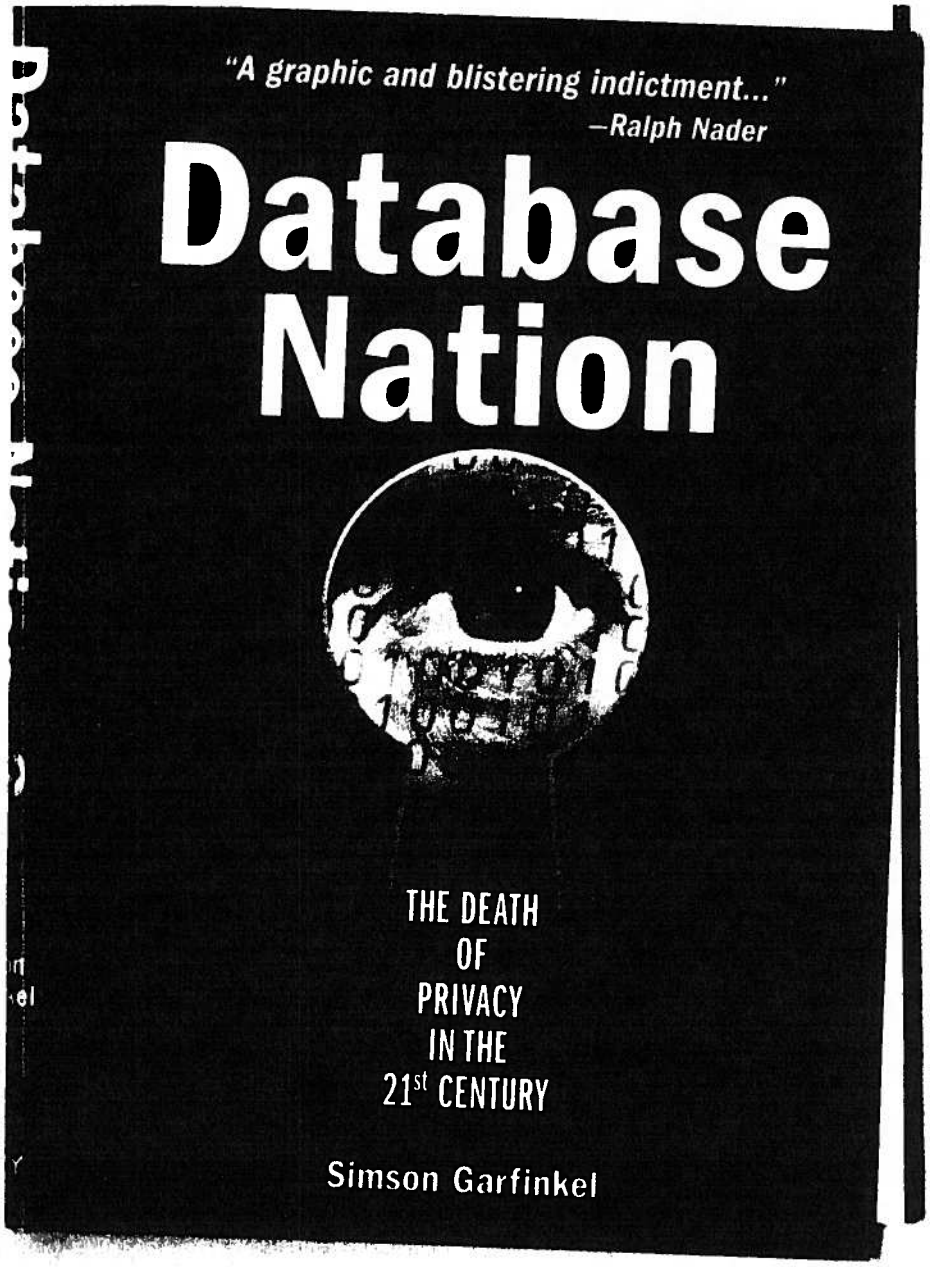

CHAPTER ONE

PRIVACY UNDER ATTACK

You wake to the sound of a ringing telephone—but how could that happen?

Several months ago, you reprogrammed your home telephone system so the phone would never ring before the civilized hour of 8:00 a.m. But it's barely 6:45 a.m. Who could be calling at this time? More importantly, who was able to bypass your phone's programming?

You pick up the telephone receiver, then slam it down a moment later. It's one of those marketing machines playing a prerecorded message. Computerized telemarketing calls have been illegal within the United States for more than a decade now, but ever since international long-distance prices dropped below 10 cents a minute, calls have been pouring in to North America from all over the world. And they're nearly all marketing calls—hence the popularity of programmable phones today. What's troubling you now is how this call got past the filters you set up. Later on, you'll discover how: the company that sold you the phone created an undocumented "back door"; last week, the phone codes were sold in an online auction. Because you weren't paying attention, you lost the chance to buy back your privacy.

Oops.

Now that you're awake, you decide to go through yesterday's mail. There's a letter from the neighborhood hospital you visited last month. "We're pleased that our emergency room could serve you in your time of need," the letter begins. "As you know, our fees (based on our agreement with your HMO) do not cover the cost of treatment. To make up the difference, a number of hospitals have started selling patient records to medical researchers and consumer marketing firms. Rather than mourn this distasteful behavior, we have decided to ask you to help us make up the difference. We are recommending a tax deductible contribution of $2[illegible] to help defray the cost of your visit."

The veiled threat isn't empty, but you decide you don't really care who finds out about your sprained wrist. You fold the letter in half and drop it

into your shredder. Also into the shredder goes a trio of low-interest credit card offers.

Why a shredder? A few years ago you would have never thought of shredding your junk mail—until a friend in your apartment complex had his identity "stolen" by the building's superintendent. As best as anybody can figure out, the super picked one of those preapproved credit-card applications out of the trash, called the toll-free number, and picked up the card when it was delivered. He's in Mexico now, with a lot of expensive clothing and electronics, all at your friend's expense.

On that cheery note, you grab your bag and head out the door, which automatically locks behind you.

When you enter the apartment's elevator, a hidden video camera scans your face, approves your identity, and takes you to the garage in the basement. You hope nobody else gets in the elevator—you don't relish a repeat of what happened last week to that poor fellow in 4G. It turns out that a neighbor recently broke up with her violent boyfriend and got a restraining order against him. Naturally, the elevator was programmed to recognize the man and, if he was spotted, to notify the police and keep the doors locked until they arrived. Too bad somebody else was in the elevator when it happened. Nobody realized the boyfriend was an undiagnosed (and claustrophobic) psychotic. A hostage situation quickly developed. Too bad for Mr. 4G. Fortunately, everything was captured on videotape.

Your car computer suggests three recommended approaches to your office this morning. You choose wrong, and a freak accident leaves you tied up in traffic for more than half an hour. As you wait, the computer plays an advertisement for a nearby burger joint every five minutes. You can't turn it off, of course: your car computer was free, paid for by the advertising.

Arriving late at work, you receive a polite email message from the company's timecard system; it knows when you showed up, and it gives you several options for making up the missed time. You can forgo lunch today, work an extra 45 minutes this evening, or take the 45 minutes out of your ever-dwindling vacation time. The choice is yours.

You look up and force a smile. A little video camera on your computer screen records your smile and broadcasts it to your boss and your coworkers. They've told you that Workplace Video Wallpaper™ builds camaraderie—but the company that sells the software also claims that the pervasive monitoring cuts down on workplace violence, romances, and even drug use. Nowadays, everybody smiles at work—it's too dangerous to do otherwise.

The cameras are just one of the ways you're being continually monitored at work. It started with electronic tags in all the company's books and magazines, designed to stop the steady pilferage from the library. Then, in

the aftermath of a bomb scare, employees were told they'd have to wear badges at all times, and that desks and drawers would be subject to random searches. (Rumor has it that the chief of security herself called in the bomb threat—a ploy to justify the new policies.)

Next month, the company is installing devices in the bathrooms to make sure people wash their hands. Although the devices were originally intended for the healthcare and food industries, a recent study found that routine washing can also cut down on disease transmission among white-collar workers. So the machines are coming, and with them you'll lose just a little bit more of your privacy and your dignity.

This is the future—not a far-off future, but one that's just around the corner. It's a future in which what little privacy we now have will be gone. Some people call this loss of privacy "Orwellian," harking back to *1984*, George Orwell's classic work on privacy and autonomy. In that book, Orwell imagined a future in which privacy was decimated by a totalitarian state that used spies, video surveillance, historical revisionism, and control over the media to maintain its power. But the age of monolithic state control is over. The future we're rushing towards isn't one where our every move is watched and recorded by some all-knowing "Big Brother." It is instead a future of a hundred kid brothers that constantly watch and interrupt our daily lives. George Orwell thought that the Communist system represented the ultimate threat to individual liberty. Over the next 50 years, we will see new kinds of threats to privacy that don't find their roots in totalitarianism, but in capitalism, the free market, advanced technology, and the unbridled exchange of electronic information.

WHAT DO WE MEAN BY PRIVACY?

The concept of privacy is central to this book, yet I wish I had a better word to express the aspect of individual liberty that is under attack by advanced technology as we enter the new millennium.

For decades, people have warned that pervasive databanks and surveillance technology are leading inevitably to the death of privacy and democracy. But these days, many people who hear the word "privacy" think about those kooks living off in the woods with their shotguns: these folks get their mail at post office boxes registered under assumed names, grow their own food, use cash to buy what they can't grow for themselves, and constantly worry about being attacked by the federal government—or by space aliens. If you are not one of these people, you may well ask, "Why should I worry about my privacy? I have nothing to hide."

The problem with this word "privacy" is that it falls short of conveying the really big picture. Privacy isn't just about hiding things. It's about self-possession, autonomy, and integrity. As we move into the computerized world of the twenty-first century, privacy will be one of our most important civil rights. But this right of privacy isn't the right of people to close their doors and pull down their window shades—perhaps because they want to engage in some sort of illicit or illegal activity. It's the right of people to control what details about their lives stay inside their own houses and what leaks to the outside.

To understand privacy in the next century, we need to rethink what privacy really means today:

- It's not about the man who wants to watch pornography in complete anonymity over the Internet. It's about the woman who's afraid to use the Internet to organize her community against a proposed toxic dump—afraid because the dump's investors are sure to dig through her past if she becomes too much of a nuisance.
- It's not about people speeding on the nation's highways who get automatically generated tickets mailed to them thanks to a computerized speed trap. It's about lovers who will take less joy in walking around city streets or visiting stores because they know they're being photographed by surveillance cameras everywhere they step.
- It's not about the special prosecutors who leave no stone unturned in their search for corruption or political misdeeds. It's about good, upstanding citizens who are now refusing to enter public service because they don't want a bloodthirsty press rummaging through their old school reports, computerized medical records, and email.
- It's not about the searches, metal detectors, and inquisitions that have become a routine part of our daily lives at airports, schools, and federal buildings. It's about a society that views law-abiding citizens as potential terrorists, yet does little to effectively protect its citizens from the real threats to their safety.

Today, more than ever before, we are witnessing the daily erosion of personal privacy and freedom. We're victims of a war on privacy that's being waged by government eavesdroppers, business marketers, and nosy neighbors.

Most of us recognize that our privacy is at risk. According to a 1996 nationwide poll conducted by Louis Harris & Associates, one in four Americans (24%) has "personally experienced a privacy invasion"[1] —up from 19% in 1978. In 1995, the same survey found that 80% of

Americans felt that "consumers have lost all control over how personal information about them is circulated and used by companies."[2] Ironically, both the 1995 and 1996 surveys were paid for by Equifax, a company that earns nearly two billion dollars each year from collecting and distributing personal information.

We know our privacy is under attack. The problem is that we don't know how to fight back.

The Role of Technology

Today's war on privacy is intimately related to the dramatic advances in technology we've seen in recent years. As we'll see time and again in this book, unrestrained technology ends privacy. Video cameras observe personal moments; computers store personal facts; and communications networks make personal information widely available throughout the world. Although some specialty technology may be used to protect personal information and autonomy, the overwhelming tendency of advanced technology is to do the reverse.

Privacy is fundamentally about the power of the individual. In many ways, the story of technology's attack on privacy is really the story of how institutions and the people who run them use technology to gain control over the human spirit, for good and ill. That's because technology by itself doesn't violate our privacy or anything else: it's the people using this technology and the policies they carry out that create violations.

Many people today say that in order to enjoy the benefits of modern society, we must necessarily relinquish some degree of privacy. If we want the convenience of paying for a meal by credit card, or paying for a toll with an electronic tag mounted on our rear view mirror, then we must accept the routine collection of our purchases and driving habits in a large database over which we have no control. It's a simple bargain, albeit a Faustian one.

I think this tradeoff is both unnecessary and wrong. It reminds me of another crisis our society faced back in the 1950s and 1960s—the environmental crisis. Then, advocates of big business said that poisoned rivers and lakes were the necessary costs of economic development, jobs, and an improved standard of living. Poison was progress: anybody who argued otherwise simply didn't understand the facts.

Today we know better. Today we know that sustainable economic development *depends* on preserving the environment. Indeed, preserving the environment is a prerequisite to the survivability of the human race. Without clean air to breathe and clean water to drink, we will all surely die. Similarly, in order to reap the benefits of technology, it is

more important than ever for us to use technology to protect personal freedom.

Blaming technology for the death of privacy isn't new. In 1890, two Boston lawyers, Samuel Warren and Louis Brandeis, argued in the *Harvard Law Review* that privacy was under attack by "recent inventions and business methods." They contended that the pressures of modern society required the creation of a "right of privacy," which would help protect what they called "the right to be let alone."[3] Warren and Brandeis refused to believe that privacy had to die for technology to flourish. Today, the Warren/Brandeis article is regarded as one of the most influential law review articles ever published.[4] And the article's significance has increased with each passing year, as the technological invasions that worried Warren and Brandeis have become more commonplace.

Privacy-invasive technology does not exist in a vacuum, of course. That's because technology itself exists at a junction between science, the market, and society. People create technology to fill specific needs, real or otherwise. And technology is regulated, or not, as people and society see fit.

Few engineers set out to build systems designed to crush privacy and autonomy, and few businesses or consumers would willingly use or purchase these systems if they understood the consequences. What happens more often is that the privacy implications of a new technology go unnoticed. Or if the privacy implications are considered, they are misunderstood. Or if they are understood correctly, errors are made in implementation. In practice, just a few mistakes can turn a system designed to protect personal information into one that destroys our secrets.

How can we keep technology and the free market from killing our privacy? One way is by being careful and informed consumers. But I believe that government has an equally important role to play.

THE ROLE OF GOVERNMENT

With everything we've heard about Big Brother, how can we think of government as anything but the enemy of privacy? While it's true that federal laws and actions have often damaged the cause of privacy, I believe that the federal government may be our best hope for privacy protection as we move into the new millennium.

The biggest privacy failure of American government has been its failure to carry through with the impressive privacy groundwork that was laid in the Nixon, Ford, and Carter administrations. It's worth taking a look back at that groundwork and how it may serve us today.

The 1970s were a good decade for privacy protection and consumer rights. In 1970, Congress passed the Fair Credit Reporting Act. Elliot Richardson, who at the time was President Nixon's secretary of health, education, and welfare (HEW), created a commission in 1970 to study the impact of computers on privacy. After years of testimony in Congress, the commission found all the more reason for alarm and issued a landmark report in 1973.

The most important contribution of the Richardson report was a bill of rights for the computer age, which it called the Code of Fair Information Practices (see the shaded box). That Code remains the most significant American thinking on the topic of computers and privacy to this day.

CODE OF FAIR INFORMATION PRACTICES

The Code of Fair Information Practices is based on five principles:

- There must be no personal data record-keeping systems whose very existence is secret.
- There must be a way for a person to find out what information about the person is in a record and how it is used.
- There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
- There must be a way for a person to correct or amend a record of identifiable information about the person.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

Source: Department of Health, Education, and Welfare, 1973.

The biggest impact of the HEW report wasn't in the United States, but in Europe. In the years after the report was published, practically every European country passed laws based on these principles. Many created data protection commissions and commissioners to enforce the laws.[5] Some believe that one reason for this interest in electronic privacy was Europe's experience with Nazi Germany in the 1940s. Hitler's secret police used the records of governments and private organizations in the countries he invaded to round up people who posed the greatest threat to the German occupation; postwar Europe

realized the danger of allowing potentially threatening private information to be collected, even by democratic governments that might be responsive to public opinion.

But here in the United States, the idea of institutionalized data protection faltered. President Jimmy Carter showed interest in improving medical privacy, but he was quickly overtaken by economic and political events. Carter lost the election of 1980 to Ronald Reagan, whose aides saw privacy protection as yet another failed Carter initiative. Although several privacy protection laws were signed during the Reagan/Bush era, the leadership for these bills came from Congress, not the White House. The lack of leadership stifled any chance of passing a nationwide data protection act.

In fact, while most people in the federal government were ignoring the cause of privacy, some were actually pursuing an antiprivacy agenda. In the early 1980s, the federal government initiated numerous "computer matching" programs designed to catch fraud and abuse. (Unfortunately, because of erroneous data, these programs often penalized innocent individuals.[6]) In 1994, Congress passed the Communications Assistance to Law Enforcement Act, which gave the government dramatic new powers for wiretapping digital communications. In 1996, Congress passed a law requiring states to display Social Security numbers on driver's licenses, and another law requiring that all medical patients in the U.S. be issued unique numerical identifiers, even if they paid their own bills. Fortunately, the implementation of those 1996 laws has been delayed, largely thanks to a citizen backlash.

Continuing the assault, both the Bush and Clinton administrations waged an all-out war against the rights of computer users to engage in private and secure communications. Starting in 1991, both administrations floated proposals for use of "Clipper" encryption systems that would have given the government access to encrypted personal communications. President Clinton also backed the Communications Decency Act (CDA), which made it a crime to transmit sexually explicit information to minors—and, as a result, might have required Internet providers to deploy far-reaching monitoring and censorship systems. When a court in Philadelphia found the CDA unconstitutional, the Clinton administration appealed the decision all the way to the Supreme Court—and lost.

Finally, the U.S. government's restrictions on the export of encryption technology have effectively restrained the widespread use of this technology for personal privacy protection within the United States.

As we move forward into the twenty-first century, the United States needs to take personal privacy seriously again. The final chapter of this book explores ways our government might get back on track, and suggests a federal privacy agenda for the twenty-first century.

FIGHTING BACK

Privacy is certainly on the ropes in America today, but so was the environment in 1969. Thirty years ago, the Cuyahoga River in Ohio caught on fire and Lake Erie was proclaimed dead. Times have certainly changed. Today it's safe to eat fish that are caught in the Cuyahoga, Lake Erie is alive again, and the overall environment in America is the cleanest it's been in decades.

There are signs around us indicating that privacy is getting ready to make a comeback as well. The war against privacy is commanding more and more attention in print, on television, and on the Internet. People are increasingly aware of how their privacy is compromised on a daily basis. Some people have begun taking simple measures to protect their privacy, measures like making purchases with cash and refusing to provide their Social Security numbers—or providing fake ones. And a small but growing number of people are speaking out for technology *with* privacy, and putting their convictions into practice by developing systems or services that protect, rather than attack, our privacy.

Over the past few decades, we've learned that technology is flexible, and that when it invades our privacy, the invasion is usually the result of a conscious choice. We now know, for instance, that when a representative from our bank says:

> I'm sorry that you don't like having your Social Security number printed on your bank statement, but there is no way to change it.

that representative is actually saying:

> Our programmers made a mistake by telling the computer to put your Social Security number on your bank statement, but we don't think it's a priority to change the program. Take your business elsewhere.

Today we are relearning this lesson and discovering how vulnerable business and government can be to public pressure. Consider these three examples from the past decade:

Lotus Development Corporation. In 1990, Lotus and Equifax teamed up to create a CD-ROM product called "Lotus Marketplace: Households" that would have included names, addresses, and demographic information on every household in the United States, so small businesses could do the same kind of target marketing that big businesses have been doing since the 1960s. The project was canceled when more than 30,000 people wrote to Lotus demanding that their names be taken out of the database.

Lexis-Nexis. In 1996, Lexis-Nexis suffered an embarrassing public relations debacle when it was revealed that their P-TRAK database service was publishing the Social Security numbers of most U.S. residents. Thousands of angry consumers called the company's switchboard, effectively shutting it down for a week. Lexis-Nexis discontinued the display of Social Security numbers 11 days after the product was introduced.

Social Security Administration (SSA). In 1997, it was the U.S. Social Security Administration's turn to suffer the public's wrath. The press informed U.S. taxpayers that the SSA was making detailed tax history information about them available over the Internet. The SSA argued that its security provisions—requiring that taxpayers enter their name, date of birth, state of birth, and mother's maiden name—were sufficient to prevent fraud. But tens of thousands of Americans disagreed, several U.S. senators investigated the agency, and the service was promptly shut down. When the service was reactivated some months later, the detailed financial information could not be downloaded over the Internet.

Technology is not autonomous; it simply empowers choices made by government, business, and individuals. One of the big lessons of the environmental movement is that it's possible to shape these choices through the political process. This, I believe, justifies the involvement of government on the privacy question.

WHY THIS BOOK?

In this book we'll take a look at today's wide-ranging—and frightening—threats to our personal privacy:

The end of due process. Governments and businesses went on a computer buying spree in the second half of the twentieth century, replacing billions of paper files with electronic data processing systems. Today, humans often are completely absent from digital decision making. As a result, we've created a world in which the smallest clerical errors can have devastating effects on a person's life. It's a world where computers are assumed to be correct, and people wrong.

The fallibility of biometrics. Fingerprints, iris scans, and genetic sequences are widely regarded as infallible techniques for identifying human beings. They're so good, in fact, that 50 years from now, identification cards and passports probably won't exist. Instead, a global data network will allow anyone on the planet to be instantly identified from the unique markings of that person's own body. Who controls

access to the databank, who has the power to change its contents, and what do we do if the infallible system is nevertheless wrong?

The systematic capture of everyday events. We are entering a new world in which every purchase we make, every place we travel, every word we say, and everything we read is routinely recorded and made available for later analysis. But while the technology exists to capture this data, we lack the wisdom to figure out how to treat it fairly and justly. The result is an unprecedented amount of data surveillance, the effects of which we're just beginning to grasp.

The bugging of the outside world. Orwell thought the ultimate threat to privacy would be the bugging of bedrooms and offices. Today, an equally large threat to freedom is the systematic monitoring of public places through microphones, video cameras, surveillance satellites, and other remote sensing devices, combined with information processing technology. Soon it may be impossible for most people to escape the watchful outdoor eye.

The misuse of medical records. Traditionally, medical records have been society's most tightly held personal records. The obligation to maintain patient confidentiality is widely regarded as a fundamental responsibility of medical professionals. But patient confidentiality is at odds with the business of health insurance—a business that would rather turn away the sick than cure them.

Runaway marketing. Junk mail, junk faxes, junk email, and telemarketing calls during dinner are only the beginning of the twenty-first century's runaway marketing campaigns. Marketers increasingly will use personal information to create solicitations that are continual and virtually indistinguishable from news articles, personal letters, and other kinds of noncommercial communications.

Personal information as a commodity. Personal identification information—your name, your profession, your hobbies, and the other bits that make up your self—is being turned into a valuable property right. But instead of being given to individuals to help them exert control over their lives, this right is being seized by big business to ensure continued profits and market share. If you don't even own your own name, how can you have a sense of self-worth?

Genetic autonomy. Breakthrough advances in genetics make it possible to predict disease, behavior, intelligence, and many other human traits. Whether or not these predictions are correct, they will change how people are perceived and treated. Will it be possible to treat people fairly and equally if there is irrefutable scientific evidence that

people have different strengths, different weaknesses, and different susceptibilities to disease? If not, how is it possible to maintain a democratic society when this information is easily available?

The micromanagement of intellectual property. Businesses are becoming increasingly vigilant in detecting the misuse of their own intellectual property. But piracy is hard to prevent when technology can turn every consumer into an electronic publisher. To prevent info-theft, publishers are turning to increasingly intrusive techniques for spying on their customers. Once this technology is in place, it is unlikely that it will be restricted to antipiracy protection.

The individual as terrorist. Astonishingly lethal technologies are now widely available throughout society. How can society reasonably protect itself from random acts of terrorism without putting everyone under surveillance? How can society protect itself from systematic abuses by law enforcement officials, even when those abuses seem to be in the public interest?

Intelligent computing. The ultimate threat to privacy will be intelligent computers—machines that can use human-like reasoning powers, combined with blinding calculating speed, to assemble coherent data portraits, interpret and anticipate our mental states, and betray us with false relationships.

This is a broad collection of issues, but it's no less broad than the future itself. This book's purpose is to show the privacy implications of many ongoing technological developments, and to show good cause for abandoning today's laissez-faire approach to privacy protection. Once you have a good vision of the technological future we're shaping, you'll be better equipped to mold it.

Although this book is subtitled *The Death of Privacy in the Twenty-First Century*, it is designed to bring about a different end. Nearly 40 years ago, Rachel Carson's book *Silent Spring* helped seed the U.S. environmental movement. And to our credit, the silent spring that Carson foretold never came to be. *Silent Spring* was successful because it helped people to understand the insidious damage that pesticides were wreaking on the Earth's environment, and it helped our society and our planet plot a course to a better future.

This book, likewise, seeks to show the plethora of ways that technology is killing one of our most cherished freedoms. Whether you call this freedom the right to digital self-determination, the right to informational autonomy, or simply the right to privacy, the shape of our future will be determined in large part by how we understand, and ultimately how we control or regulate, the threats to this freedom that we face today.

CHAPTER TWO

DATABASE NATION

WASHINGTON, DC, 1965. The Bureau of the Budget's proposal was simple yet revolutionary. Instead of each federal agency's investing in computers, storage technology, and operations personnel, the United States government would build a single National Data Center. The project would start by storing records from four federal agencies: population and housing data from the Bureau of the Census; employment information from the Bureau of Labor Statistics; tax information from the Internal Revenue Service; and benefit information from the Social Security Administration. Eventually, it would store far more.

While the original motivation was simply to cut costs, it soon became clear that there would be additional benefits. Accurate statistics could be created quickly and precisely from the nation's data. By building a single national database, the government could track down and stamp out the misspelled names and other inconsistent information that haunts large-scale databank projects. A single database would also let government officials and even outsiders use the data in the most efficient manner possible.

The Princeton Institute for Advanced Study issued a report enthusiastically supporting the databank project, saying that centralized storage of the records could actually improve the security of the information, and therefore the privacy of the nation. Carl Kaysen, the Institute's director and the chairman of the study group, further urged that Congress pass legislation that would give the records additional protections, provide for privacy, and promote accountability of the databank workers. Others latched on to the idea, and the concept of the National Data Center slowly evolved into that of a massive databank containing cradle-to-grave electronic records for every U.S. citizen. The database would contain every person's electronic birth certificate, proof of citizenship, school records, draft registration and military service, tax records, Social Security benefits, and ultimately, their death