven-year-old: at times whimsical and humorous, while obviously a sobering experience for him—computer games weren't supposed to end this way. The boys had been assigned a hearing date with Judge Patterson, an older local jurist with what Ralph said was a reputation for fairness and restraint. Even Michael's mother, Margaret Phillips, the nervous one in their group, was no longer so upset—partly the work of Becky's calming influence.

Martin walked back to his bedroom carrying two books Becky had lent him. He hadn't heard of the priest Kevin had quoted, Matthew Fox, but Becky had promised to show Martin one of Fox's recent books. She'd come up with "The Reinvention of Work."

"An interesting book, not what you'd expect from the title," she had said. "Fox is … well, not liberal—he doesn't like that term—he'd rather be called radical. The Catholics kicked him out of his order, and now he's one of 'us,' an Episcopal priest, but still controversial."

She had also brought Martin her copy of "Walden," which Martin had glanced at with a real start: It was edited by Joseph Wood Krutch. Maybe that explained why Krutch hated Skinner, Martin decided. Krutch must be some big Thoreau scholar.

Martin's thoughts were interrupted by Ralph rapping on the open bedroom door. "If you're not busy, I want to talk seriously with you."

"Let me get a couch and smelling salts."

Ralph led the way to the living room and gestured toward chairs. "I'll come right out with it," said Ralph. "I want you to work for us, as our Security Administrator—we obviously need one. And to do other programming. You should be able to continue your consulting, so it wouldn't be such a change. I can be liberal about leaves of absence, for you to visit companies you work with, for your seminars. You telecommute much of the time anyway."

As usual Ralph wouldn't let Martin interrupt. "This town is an exciting experiment, finding solutions to social problems. You want less surveillance, more of the illusion of freedom. Fine. Come work here and you can influence the outcome. The pay won't be so great, but this is a good place to live, a good place to survive into the next century."

"If you're that worried, if it all truly falls apart, no place will be safe, except maybe New Zealand, or a small Pacific Island."

Ralph shook his head, more serious now. "You're sounding like Kevin. But if the worst comes, we might make it right here. Several of us in the town's government are working on contingency plans for a societal breakdown, or for other extreme problems. This city has good natural barriers, and we have a local food supply. I've been thinking about this a lot lately, but I have to be careful. Some of our citizens would go crazy if they caught us planning for an apocalypse. I just see it as having plans in place for good times and bad."

"What would you use for weapons, if it came to that?"

"We would never stand up against a well-equipped military group; I'm only planning for a partial collapse, to deal with armed transients and refugees. But anyway, what do you think? I mean about working here. Are you interested?"

"I'll answer if you get me coffee." After Ralph poured a cup and brought it to him, he said. "I don't know." Ralph started a mock scream, but Martin went on, "Hold it. I've thought about this, but I'm worried about getting bored—no stimulation. OK, you have a poetry reading group, but how often does the town put on a play?"

"Once a week," said Ralph promptly. "More often in the summer. Of course just amateur productions. But Skinner himself brought up the issue of boredom. After he wrote 'Walden Two,' people wanted

to found actual Walden Two communities. I read an article about several. An interviewer asked Skinner whether he thought he'd like to live in one. It sounded a bit mealy-mouthed—he invents such a society but doesn't personally want to live there. Lack of stimulation was his excuse. He worried that there would be no one in his field, no one to converse with. Also Skinner's wife was even less inclined to enjoy such an environment."

Martin gestured with the coffee cup, almost spilling it. "That's the problem exactly. It's fun to visit your town for awhile, but in the longer term, what would I do for bookstores, for libraries. I'm used to a big city."

"Don't you see," said Ralph, "the world is changing. We are living in a global village; it's not just an aphorism. The networks now in place and future ones will change everything. Skinner wrote letters by hand; he was never a computer user. He never thought about real-time video links, about multimedia, about conferences or performances by remote individuals. You want to watch a play? You will *perform* in a virtual play, with the actors and audience scattered across the globe. I tell you, isolation is disappearing as a problem. Tell the truth—don't many of your friends keep in contact with you over the Internet?"

"Yes, but what about good bagels for breakfast, and watching a big city wake up in the morning."

"Let's go out for an evening walk. We'll have the town itself as a background."

Hundreds of fireflies were flashing like neon signs. Martin hadn't seen fireflies since grade school. A few blocks of walking and Ralph started again. "I admit, you can't get everything here. No bagels, except frozen ones, or you can get fresh about sixty miles south. A town like this might appeal to you more if you were ready to settle down, a family and all that."

"More matchmaking."

"Maybe having a girlfriend would be an attraction, and there is no large pool of suitable future spouses for you here, that's true—a smaller number of possibilities, though all you need is one. My point is that big cities are better for bachelors, while smaller towns fit a

simpler lifestyle."

"You should talk," Martin said. "Mister eligible bachelor."

"I'm working on it. But stick to the subject. *You* are the subject. I've got a final reason you should stay. In Skinner's *Walden Two* the main character decides to join their community at the end. Do you want to screw the story up here with a different ending?"

The main character of a story. Martin felt weird, dizzy. Who was he? Where had he come from? Was he a character in a story? Would he become one? Reality cracked open—he saw past and future spread at his feet. Ralph's and Becky's personalities melted into his—Martin the rational part, Ralph the practical, and Becky the intuitive, that mysterious part. He had a god's powers—a 4-dimensional view of space and time. He could reach out to change the past, to correct mistakes. He could make any future happen. He saw myself in endless futures doing amazing things. But this way was cheating, not playing by the rules. He took a deep breath, closed his eyes, tried to imagine Walden Three again.

Ralph was talking. "... what's the matter? Are you ill?"

"I felt strange." There was a park bench nearby to sit on. "I'm all right. Just let me sit for a second."

After Martin recovered a bit, he said, "I'll think about it, sleep on it."

When they got back, Ralph had a phone message from Bob Laherty, the source of the town's 'Walden Three' nickname so irritating to Ralph. When Ralph returned the call, he found that Laherty wanted to talk—insisted on coming over. Ralph tried to beg off, but he found it difficult to say no to anyone.

"I'll record this just in case," said Ralph. "And I want you to stay, as a witness. I don't trust him."

"Why not blast him with a shotgun as he gets to the door?" Martin said while Ralph paced around, straightening up and grumbling. Martin added, "And who's going to run the video camera?"

Ralph pointed to his pocket. "Just a mini-recorder, audio only."

Martin had trouble adjusting to the short delay needed to go from one place to another in the town; Laherty knocked on the door just as Ralph started the recorder. Ralph shook his hand and introduced him

to Martin.

Laherty didn't look or sound like Martin had expected. In a display of his worst prejudices, Martin had anticipated a short, red-faced farmer, with a thick regional accent. Instead Laherty towered above them, though he was thin, and he hurt Martin's hand with his handshake—a smooth grip by someone who doesn't realize how strong he is.

Laherty turned to Ralph. "I'll get to the point. I talked with Kevin for several hours this afternoon. He's upset, of course. I know his perspective, and now I want yours."

"How much did Kevin tell you?" Ralph glared at him. "He's the one that's been leaking the health data. Do you know that? And he caused the power outage last Sunday evening; he's not denying that. You have obviously influenced him to act as he did."

"I've often talked with him, but until this afternoon I truly didn't know he had done anything wrong. In fact, believe me, I was shocked. But it's done now, and I'm not even sure it was illegal. You and others are pushing him around, talking about jail or community service, while he hasn't consulted a lawyer. He needs somebody on his side."

Ralph was getting red in the face. "You take quite an interest in this boy. But he's not the only one involved—Father Joseph Phillips's boy Michael also participated. The Phillips family and Susan and I decided that the boys should just own up to what they'd done. I admit that Kevin might have avoided charges altogether with a smart lawyer. The issues are technical, and we had only circumstantial evidence until their statements to the police. But unlike me, you know almost nothing about Kevin. I'm not sure you have his best interests in mind."

"You're patronizing me," Laherty said. "I know all about him and his difficulties growing up with a single mother. I know about the stress of his relationship with you. He's remarkably intelligent, but isolated in this town—at his high school, with his peers. I've been working with him on and off for nearly a year—part of my ministry. And you dare to say I don't have his best interests at heart."

Martin decided to dip his own paddle into the water. "Lets cool down. It sounds like we all want what's best for Kevin." In as rea-

sonable a voice as he could muster, Martin continued. "And that's where this is all headed. Who else should decide what to do except the parents involved?"

"I'll tell you, I do trust Joseph," Laherty said. "He's a good man; he's sincere. Kevin mentioned him last night, and that's part of the reason I'm here talking with you and not filing legal papers through my lawyer. Kevin thinks the idea of community service is ridiculous, an insult, but I feel it does have merit. You need me, though. *I*'m the one who could talk Kevin into a compromise. Kevin probably told you that he'd rather go to jail."

"He mentioned his preference for jail," Ralph said. "He sounds crazy when he's in this mood. And you're encouraging him, abetting him, making him worse. I suspect he got many of his ideas from you. He was quoting the Unabomber and someone named Fox."

"I need to talk with Kevin again if he's quoting those two together. The Unabomber is crazy, but I'm a fan of Matthew Fox, and I've told Kevin about him."

Laherty motioned to chairs. "We should sit down. I didn't encourage him to do this hacking, or to do anything illegal—especially not cutting off electric power. I want open, verbal opposition. But Kevin's ideas aren't crazy—just at variance with yours. You, like most of society, use a high level of technology, without any comparable level of spiritualism. Your approach has no spiritual side."

"I have a spiritual side. But what about your ideas?—loaded down with worn-out, contradictory assumptions, like free will and supernatural authority."

"Ralph!" Martin was appalled. "Don't pick a fight."

"It's all right." Laherty looked at ease, not like anyone with a need to fight. "I make those assumptions, but they're not contradictory. I know what you think I am: a Bible-thumping zealot. They call me a fundamentalist, but I don't know what that means. I do believe in free will, and I do believe in supernatural authority." He gestured as if to include the town. "Out there, they think I believe the world is flat—that I'm against all technology and believe every word, literally, of the Bible, that I've never read anything else. I'm more sophisticated than that. Ralph, I wonder if you and your cohorts know what you're

doing, know the implications."

Ralph had a prompt reply ready. "We do. We're using computer technology to improve security, to make the town safer, make it run better. And we're improving people's access to information, providing guarantees of their privacy. I feel good about the work we're doing."

"You know," Laherty said to Ralph, "I've followed your work for several years now. There's no question in my mind—you're a man of personal honesty and integrity. Part of me respects that, and part finds it sad to see intelligent individuals so naive and trusting. You've created your surveillance systems, with their vast capabilities. And of course the controls are in the hands of people. No amount of system security can negate this environment, the one governing the machines themselves. You see, you are concentrating power in the hands of those who run and control the control system. This leads to corruption—it justifies the fear of control. Your system requires incorruptible humans to run it; humans aren't like that."

Ralph broke in. "W[e do, w]e will provide open information to the public about the controls, the machines, the surveillance systems. Citizens' committees determine policy. I'm not offering a guarantee against misuse, but complete audits of past activity will always leave those in control accountable."

"Ah, you're not offering guarantees," Laherty countered. "I *guarantee* that your system will be abused, used for private and inappropriate ends." He held up his hand to keep talking. "I do trust you, but what about your co-workers, your successors? What if a bad person gets control of the controls? You may never have seen a truly evil individual, but I have—they're out there, waiting to take over your surveillance mechanisms." Laherty gave Ralph an odd sideways look. "I heard a rumor—a week ago—about a blimp the police were using, supposedly for surveillance. Do you know anything about that?"

"I can't comment on police equipment," Ralph said carefully.

"It's true, then. I thought as much. The rumor said Hoffmann had helped them buy the blimp and that *you* killed the project. Good for you. But that shows what can happen, what *will* happen."

"There'll be isolated incidents of abuse—a few major occur-

rences of surveillance misuse in the whole country. Indeed. But that's all. In time, we will close all the loopholes, prevent any subversion of the controls. And as I said already, a later audit will always show up the abuse."

"Did you know that Pat Hoffmann is planning to run for mayor?" asked Laherty.

Ralph looked startled. "He wouldn't get elected. And if elected, he wouldn't have much influence on affairs in the town."

"Wrong on both counts," Laherty said. "With his money to help, he may very well get elected, and he's exactly the kind of person I have in mind who would misuse your mechanisms."

"I thought you were Hoffmann's buddy. And he's opposed to all our surveillance technology."

"Publishing a column in Hoffmann's newspaper doesn't make me his good friend. I know what he is: an evil old man—given the proper circumstances, a violent, dangerous man. You think of Hoffmann as anti-technology, but he's nothing if not adaptable. I expect he would find your technological innovations useful."

Martin wondered to himself if every town, every organization, had these people, like Hoffmann, waiting in the wings, waiting to take over. Not the foolish and ignorant, but intelligent, motivated, talented people who were prepared to misuse technology. That was the final flaw with Skinner's depiction of a Walden Two community: no true internal threats, no one on the inside willing to subvert and destroy their society.

"I get frustrated talking with you," Laherty continued. "You mean well, but you've been seduced by computer gadgets. These machines don't *solve* problems; they may patch up problems short-term, and they always create long-term problems. The machines aren't evil in themselves, but the people who use them can be evil.

"I've got to leave now." Laherty stood up to go. "I'll talk with Kevin. I think I can get him to go along with the judgment of the court, and not request a jail sentence. He has to stop this interference and concentrate on open, legal methods. But count on it: I'll not let up until you've taken down your cameras."

"I'm frustrated too," Ralph said. "Don't you see, the cameras

only show an image that anyone could see for themselves—public activities. A individual could always follow you around in public."

"Bah, sophistry. You've got infrared cameras, and facial recognition software. Eventually you'll be in a position to do a better job following people than an army of private investigators could—the capacity for total control. And then it will be misused.

"I'm amazed at surveillance people like you," Laherty added. "Don't you have higher goals? Goals more important than watching what others do?"

"I'm no 'surveillance' person," said Ralph with heat. "And I *have* other goals. We can't get to any goals if we lose control of society. You're worried about abuses of power by those in control. Well, I'm worried about abuses, too: child abuse, spouse abuse, abuses committed by criminals, and drunks, and other addicts. You're concerned with the criminals, while I look to their victims."

Martin could give Laherty credit, he really wasn't trying to pick a fight as he said, "You see, we agree very well after all as to goals and what's important. I just don't believe in your solution. And you're right—I *am* concerned with criminals. They don't need judgment and punishment, but love and forgiveness. There's only one true solution: they should be born again."

"I see," said Ralph. "Unless they're born-again Christians there's no hope for them."

"Absolutely wrong. There is hope for each person—even for those who never hear of Christ. God's grace is everywhere in the world, just hard to discern—the smallest seed of repentance placed in a man, and it grows into a tall plant that will change his life.

"I want to talk with you at greater length," Laherty went on more briskly. "To see where we agree. Let's try it soon—maybe with Martin here, too. I know we share many views, and identifying this common ground is a good reconciliation technique. For now, you and Susan should be patient with Kevin. He'll make his own big contribution, I know it."

Martin walked Laherty to his car, expecting a Mercedes at least, and certainly not his beat-up Chevy. He gave Martin another bone-crunching handshake, and they exchanged a few words. As he drove

off, Martin could see two crudely-lettered bumper stickers illuminated by a street light. On the left was, “Love one another for Christ’s sake!” while the right side proclaimed, “Jesus is coming and He’s really pissed!”

13. Epilogue

Tuesday noon, October 20

The fuzzy video image showed the back of a stocky man with close-cropped hair. He tore off a piece of tape and wrapped it around a clock and a battery. Wires dangled from the battery, whose rectangular bulk dwarfed what looked like a wind-up clock. Another strip of tape went around two short pipes, capped at the ends. Then the pipes and clock-battery combination received a share of tape.

A tiny microphone relayed the man's voice. "I'll keep those bragging kids out of this project. They'd want all their friends to know." Tongue between his teeth, he kept on muttering and mumbling to himself while he attached more wires and the detonator—but nothing dangerous yet. Those cops would see—take his rifle, lecture him. No one paid attention to him but to lecture, to talk down. He'd show them all. He could improvise anything. As a teen-ager so long ago he'd loved to set off large firecrackers in unexpected places—once even in the police station itself. He would drill a hole through the base of a cone of incense, stick the fuse in, and light the cone's top. It had never failed to go off after about five minutes, time to get away.

Ready for the final connections, and he was more nervous than he'd expected. A slip-up would kill him, but the tiny wires on the alarm hand had made perfect contact with only a small light bulb attached. The hand would make two-thirds of a revolution, and in sixteen hours, a small explosion. No big deal, not to kill anyone, just enough to get their attention. Now! The attachments were made, the clock set. Crude, but effective, it should go off about two in the morning.

He'd spent the whole previous day looking for a good place to leave his offering. The town had an open square at its center, with

an ugly statue of a former war hero. He'd always hated that statue—had painted it, defaced it as a child, and now he would blow it up. He'd made a clever carrying bag with a hole for a bottom, holding an inner bag that could be released and unobtrusively left behind. The inner bag was painted a mottled green and would almost disappear beside a bush at the statue's base. Even a camera pointed right at him would only show him resting briefly and moving on, apparently not leaving anything. With luck they wouldn't notice the bag. He smiled in anticipation as he headed out the door with his bags and his bomb.

On another screen a tiny bright-red figure now moved among the green and yellow ones. Two watching police officers exchanged significant glances; then one reached for a phone.

The standard mistakes continued—ecosystem destruction, depletion of food sources, loss of topsoil, pollution. With not enough edible resources to feed everyone, farm prices quadrupled, then went higher yet. Levels of greenhouse gases climbed upward despite cries for their reduction. After ten years, rising ocean waters threatened to flood coastal cities. Hoards of refugees fled the areas at risk—over two hundred million people on the move. Depression followed the collapse of the world economy. Once areas were isolated, the depression tightened, leading to a loss of control by larger governments; local feudal realms took over. The old testament scourges stalked the land.

"Damn," Martin Davis muttered as he saved one more failed scenario in the NewWorld simulator, a program that modeled the earth's future. He'd gotten it free off the net

He sat before a huge computer screen in a small room near Ralph's office. At least it was a room to himself and not a cubicle. The six months since he'd come to town had passed quickly—always with more to do. He thought about the image the old police surveillance blimp might have shown now after half a year—a nearly identical view of the town, no obvious changes. But he knew the town and the larger world had altered a good deal, and the pace of change

was accelerating. It was subtle, though—nothing visible from above. More computers with more power were hooked into more capable networks with better hardware and software, providing opportunities for access to information—more electronic interaction of the town with the larger world. A technology still in its infancy, so where was it heading? What would the world be like when each person could retrieve every bit of public information anywhere? When groups of remote individuals could participate in many activities as if they were physically together? Martin's biggest contribution had made official meetings in this brave new Walden accessible in real-time or archived for later viewing. The meetings were part of the town's web site, so anyone in the world could see them. It had cost almost nothing, no new hardware. The citizens also had unusually good privacy of their communications, and new means for open expression of their views. But nobody, nobody knew where it would lead. Some would never use the new technology, Martin thought, but just as isolated unvaccinated animals in an otherwise vaccinated population share the general safety, even the non-users would benefit from improved security and privacy and free speech, not to mention the all-important open access to information.

Martin was adjusting to the implications of life in a more controlling society, and there were mostly benefits, so far. Mentally, he put emphasis on the "so far." He himself was helping shift to openness and away from surveillance and control. He now hardly thought about cameras watching him in public, but he did have an automatic assumption of his safety anywhere and at any time.

Martin started up a new simulation. His thoughts drifted to the evening months ago when he'd come upon two drunk men looking for trouble. Just as he began to wonder what he would do, a bright light came on in a tree, and a disembodied voice called one of the men by name. The two grumbled and dispersed. A police officer watching him through a camera—was that different from the same officer happening to wander by at the proper moment? The hardware allowed them to be many places at once, while the software called their attention to possible trouble. Was it bad to do a better job keeping the peace?

A local television news story had recently told of a farm couple's murdered son. They lived outside a nearby town. A mental patient was released early under a special state program; he'd deceived his doctors and was not ready for the world outside his hospital. The father's grief over the loss of his only child was written on his face. He'd spent four years trying to change state laws, trying to do something, anything. The couple was too old to have more children, and their empty lives stretched before them. Why not maintain effective control over a newly-released person with known mental problems who had killed before?

Martin glanced at the clock icon on the screen. Eleven-thirty, not much time to finish another simulation run before lunch. Becky was coming by to take him out for barbecue. No matter how he tweaked the program, the outcome was always bad: collapse and starvation. In fact, the best long-term outcomes came after a horrible disaster, say, a rapidly spreading lethal virus, one that killed much of the population. The software let him introduce new higher-yield plant species or unexpected sources of energy, but always after a few years of prosperity, the world fell apart again. Stability only came from extreme assumptions, like strict population control.

After awhile Ralph had laughed at his fixation with the game. "Don't you know, environmental crazies, greens, wrote that software. Of course it'll predict ecological disaster."

"It doesn't seem that way," Martin had said. "It lets you insert any bias you want, from optimistic to pessimistic. And you shouldn't talk that way, you know. The pro-growth faction loves to label the other side as 'environmental extremists.' "

Ralph was his boss now, so Martin was glad he allowed game-playing at work. Ralph had a theory that workers needed a release from their work—to do something weird now and then, amusing or frivolous. Another crime, thought Martin: misuse of the town's resources, justified as a need for release, for relaxation. Well, the simulation was his outlet at present. He'd continued telling Ralph about the program: "This simulation starts with an object-oriented description of the physical world. Then one builds scenarios that one can run forward into the future. They even give you 'alternate pasts,' like

one where Hitler died and never invaded Russia. History's greatest criminal, eliminated by a few lines of computer code. Will the 'real' world ever be so malleable as this?"

He'd been selling Ralph on the program a week before, but Ralph had no time to play with it. Instead Ralph kept coming up with plans on top of plans for their real work: Coordinate the town's information; make it accessible where possible. Adults already had access to the scanned images from cameras; a special project was to encourage private volunteers to watch the images in shifts, like old-fashioned neighborhood block watches, though they had software agents already doing this work. Then one needed to *deny* access to private information—a harder task. Even a child's teacher shouldn't know everything about a pupil—whether he's undergone psychotherapy, say. Ralph was using a hybrid of military and commercial access controls, and they now encrypted the network traffic.

Martin had shown the simulation to Kevin, the hacker, who had briefly been his roommate, but there was no spark of interest. It had been a crazy thing to do, but he'd talked Ralph and Kevin's mother, Susan, into letting Kevin share an apartment with him. Susan and Ralph had gotten married, and they soon saw what a strain it was for Kevin to stay with them. The court had sentenced Kevin to several hundred hours of community service and two years probation. But Kevin was gone now, with his probation officer's permission, out in the South Pacific on a Greenpeace ship, officially there to look for meteor remnants from Mars in Antarctica, but also ready for environmental confrontations. It surprised Martin how much hope they all placed in Kevin.

There was a rumble, a shaking of the building. Martin, like any good former Californian, assumed it was an earthquake until he remembered where he was. If not an earthquake, then what? A sonic boom? He glanced again at the screen's clock icon. Almost noon. Becky was due, and she was seldom late.

He started the simulation again from the present with modest population control, to see how little control would keep the world stable for a hundred years. He put in other optimistic parameters, while trying to avoid anything extreme. Soon he was totally absorbed, like a

child with a new video game.

Martin thought he might show the results to Bob Laherty when they met tomorrow for lunch—their fifth meeting. Martin hadn't been able to get Ralph to join them, but Martin enjoyed arguing with Laherty, whose probing mind kept poking holes in their plans. Each of Martin's answers just led to more questions. Martin had admitted that they couldn't make a system immune to abuse by the government, but they could try, and Laherty, though not impressed, was at least listening to their plans for open, uncensored access to information.

By twelve-fifteen he was getting grumpy, part of his lunch hour gone, when Becky opened the door. She looked disheveled, stressed somehow. Then he saw blood on her forehead.

"What happened? You're bleeding." Martin said.

"I'm—all right," she said. "Just a bit disoriented."

"Sit down. You don't look so good. Let me get paper towels."

She sat till Martin came back. He then held a damp towel against the cut on her forehead. Now her hands and lips were shaking, making her hard to understand.

"It was a bomb, out in the town square. It looked as if several people were hurt."

"*You* were hurt," Martin said. "Why did you come here. You should go to the hospital. You shouldn't act so brave."

"I'm not brave; I really don't think it's much, and I hate hospitals."

Martin peeled back the paper towel and examined the cut. "Trust me on this. It looks deep enough that you should get stitches. Do you think you can walk? The hospital's only a few blocks away." Martin changed his mind. "No, you shouldn't walk. I'll bring my car around."

In the car, Martin asked about the bomb. "I thought it was an earthquake at first."

"I don't know anything about it. Just a big explosion, and then people running over. Someone tried to help me, but I waved him away."

There were several others from the bomb site in the emergency room, and they had the usual endless wait to see a physician while

a clerk asked all sorts of questions about insurance. Before anyone looked closely at her head, a police officer talked with Becky for a long while, out of Martin's hearing. Then he waited another twenty minutes while she received an X-ray.

Later Ralph showed up as a physician put in her stitches. At one point Martin said to Ralph, "I thought crime was impossible in this town."

"Not funny," said Ralph.

"I wasn't trying to be funny. It looks like Becky is all right, but what about the next time, the next bomb? I thought your cameras would spot a person carrying a bomb around."

"They might if it were a black cartoon bomb with a long fuse hanging down. Even big cities don't have bombs go off too often; we've never had a bomb explode in this town. Never. Thank God no one but the bomber was badly hurt—the bombing 'suspect' I should say. There were just a few other people with minor cuts, like Becky."

"I don't call that minor. They X-rayed her head and are still worried about a possible concussion."

"I'm starting to think like law enforcement: anything short of a major injury is minor. But the doctor I talked with was optimistic. The bomb also damaged the base of a statue, tore off one bronze leg. There were broken windows, and that's it.

"Who is this bomber?" Martin asked. "Is he in custody now?"

"He was badly hurt—I'm not sure what his injuries are or if he'll survive. He's off by helicopter transport to the Level One trauma center about sixty-five miles south of here. We're not prepared to deal with such injuries.

"His name is Richard Lane," Ralph continued. "One of the local crazies, part of our opposition. He was the leader of a small group destroying cameras and other equipment."

Ralph ran fingers through what hair he had left and started sounding distracted. "I keep thinking about how our controls, just their existence, seem to provoke antisocial behavior in a few individuals, behavior they wouldn't normally think of. This bomber has a good job; he's an intelligent guy. The police were careful when they told him they knew about his sabotage activities. They were almost nice

to him—probation is all he got, because he had no record. But now this, the bomb."

"What happened, anyway?" Martin asked. "How did his own bomb catch him?"

"I have a theory," said Ralph. "I've known Richard for years. He's not the type to kill people. He likes gestures. I would guess that his bomb had a timer, set to go off late tonight. There's seldom anyone around here after midnight. When he set the bomb down at the base of that statue, maybe it wasn't steady—fell over and jiggled the wires. We may never know for sure, but the department has video tape from a bug inside his house that should help."

"How about other surveillance camera images?"

"That's the silly part, like a sick comedy. Because of the earlier episodes, we've been keeping track of him—his home is wired, as I said, and the software has him tagged as a special 'red' individual. He had his bomb in a grocery bag with handles, and the exaggerated way he tried to be nonchalant as he carried it was almost a parody. Two officers were heading over to arrest him as the bomb exploded. He wouldn't have gotten away with this even if he hadn't been hurt."

"So it was easy to follow him," Martin said, "since he had done his earlier sabotage. But even so, you didn't stop the bomb from going off. What would you do in a larger city, with so many more random events?"

"A lone bomber who isn't suspected—one of the Unabomber types out there—well, we might catch him before the fact, say, buying dangerous materials, but mostly we'll only be able to prove who did it. And obviously the surveillance would be harder in a big city. Our techniques do scale up, but with a hundred times as many people, who knows? The facial and voice recognition software should work well after a ten-fold increase, since our error rate here is so low, but a hundred-fold increase? The software agents and the humans doing the monitoring might be swamped with data. I'd like to try it out, though."

Just then Martin noticed Ralph staring intently across the room. Looking in that direction, Martin encountered a bleak gaze focused on them. Against all likelihood, it was Patrick Hoffmann, the pub-

lisher, here in the emergency room, though he didn't appear hurt. Ralph visibly straightened and tensed when Hoffmann walked over to them.

Ralph spoke first. "You must be here to see about your friend Richard Lane. He's gone, though, transported south by helicopter; you can pay him later for his work."

"That's a lie, a damned lie, and you know it."

"Well, he likely won't be testifying against you, so your luck holds this time."

"I could sue for slander, for making false accusations," Hoffmann said smoothly. "And you should congratulate yourself, Ralph. You kept me from getting elected mayor, but another election is coming in eighteen months. I think I'll make it, and afterward there'll be an accounting—find out what you and your friends are doing and why. A reorganization. Maybe some of you people need a new job elsewhere, for a better career, more satisfaction."

Ralph's voice was tightly controlled. "In fact, the town is too smart to make you mayor, now or later. Maybe *you* 'd be happier in a different town."

Martin noticed Hoffmann's clothes for the first time—very expensive—his perfect silk tie and perfect imported shoes. Did he always dress this way? Was he really as bad as Ralph seemed to think? "You even drove Kevin away," Hoffmann said, "after denying me my rights to him all these years."

"Your rights!" snapped Ralph. "Just your little fantasy designed to drive Susan crazy. I'm busy now; I don't want to talk with you. Thanks for warning me about the next mayor's race."

"I'm always happy to help you—any time."

Hoffmann directed a dark scowl at Ralph as he walked away. He sat down across the room and resumed a conversation with a middle-aged man waiting for treatment.

"What was Hoffmann talking about?" Martin asked. "His 'rights' to Kevin."

"Please don't repeat this around, but you may have noticed a superficial similarity between Hoffmann and Kevin. Hoffmann latched onto this and onto the fact that Susan divorced before Kevin was

born. Susan and Hoffmann's younger brother were friends, though she never had 'relations' with him. Anyway, Hoffmann claims Kevin is his nephew."

"That ought to be verifiable," said Martin.

"Oh, the brother is dead now, buried somewhere, I don't know where. It's all conveniently uncheckable, and typical of Hoffmann to come up with a complex and bizarre theory to make trouble. He even wanted genetic testing of Kevin; Susan, along with Kevin's real father, refused to consider it, of course. Both their lawyers strongly recommended against giving in to testing. I'm more worried, though, about Hoffmann as mayor. He would seize control and then do God knows what."

"So keeping control out the wrong hands—that's the weak point of your proposals, just as Laherty maintains."

"We've always had that problem; we always will. I've said it before: the open access to information will help prevent these clever, ruthless people from taking charge, and will limit their activities if they do seize power."

But, Martin thought, the power hungry would still be around waiting for their chance. If Ralph was right, Hoffmann was such a person, and in any event others would be ready. He spoke up again: "Another approach besides openness is decentralized power, distributed control. The sharing of power, the checks and balances, has often worked in America to curb those who would control everything."

At that moment, Becky came out to them with a bandaged head, evidently finished getting stitches. She had refused to let Martin call her parents, saying that her mother would just "go crazy" at the news. A few more forms to deal with, and she was free to leave, clutching printed instructions.

They said good-by to Ralph and headed for Martin's car, as he related what Ralph had said about the bomber.

"Richard Lane," she said with distress. "I know him. I knew him well. He was two grades ahead of me in high school. What terrible news. I hope he recovers."

"How could anyone commit an act like this?" Martin wondered

aloud. "Such trivial motivation leading to such a serious crime. It's crazy."

"No, not crazy," she said. "This is the way we are. Anyone, everyone has within themselves the potential to go down this path. I'm what one calls a 'Christian pessimist' at heart. People will always want to commit crimes; people are intrinsically evil. It sounds harsh, but even some 'brain research' is leading to the same conclusion—a fundamental flaw in the brain's wiring. At best Ralph's methods will lead to people who don't commit crimes because they fear getting caught. Individuals must choose to do good acts, must freely choose, of their own free will. If people act well from fear of punishment, then we may have an orderly and controlled society, but not a free one. And if people only do good because they expect a reward, say, heaven, we're no better off. Only when people freely choose to do good for no other reason than that it is right to do so, only then do we reach anything like an ideal. Doing good is its own reward. This is the 'repenting' of Christian thought—do you know that 'repent' means to 'think again' or to 'turn to a new direction'? This is the mystery of being born again—the mystery expressed by the phrase 'and the light shines in the darkness, and the darkness grasp it not' or by 'the way' of Taoism."

She paused for breath, while Martin muttered that she was a "good soul."

"I'm not the unsophisticated person you might think. You see, years ago I worked in a big-city women's shelter. I saw horrors there—women abused, beaten, raped, and worse. Doing good, doing what's right, requires constant awareness and work—more work than many in society want to expend."

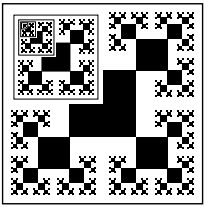
An inner part of Martin was stirred more than he would have thought possible. He dropped her off at her home, where as expected her mother soon was nearly hysterical even though Becky looked fine. He got promises from her mother to take care of her, to let him know if she needed anything. He drove home in an odd mood. She'd come to his office even after her injury. Did that mean anything? For six months he'd wondered if she really liked him, and maybe this was the answer. What did he want? Why not settle down?

The next day he brought her flowers—a trick his sister had taught him long ago. Becky disclaimed a need for flowers but was clearly pleased. She seemed chagrined, even embarrassed. “Sorry for the bad mood yesterday. I’m not usually so … pessimistic. I don’t really think people are mainly evil. Most people are filled with light—a glow from the inside if you look for it.”

To Martin she looked like an innocent from some modern garden of Eden. He’d heard that metaphor used for honeybees, those industrious gatherers of nectar, who make honey and wax, who are fierce in their swarming and stinging, and are devoted to their queen. Once, these bees were thought to be divine, perfect creatures escaped from Eden. And was Becky such a creature? No, just romantic nonsense, Martin said to himself firmly, and old-fashioned science, too. For a biologist sees a honeybee hive as a single social organism weighing a kilogram or so; to the computer scientist these bees illustrate complexity emerging from many simpler parts, and control from below.

And what about Becky? She wasn’t perfect—just superior to him. Why would someone like her want him with his faults? But maybe she did. He’d been a fool for too long, drifting, dawdling. It was time to rethink his life, take charge of his future.

So many possibilities and choices and decisions lay ahead. And even with accumulated wisdom, reason, and inspiration, even with access to information, privacy, and free speech, and with tools like simulation, one could only see a little way through the haze, just enough to try for an upward path.



References

Even in this new online world there is still a place for careful scholarly references in many works, as for example in a study putting forward a new interpretation or a better understanding of some historical event. For speculative books like this one that cover current issues, references to printed material are often out of date before anyone reads the words. An immense amount of material is online covering the topics of this book, and it is constantly growing and changing.

I propose to give some useful references here, assuming that the reader will turn to the internet for more detailed material.

A URL in a printed book is particularly annoying because it has to be exactly entered into a computer. Instead I will maintain a web page giving current references, including especially links to material.

Preface, page ix.

Libraries and the internet are saturated with information about utopias, about Thoreau, and about B.F. Skinner.

For information about communities based on Skinner's *Walden Two*, see the excellent book *Living Walden Two: B.F. Skinner's Behaviorist Utopia and Experimental Communities,* Hilke Kuhlmann, University of Illinois Press, 2005. This book includes a thorough discussion of Skinner's novel, with praise and criticism of it, and an overview of Skinner's ideas and work. The bulk of the book describes the only two attempts at societies modeled after his book that were successful enough to still exist.

Another good source about Skinner is Daniel Bjork's 1993 biography, where he discusses Skinner's interest in *Walden* as a young man. Initially Skinner called his book "The Sun Is But a Morning Star," the very last sentence of Thoreau's book.

Children, especially boys, are notorious for starting fires. It's interesting that in American people uniformly teach that fires are very dangerous and that no young person should ever start a fire or even touch matches, whereas in parts of Europe young children are deliberately taught how to use matches and start fires.

1. Introduction, page 1.

Durkheim and his theories are covered in most sociology books, and in fact in the late 1800s he popularized the word "sociology" for a field distinct from philosophy. Good English translations from French of his books are readily available, along with a great deal of online material.

By far the best book about the challenges humanity faces in the twenty-first century is: *Collapse: How Societies Choose to Fail or Succeed*, by Jared Diamond, Penguin, 2006, 2011. This excellent book is comprehensive, with a large list of "Further Readings" at the end.

Diamond lists 12 environmental problems that could lead to collapse (referred to in Chapter 1). Eight problems affecting past societies: "deforestation and habitat destruction, soil problems (erosion, salinization, and soil fertility losses), water management problems, overhunting, overfishing, effects of non-native species on native species, human population growth, increased per-capita impact of people." Four new problems: "human-caused climate change, buildup of toxic chemicals in the environment, energy shortages, and full human utilization of the Earth's photosynthetic capacity."

The full title of Kevin Kelly's book is: *Out of Control: The New Biology of Machines, Social Systems, & the Economic World,* Basic Books, 1995. Kelly is talking about distributed control or control from below, which certainly works for some interesting systems, especially biological ones. In this book I'm worried about human activities that are out of control, including especially those leading to climate change, and the climate change itself.

The quote from Orwell comes from his novel *1984.* Orwell's famous essay *Politics and the English Language* rails against deliberately softened words used for hard realities, as when War Depart-

ments had the "War" replaced by "Defense." People are no longer "fired" from a job, but are detached in a number of pleasant-sounding ways. An extreme recent example involved an airline passenger forcefully removed to allow airline employees to travel; the head of the airline used the word "re-accommodate" for this. Even scribes rewriting parables by Jesus in the Bible would soften and weaken the language. People have been fascinated with the idea that language determines thought.

"For example, given an amount of feed for beef stock, the weight of edible beef produced is four percent of the total weight of the feed." This comes from: "CrossTalk: Why Chicken Rules," by Vaclav Smil, *IEEE Spectrum*, Jan 2020, pp. 18-19.
For chicken the value is 15 percent.
Another figure: Units of feed per unit of edible meat: Chicken: 3-4, Beef: 20-30.

Thanks

Index

Author

Neal R. Wagner recently retired as Associate Professor of Computer Science from the University of Texas at San Antonio. In addition to UTSA, he taught at the University of Texas at El Paso, the University of Houston, and Drexel University.

He received a PhD degree in mathematics from the University of Illinois at Urbana-Champaign. He taught and did research in that area for several years until he turned to the Dark Side (computers).

He then specialized in cryptography and database security, with thirty scientific articles published. He received grants from several sources, including the National Science Foundation.

He is best known for early work on digital fingerprints and for discovering a specialized approach to create public-key cryptosystems based on the word problem for groups.

He studied for a year at the Universität Hamburg, and for two years he worked on realtime simulations of the Space Shuttle at NASA's Johnson Space Center.

At present he is working on a non-fiction book:

Seeking the Superman: No Need For Heroes,

and a science fiction novel:

The Moon has its Dark Side.