# AMERICA THE VULNERABLE

*Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*

JOEL BRENNER

THE PENGUIN PRESS
NEW YORK
2011

# AMERICA THE VULNERABLE

*Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*

JOEL BRENNER

THE PENGUIN PRESS
NEW YORK
2011

# AMERICA THE VULNERABLE

*Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*

JOEL BRENNER

THE PENGUIN PRESS
NEW YORK
2011

# Table of Contents

*Title Page*
*Copyright Page*
*Dedication*
*Introduction*

Chapter 1 - ELECTRONICALLY UNDRESSED
Chapter 2 - A PRIMER ON CYBER CRIME
Chapter 3 - BLEEDING WEALTH
Chapter 4 - DEGRADING DEFENSE
Chapter 5 - DANCING IN THE DARK
Chapter 6 - BETWEEN WAR AND PEACE
Chapter 7 - JUNE 2017
Chapter 8 - SPIES IN A GLASS HOUSE
Chapter 9 - THINKING ABOUT INTELLIGENCE
Chapter 10 - MANAGING THE MESS

*Acknowledgements*
*NOTES*
*A ( VERY) SELECT BIBLIOGRAPHY*
*INDEX*

THE PENGUIN PRESS
Published by the Penguin Group
Penguin Group (USA) Inc., 375 Hudson Street, New York, New York 10014, U.S.A. ● Penguin Group (Canada), 90 Eglinton Avenue East, Suite 700, Toronto, Ontario, Canada M4P 2Y3 (a division of Pearson Penguin Canada Inc.) Penguin Books Ltd, 80 Strand, London WC2R 0RL, England Penguin Ireland, 25 St. Stephen's Green, Dublin 2, Ireland (a division of Penguin Books Ltd) Penguin Books Australia Ltd, 250 Camberwell Road, Camberwell, Victoria 3124, Australia (a division of Pearson Australia Group Pty Ltd) Penguin Books India Pvt Ltd, 11 Community Centre, Panchsheel Park, New Delhi–110 017, India Penguin Group (NZ), 67 Apollo Drive, Rosedale, Auckland 0632, New Zealand division of Pearson New Zealand Ltd) Penguin Books (South Africa) (Pty) Ltd, 24 Sturdee Avenue, Rosebank, Johannesburg 2196, South Africa

Penguin Books Ltd, Registered Offices
80 Strand, London WC2R ORL, England

First published in 2011 by The Penguin Press,
a member of Penguin Group (USA) Inc.



Portions of Chapter 10 appeared in "Privacy and Security: Why Isn't Cyberspace More Secure?" by Joel Brenner, *Communications of the ACM*, November 2010.

LIBRARY OF CONGRESS CATALOGING IN PUBLICATION DATA
Brenner, Joel.
America the vulnerable : inside the new threat matrix of digital espionage, crime, and warfare / Joel Brenner.
p. cm.
Includes bibliographical references and index.
ISBN : 978-1-101-54783-0
1. Computer crimes—United States—Prevention. 2. Internet in espionage—United States. 3. National security—United States. I. Title.
HV6773.2.B74 2011
364.16'80973—dc23
2011019801

*For Victoria*

# INTRODUCTION

HOW DID THE Chinese manage to remotely download up to twenty terabytes of information from th Defense Department—equal to about 20 percent of all the data in the Library of Congress? And why don't we know exactly what they took? How did WikiLeaks get its hands on classified diplomatic cables, and why hasn't the U.S. government been able to shut it down? How did the specifications for the avionics and armor on the president's helicopter end up in Tehran, and what has that got to do wit the theft of Supreme Court Justice Stephen Breyer's private data from his investment adviser? The answers to these questions reveal alarming threats to our personal, corporate, and national security that come from a new type of espionage and from the sudden transparency that electronic connectivit has brought to all aspects of our lives. Your difficulties with electronic privacy, the electronic theft o America's cutting-edge technology, and the government's loss of state secrets are a lot more alike than you know.

I spent most of the first decade of the twenty-first century working at the heart of the U.S. government's efforts to thwart spying and terrorism against us, first as inspector general of the National Security Agency, and then as chief of counterintelligence for the director of National Intelligence. As I carried out these assignments, I saw plenty of the old-fashioned kind of espionage, but I also witnessed the dramatic rise of a new kind of spying that exploits digital technology itself, and the fact that we have all come to rely so thoroughly on that technology.

During my tenure in government I came to understand how steeply new technology has tipped the balance in favor of those—from freelance hackers to Russian mobsters to terrorists to states like China and Iran—who want to learn the secrets we keep, whether for national, corporate, or personal security. Much of my understanding arose from classified work that I cannot discuss here or anywhere. But I can share the insights I gleaned about this new form of espionage: how it works; wha the biggest and most vulnerable targets are; who does it best; as well as what it means for the future o warfare, intelligence, market competition, and society at large. I also came to understand what we ca —and cannot—do to counter this flood of espionage.

The truth I saw was brutal and intense: Electronic thieves are stripping us blind. I'm not just talkin about the pirating of DVDs and movies in Asia or somebody ripping off your Social Security number That's bad enough, but it's worse than that. Technologies that cost millions or billions to develop are being bled out of our corporate laboratories via the Internet; or they're slipping out after hours on thumb drives, walking onto airplanes bound for foreign ports, and reentering the country as finished products developed by foreign entrepreneurs. In effect, we're buying back our own technology. Other Western firms, meanwhile, are bleeding trade secrets, engineering designs, know-how, and other intellectual property through electronic leakage. In the public sector, sensitive diplomatic cables are suddenly splashed across the headlines worldwide. The same organizations that broadcast those cable gleefully distribute lists of critical infrastructure—airports, bridges, chemical plants—that are the most vulnerable to attack. And as I describe in the pages that follow, we're losing strategically sensitive data about aircraft and ship design, radars, and other defense technology, as well as information about auto manufacturing, engineering designs, and other commercial innovations. This theft contributes to the tidal flow of capital from West to East that threatens our prosperity, and it could in wartime cost many American lives.

This kind of theft is targeted and systematic. The U.S. Navy spent about $5 billion to develop a quiet electric drive for its submarines and ships so they'd be silent and hard to track.[1] Chinese spies stole it. The navy spent billions more to develop new radar for their top-of-the-line Aegis Cruiser. Chinese spies stole that, too. The electronic intelligence services of the Chinese and the Russians are working us over—taking advantage of our porous networks and indifference to security to steal billions of dollars' worth of military and commercial secrets. Some of our allies, like the French and the Israelis, have tried it too.

Pentagon information systems have been under attack since at least 1998. In August 2006, Major General William Lord of the air force let the public in on the secret when he mentioned that massive heist of up to twenty terabytes. To carry this volume of documents in paper form, you'd need a line o moving vans stretching from the Pentagon to the Chinese freighters docked in Baltimore harbor fifty miles away. If the Chinese tried to do that, we'd have the National Guard out in fifteen minutes. But when they did it electronically, hardly anyone noticed. As it happens, the data were stolen from the Pentagon's unclassified networks, but those networks hold lots of sensitive information—including the names and private identifying information of every man and woman in the U.S. armed forces.

It would be a serious mistake to think that the difference between classified and unclassified is the difference between important and unimportant, or sensitive and nonsensitive. Lots of information is sensitive but not classified, especially when it relates to technology and personnel. According to the air force's General Lord, when the Chinese pulled off this heist, they were "looking for your identity so they can get into the network as you."[2] General Lord did not reveal what is perhaps even more troubling: We don't know exactly what data were taken because the Defense Department doesn't bother to encrypt this kind of data. They thought it was too much trouble. But the Chinese, on their way out the electronic door, did encrypt it. Too much trouble? They didn't think so.

According to the Government Accountability Office, the number of unauthorized accesses or installations of malicious software on U.S. government computers increased by 650 percent since 2006.[3] The trend is disquieting, and the official data almost certainly undercounts the problem.

And this trend is hardly limited to the public sector. To give just one example of the magnitude of threat aimed at private companies: A sophisticated team of hackers broke into a Royal Bank of Scotland payroll system in late 2008 and stole information that let them counterfeit credit balances o ATM cards. They then mounted a coordinated attack on 139 ATMs in the United States, Canada, Russia, and China that netted about $9 million in thirty minutes. If this were a traditional bank robbery, it would rank as one of the largest in history. Chinese and Russian cyberoperators have mad advanced, persistent intrusions into the networks of other banks too—to what end, we don't yet know This kind of intrusion infects a system with malicious code that's difficult—sometimes even impossible—to wipe out, because it continually changes to evade detection. It opens electronic "trapdoors" so that outsiders can bypass the system's security, and if one door is nailed shut, the cod automatically opens another one. We don't even know who's doing this. This point will come up aga and again throughout this book, because our inability to figure out who's responsible for illegal behavior on our electronic networks is a fundamental reason why we can't safeguard our personal data, corporate intellectual property, or national defense secrets.

Nor can we ensure the safety of the infrastructure without which our world would collapse: electricity grids, financial systems, air-traffic control, and other networks. All these systems run electronically; all run on the same public telecommunications backbone; and increasingly all run on commercial, off-the-shelf hardware and software that can be bought anywhere in the world. Many of

these systems have already been penetrated by criminal gangs or foreign intelligence services—sometimes to steal, sometimes to reconnoiter for uncertain purposes—using offensive tools that are often more effective than our defenses. All of these systems could become targets for disruption in wartime or even during a lower-grade conflict like a diplomatic standoff.

These are all things I learned during my four and a half years as inspector general of the nation's electronic intelligence service, the National Security Agency, and my subsequent three years as head of U.S. counterintelligence. In the latter job I was responsible for strategy and policy coordination among the CIA, FBI, Defense Department, and other government departments and agencies. Counterintelligence is the business of dealing with foreign intelligence activities against our own intelligence services, military, and national security infrastructure. This business used to be concerne almost entirely with foreign spies, and that remains its core mission. But electronic espionage has increased exponentially since the mid-1990s, so counterintelligence has become deeply concerned with what's happening on—and to—the nation's electronic networks.

ONE MORNING ABOUT five months after 9/11, I was perched on a sofa in a large office on the top floor of a glass-enclosed building called OPS 2B, in Fort George G. Meade, Maryland, thirty miles north of Washington, answering questions from then Lieutenant General Michael V. Hayden, the director of the National Security Agency, and his then deputy William Black. They were interviewing me for the position of the NSA's inspector general. This is a nonpolitical, top-secret job at the top level of the intelligence community's version of the civil service. The IG is in charge of internal investigations, and he audits and inspects the agency's operations for fraud, abuse, and just plain inefficiency. Along with the head of security, he's one of the two people in any agency—especially a intelligence agency—you do not want darkening your doorway. Like most people, I'd rather be liked than disliked, but if you need to be liked, this job is not for you. By my early thirties, however, havin been an antitrust prosecutor, I was already used to lawyers for price fixers and monopolists accusing me of single-handedly destroying the U.S. economy. I knew what I'd be in for if I got the job.

A cordial man in his late fifties, Mike Hayden was unassuming even with three stars on each shoulder of his blue air force uniform. Hayden had run signals intelligence, or SIGINT, for the air force, and before that had flown countless hours in the windowless fuselage of unmarked airplanes, wearing earphones and collecting radio signals in Eastern Europe. He had also been deputy chief of staff to the four-star commander in Korea. But he was not a techie. Hayden had been the star pupil of the nuns and priests in an Irish Catholic neighborhood in Pittsburgh and had driven a taxi to work his way through Duquesne University, where he studied history, not engineering or computer science. He was ambitious, but he never forgot his Pittsburgh roots.

Black was a different type altogether. If you looked at an organization chart of the NSA at the time all the solid lines ran predictably to Hayden, the NSA director, or DIRNSA, and the dotted lines ran a over, but the invisible lines ran to a table in Bill Black's next-door office, where this bald, blunt character in cowboy boots summoned subordinates, pulled bureaucratic levers, and worked the phones. On the wall over his left shoulder he had hung a drawing of Wyatt Earp, so when you sat at h table you were staring down the barrel of Earp's Buntline Special. Bill was a bureaucratic operator, and many feared him. I liked him. He grew up on a ranch in New Mexico, and in the late stages of the cold war ran what was then called A Group. A Group was the NSA's main game: It was in charge of collecting signal intelligence against the Soviet Union. A dark master of electronic intelligence, Bill

knew every intelligence satellite in the sky and what it did, and every success and every blunder in th history of the NSA, which he loved deeply. He knew the wheels within the wheels. He also had a wellearned reputation as a tough SOB who wasn't afraid to make decisions. (In government, anybody who isn't afraid to make decisions is regarded as an SOB.) After 9/11, Hayden brought Black back from retirement, and the two of them were determined to steer the NSA out of the doldrums, budget slashing, and decline of the 1990s. They wanted an outsider as IG, someone not afraid to tell them th truth.

And so began my near nine-year journey into the belly of the intelligence beast, first at the NSA ar then running counterintelligence for the director of National Intelligence, where my biggest headache was cyberespionage in a world where everything was becoming electronically connected to everythin else. In those positions I had a hair-raising view of the incessant conflicts being waged in cyberspace —conflicts short of war but involving concerted attempts to penetrate our nation's information systems and critical infrastructure. Some of these conflicts could indeed turn into war, but the tendency to treat them as such is likely to lead us astray. In American law and politics, "war" and "peace" are presented as a binary toggle switch: We're either enjoying peace or waging war. In this view, in which the world is drawn with straight lines and right angles, peace and struggle cannot coexist. But the world is not so easily compartmentalized, and as I argue in this book, we are now in period, typical in international affairs, in which conflict and symbiosis, struggle and trade, exist side by side in a condition that is neither war nor peace, and which is both promising and dangerous.

Personal and organizational secrets all live on the same electronic systems. Gaming and social media technologies once thought to be solely for personal and entertainment uses are now at the fron edge of many business applications. Boundaries of many kinds are eroding—legally, behaviorally, electronically—in all aspects of our lives: between the public and private behaviors of ordinary people, for example, in the dress, speech, and decorum appropriate to the street, the office, or houses of worship; between what the government does and what privately owned companies do; and, not least, between nation-states and nonstate actors. Large corporations have police, military, and intelligence capabilities that are hardly distinguishable from those of most governments. Organizations like al-Qaeda, Lebanese Hezbollah, and the Russian mob operate across international borders with ease and have budgets that exceed those of many nation-states. Meanwhile, some of those nation-states are hardly more than lines on a map. Technical capabilities that a decade or two ago could be found only in advanced military aircraft—GPS, for example—now come standard in your rental car and can be bought at RadioShack for a few bucks. Computing capacity greater than governments could muster during the cold war now resides in mobile devices that fit in a pocket. The original iPhone, released in 2007, weighed a hundred times less than a portable computer from 1982, was five hundred times smaller, cost ten times less, and ran a hundred times faster.[4] There are now 5 *billion* handsets in use around the world, and three fourths of them are in the developing world.[5]

In the postindustrial West we think technology advances in the order in which it was invented—usually by us. Plumbing came before wired telephones and radio, which came before airplanes, whic came before penicillin, which came before television, and so on. But this isn't the way the rest of the world experiences modernity. Thirty years ago, approaching Lahore's airport in a Pakistan International Airlines Boeing 727, I watched out the window as a stick-wielding peasant prodded a buffalo tethered to a water wheel—a scene from biblical times. Ten years ago, in rural Yunnan Province, China, I stopped for lunch at a roadside restaurant where the ducks on the menu were slaughtered out back. The only toilet was an open-air hole in the ground, and a local businessman wa squatting over it while talking on a cell phone. Technology in the developing world is moving fast—

but not in the order we take for granted. People in the developing world may not have all the modern conveniences we do, but they do have the same digital technology and programming skills we do. An many of them have the skills to pick our electronic pockets.

The boundary between national and economic security is also eroding—has eroded, in fact, almost completely. When it comes to national security the boundary between public and corporate secrets ha also more or less vanished. The current U.S. National Security Strategy—that's the president's statement to Congress about the nation's principal security concerns—contains sixty-eight reference to economic issues.[6] The boundary between military and economic secrets remains firm in the law of Western nations, but the law is always trying to catch up with life. The technology our military relies on is mostly developed in the private sector, and most of the research it's based on is carried out in universities and private companies. The know-how of our engineering firms, the drugs that our pharmaceutical companies spend billions to develop, the trade secrets of our aerospace industry—these are the bases of our national welfare. Much of our infrastructure is also privately owned and subject to attack. Terrorists pilot jetliners indiscriminately into private office buildings as well as int the headquarters of government departments and blow up passenger trains in Russia and under the streets of London. As a result, the infrastructure, the technologies, and the information that governments must protect extend well beyond government property.

The Office of the National Counterintelligence Executive, which I headed from 2006 to 2009, is charged with protecting America's secrets. Our responsibilities required us not only to understand an thwart the systematic efforts of foreign intelligence services to insert spies into our government, but also to prevent foreign spies from working in the bowels of private industry and the nation's laboratories. But human spies are no longer the whole game. If someone can steal secrets electronically from your office from Shanghai or Moscow, perhaps they don't need a human spy. Or perhaps the spy's job is no longer stealing secrets but subverting your network to allow the secrets to bleed out over the Internet. In a networked world, I quickly saw that counterintelligence must conten with the penetrations of the public and private electronic networks that are the backbone of our communications, the storehouses of our technology, and the nervous system of our economy and government. These networks, I regret to say, are porous and insecure, vulnerable not only to casual hackers but even more so to professional electronic thieves and powerful foreign intelligence service But we want seamless, effortless interconnectivity and the productivity that comes with it—who doesn't? And so our vulnerabilities multiply as we continue to privilege convenience over security.

Meanwhile, the world is speeding up. We experience this acceleration in the pace of our daily lives in product cycles and fashion trends, in the instantaneous dissemination of information, in the awesome and continual increases in the capacity of our electronic systems, in the speed at which our products and ideas are copied and pirated. Businesses know that their ability to profit from their own innovation depends on their ability to get their products to market faster than ever and to exploit ther more quickly than ever—before they become obsolete or unfashionable, or are ripped off by an overseas pirate with low overhead and no R&D costs. Value appears and disappears with bewildering speed. Who today remembers the computing juggernauts Wang Laboratories or Digital Equipment Corporation? Financial giants like Bear Stearns, Lehman Brothers, and Washington Mutual vanished overnight.

The value of intelligence is also transitory. This is especially true of SIGINT—the electronic stuff It's useful only if you can act on it in time, and the time for action is getting shorter and shorter. Information from an African country about an impending attack on an airliner at Kennedy Airport is useless if you can't put it in the hands of security officials at the airport right away. With tactical

military intelligence—that is, on-the-spot information about unfolding situations—commanders mus be able to feed it into their decision cycles, which grow shorter and shorter.

This kind of acceleration is ubiquitous in our society. For example, if the price of a security on Wa Street is momentarily $0.005 more or less than the price of the same security in London or Frankfurt or Singapore, a trader whose electronic systems are agile enough to act on that difference can make millions in less than a second. So both the public and the private sectors are bowing to unrelenting pressure to enhance the connectivity that both increases productivity and decreases security, to short decision cycles, and to move information faster and more widely. That pressure also creates a dilemma, because the more widely and quickly you make information available, the more trouble yo have protecting it. Regardless of whether that information is a classified diplomatic cable, valuable engineering drawings, or your own medical records, when you put it on an electronic network to whic thousands of people have access, it is no longer really secret—or private. The name for this condition is transparency, and it is a fundamental condition of contemporary life, for good and ill.

In this book I hope to show that the difficulties of protecting your privacy and mine and the difficulties of keeping secrets in an intelligence agency or corporate office are remarkably alike. Secrecy is to companies and governments as privacy is to individuals. Both rise or fall on the same technologies and cultural proclivities, and at the moment both are falling precipitously.

In 1949, the architect Philip Johnson built himself a remarkable house on an eleven-acre Connecticut estate of woods and meadow: a transparent glass rectangle with a completely open floor plan, and without shades or curtains. Even the sleeping area was completely exposed to the outside. Johnson did make one concession to privacy in his glass house: He enclosed the bathroom, whose walls were the only interior structure to extend from floor to ceiling. Nearby he constructed a more conventional house, called Brick House, for weekend guests. But transparency was not an unalloyed virtue, even for a modernist architect, and soon Johnson sought police protection to ward off trespassers, and he nailed up a sign pleading: THIS HOUSE IS *NOW OCCUPIED*. PLEASE RESPEC THE PRIVACY OF THE OWNER. This measure apparently did not meet with great success, because Johnson eventually moved into Brick House and used Glass House chiefly for entertaining. Even modernist architects need places of refuge. Johnson’s transparent dwelling is now an icon of twentieth-century architecture—and a fitting image of our current predicament in which relentless transparency threatens our security and our privacy.

I begin this book by examining the threats to our personal security, all of which are more dire than we generally realize. Then I expand the focus to the welter of threats facing the larger-scale enterprises and institutions that together form our society: companies, financial markets, infrastructure, the military, and intelligence. Throughout the book, as I widen our view, we’ll see tha the same principles—the same dangers—apply at all levels, from the personal to the national. In all cases, the views I express are my own, not the U.S. government’s. Our world is becoming a collectio of glass houses that provide only the illusion of shelter. Finally, I’ll draw on my experience to offer suggestions for how all of us—individuals, companies, and the government itself—can shore up thes ever more fragile and transparent structures.

# ELECTRONICALLY UNDRESSED

YOU'VE PROBABLY DECIDED that in order to save a buck on a bunch of grapes, you'll let the supermarket compile data about your eating habits, and that in order to avoid a long line at the tollbooth, you'll let some contractor for the state know how often and at what times of day you cross that bridge or drive on that highway. Maybe you even pay for a cup of coffee with a credit card. We are what we eat—and what we buy, and who we know, and where we live, and what we look at, and where we go. All of us—not just young people—give this information away freely because it's convenient and often enjoyable to do so. Forty-five percent of Facebook users are twenty-six years ol or older, and the fastest-growing segment of that group is women over fifty-five.[1] Older people may not use Twitter, but they do use credit cards, pay tolls automatically on the interstate, bank online, an buy cars equipped with GPS.

In the last twenty years the ready availability of inexpensive, increasingly powerful, and ever-smaller networked computers has revolutionized how—and how fast—we create, process, store, and transmit information. These developments have changed our lives so pervasively, and accelerated the speed of change in our lives so sharply, that it's hard to recall what the world was like before we wer so happily and relentlessly connected. We think of letters written on paper as relics of a bygone era, but even dial-up modems or waiting thirty seconds for a Web page to load now seems quaint. In 2010 a six-year-old watching a 1980s movie asked her father, "Why is the phone attached to the wall?" If you can answer this question, you're getting old. Manual typewriters, carbon paper, party-line telephones—these are incomprehensible phrases to the majority of people now living.

Computing power has doubled every year and a half since the mid-1960s.[2] To grasp what this means, consider that in 1978 it cost about nine hundred dollars to fly from New York to Paris, and th flight took seven hours. If airline travel had accelerated at the same rate as computing power, you could now make the trip for about a penny, in less than a second.[3] Our machines have sped up—today's game processors can do at least a *billion* operations per second—but we haven't. We can't keep up with our own machines. So our machines have begun to talk to one another, making decision for us, exchanging information about us. They apply the brakes in our cars when we're too slow to do it, land huge aircraft unassisted, trade enormous volumes of securities, adjust the flow of electricity o the grid, and share data about us that we think of as private. And these machines are everywhere. The "personal digital assistant" in your pocket is more powerful than the 1960s IBM mainframe compute that occupied an entire room.

The movement of technology between government and the private sector is not a one-way street. Just as GPS has migrated from fighter planes to your car, so has technology moved from your living room to the front lines of conventional and cyber warfare. Most of the government's computing systems are developed in the private sector now, and gaming consoles have directly influenced the design of instrumentation for weapons systems. The Cyber Crimes Center in the Department of Homeland Security has even dumped the eight-thousand-dollar consoles it once used to crack the

passwords of seized computers—then replaced them with Sony's PlayStation 3s for "brute force" password attacks that run through every conceivable password until they find the right one.[4] The difference between electronic toys and business applications is vanishing.

The border between commerce and government wasn't always so porous. In the beginning the Internet and its precursors were federally funded links between universities and government researchers, and it was *illegal* to use them for commercial purposes. Congress didn't change that law until 1992.[5] Even so, many university users were furious at the thought that an educational tool woul be polluted by commerce, and as recently as the mid-1990s the Internet was still essentially a researc tool and the plaything of a few. In 1995, the idea of buying and selling on the Internet aroused more suspicion than enthusiasm, but by January 2008 there were 1.3 *billion* Internet users .[6] By 2011 the number of users had climbed to nearly 2 billion, and many of them were buying and selling online.[7] No wonder that by 2009 information technology stocks had become the single largest sector in the U.S. economy.[8] By 2015, the number of Internet hosts is expected to exceed the planet's human population.[9] Mobile data traffic is doubling every year, and all that data leaves a trail.

Going from rummaging in a file drawer to searching electronic data and images was dramatic; so was clicking a mouse instead of traveling to the library. In these cases, however, we were *fetching* things we wanted; new technology merely allowed us to fetch faster. Now data comes to us unbidden based on choices we made in the past, who our electronic friends are, and where we live. Or it comes based on where we *are,* like a coupon for a latte that shows up on our mobile phone when we walk pa the coffee shop.[10] We now live in a sea of ambient data. Or rather, each of us increasingly lives in his or her own customized virtual sea of ambient data. And wherever we swim in that sea, each of us leaves electronic evidence of where we've been and strong indicators of where we are likely to go ne —of which we are often unaware.

## The Data Market

Data is a commodity, and the market for it is measured in billions of dollars—trillions if we include electronic banking and credit card issuers. Reed Elsevier PLC, one of the world's biggest data aggregation companies, has reported a steady 10 percent annual growth of online traffic since 1999.[1] Reed Elsevier owns LexisNexis, the largest source of online legal and periodical information. It also owns ChoicePoint, which does background and public records searches; it's the outfit that checks the accuracy of the résumé you sent to a prospective employer or graduate school.[12] These companies an others like them make fortunes based on information that has always been publicly available. They aggregate that information, sort it, reformat it, and make it instantaneously available to public- and private-sector users willing to pay for it. Other firms occupy other niches: financial data for investors medical records for hospitals, doctors, and insurance companies; credit scoring for any business that gives you credit; and of course banks and credit card issuers. MasterCard alone made $5.5 billion in net revenue by managing $567 billion in charges, transactions, and settlements worldwide.[13]

Aggregated data tell a merchant what goods to stock and how to target advertising. Do you like fis but avoid red meat? Fine, we'll send you an ad when we have a fish special, but we won't waste our money sending you ads for roast beef. You prefer SUVs to convertibles, or casual clothing to suits, o

certain kinds of movies or music? Great—we won't waste our money or your time telling you about products you won't buy anyway. This is good for the merchant; arguably it's good for you, too. Aggregated data is also good for insurance companies, because without it they can't calculate premiums for groups of people that represent different levels of risk. Whether that's good for you depends on which risk pool the insurance companies put you in—and whether the data is accurate.

A single set of fingerprints probably has no value, but a bank of such prints helps the police identif criminals; DNA databases do the same. The federal DNA database holds 4.6 million profiles, or 1.5 percent of the U.S. population—mostly convicted criminals. Across the ocean, two thirds of Britons favor a law that would require *everyone's* DNA to be stored.[14] And if you visit central London you're being photographed every time you walk down the street or enter the Underground, and if you drive, your license plate is being photographed wherever you go. The better the database, the more crimes will be solved. Whether that benefit is worth the privacy loss is another question. But however you feel about that, the benefit of aggregated data in solving crime is beyond dispute.

Data are valuable in all these cases because the aggregator can link an identity with a history or a pattern of behavior. But aggregated data also have enormous social importance even without links to individuals. Without that information, public health officials don't know what diseases need more or less attention and resources, and predicting what kind of flu will strike next year would be even harde than it is. Having this data in real time, or near real time (as opposed to getting it a month or a year later), is also valuable, because it can warn that a new epidemic is breaking out right now, when we may be able to prevent or slow down its spread, and this is true whether the epidemic is natural or the result of a terrorist attack. Add personally identifying information back in, and you add more value. I helps find victims and, in some cases, the source of infection or attack.

The amount of information available about you is startling: your date of birth, driving record, medical history, credit rating, shopping patterns (including where you shop and what you buy), mortgage and property records, political contributions, vacation patterns (including the route you drive), whether you drive, telephone numbers (even if unlisted), the names of your spouse and children and business partners, your grades in school, your criminal record (if you have one)—and much else besides. In order to get that information about you, someone used to have to stand in line i several different buildings, not necessarily in the same city, just to request it, and he probably had to wait around or come back a second time to pick it up. Now, with several mouse clicks, the informatio is often available to anyone anywhere in the world who wants it.[15] Your medical records are suppose to be under lock and key, but who keeps them? Your doctor, to start with, but so does the software provider that your doctor pays to store those records, and the doctor's outside laboratory, and the insurance company that covers you, and their database administrator, who may work for someone els Information you may think is confidential, sensitive, and private is sent to many different places *automatically*, sometimes in different countries, and each leg of its transmission over public communications networks represents a potential vulnerability. There is rarely such a thing as a single unique record anymore. There are multiple copies of every record, stored in multiple places, in databases whose level of security is a mystery to most users, and sometimes even to company officials.

### *"We never don't know anything about someone"*

How did all this data become so readily available? Because you and I have given it away. In many cases we've had little choice about it—not if we want a mortgage or lease, a marriage or driver's license, or health insurance; not if we want to enter the hospital, send our children to school, contribute to a political candidate, or buy a snack on the many airlines that no longer accept cash in flight.[16] In other cases we don't even know it's happening. If you click on the credit card page of Capital One Financial's Web site, for example, thousands of lines of code representing information about your education and income level and residence will be sucked up by the company in a fraction of a second. Your machine is talking to their machine, and in that fraction of a second your machine working for them, not you. And so aggregated data snowballs. As Capital One's data contractor quipped, "We never don't know anything about someone."[17] That contractor probably doesn't think he's in the personal espionage business, but he is.

But do we care that we're being spied upon? Is this new type of commercial spy collecting secrets —or simply gathering information we freely spread around? Many people find it comforting that someone else knows where they are at all times. Mobile phone companies and location services for your car, like OnStar, advertise their ability to do just that for you. Your mobile phone or PDA make a constant record of where it goes. Mobile devices in the United States generate about 600 *billion* events per day.[18] These events don't just include the calls, text messages, and Internet connections you know you're making. They also include the silent "pings" between each cell phone and a nearby tower whether you're using the phone or not. They are the heartbeat of cell phone service and typical occur every few minutes. Each ping is tagged with geospatial location information,[19] and if you have GPS or use Wi-Fi that record is very precise—less than eleven yards. If not, the record is still pretty accurate, because the cell towers that handle your calls are constantly pinging your phone and pinpointing your location to within about a block. According to Jeff Jonas, a data expert at IBM, this information will soon warn us about events that haven't even occurred yet. Your free Gmail account, he surmises, will advise you "that your buddy Ken is going to be 15 minutes late to the pool hall this coming Thursday, unless he leaves work 15 minutes early . . . which he has done only twice in seven years."[20] With enough information about your past movements, scientists can predict your movemen with about 94 percent accuracy. Or forecast traffic congestion. By examining patterns of communication and movement, they can detect flu symptoms before you know you're getting sick. The emotional content of Twitter lets researchers predict the moves of the Dow Jones index with about 88 percent accuracy.[21] Jonas also points out that the police could use the same kind of information to watch crowds form and disperse—a powerful tool for crowd control. Or for discouraging political expression. As of mid-2011, law enforcement officials in most jurisdictions ca get geolocation data from mobile carriers simply by issuing a subpoena. Most jurisdictions don't require a warrant signed by a judge—at least not unless the surveillance is long-term or involves movements inside a dwelling.[22]

And so, little by little, we find ourselves living in a glass house. Last year's novelty is this year's necessity; your friends wonder why you don't have one. The price of last month's expensive electron luxury just fell by half. Your kid wants one for her birthday. It's not simply adults who are being watched and marketed to, identified, and classified. Sure, we give up some privacy with each little step, but we get something back: convenience, peace of mind, whatever. We may be electronically naked, but we demand it. This is the world we now live in, and let's face it: *We find that world*

*irresistible*.[23]

---

THIS IRRESISTIBLE WORLD in which we are all numbered and accounted for crept up on us largel unnoticed, but its roots are old. Americans and Western Europeans have been counting, classifying, and identifying ourselves for several hundred years, but the initial steps were slow. The first modern European census was taken in Prussia (naturally) in 1719; the United States took its first census in 1790; Britain and France[24] followed in 1801. Indeed, representative democracy required counting in order to achieve fairness in taxation and legislative representation. [25] And then, in the last quarter of the nineteenth century, two things happened that dramatically accelerated this business of identifying everybody. First, the state pension was born in Germany, and therefore the state was required to know who was owed money and at what age. Keeping increasingly exacting records was one essential resul National identity cards began to appear. Second, in big cities like London, Paris, and Buenos Aires, t police began to wonder, Who is this man we have arrested *really*? Haven't we arrested him before?

Enter Alphonse Bertillon, a low-ranking functionary in the Paris *sûreté* who in 1882 showed that h could reliably *re*identify anyone by measuring his or her head and body and making a careful record tattoos, scars, and other quirks. Bertillonage was the beginning of systematic biometrics but it was soon superseded by fingerprinting, which quickly became the identification method of choice for law enforcement agencies worldwide. We fingerprint not only those charged with crimes, but also everyone in the military, everyone who applies for a security clearance, and welfare recipients. In the UK and in some parts of continental Europe, the fingerprinting of schoolchildren is widespread, and is used in place of library cards.[26] There are now fingerprint scanners, fingerprint door locks, safes with fingerprint locks, fingerprint time clocks, and fingerprint kits for your favorite niece or nephew.[27] These devices are not being foisted on people; there's a market for them. Fingerprinting is so ubiquitous that it has become a metaphor for any system of positive identification, like "DNA fingerprinting."

The credit markets we take for granted are another aspect of this irresistible world. We could hardl live without them. Pioneered in the United States during the Great Depression,[28] these markets requi instant, accurate information about potential borrowers. Without them a home buyer could not "prequalify" for a mortgage on the phone or get instant credit to buy a refrigerator, as we now do as a matter of course. Before that, creditors didn't lend to people they didn't know, or they took property as security, like a pawnshop.

The overlapping and ever-expanding appetite of government and commerce to keep tabs on us—an our own appetite for keeping tabs on one another—means that it's virtually impossible to elude our own autobiographical trail of purchasing habits, property ownership, employment history, credit scores, educational records, and in my case, a security clearance record a mile long. If you live in India, everyone's personal data record will be a mile long, because the government there has launche a project to assign a unique twelve-digit identification number to every one of its 1.2 billion inhabitants, and to link that number to their fingerprints and iris scans. The idea is to ensure that welfare payments reach the right people and to permit India's vast impoverished population to gain access to online banking and other services.[29] Critics worry that the information will not be guarded adequately. They should also worry that aggregating data to prevent fraud also enables fraud, becaus gathering huge quantities of data in one place means it can all be stolen from one place.

Meanwhile, the shelf life of all this data gets longer and longer, because the cost of storing it has fallen like a stone. In 1990 a oneterabyte storage drive would have cost $1 million to buy. (A terabyte is a billion bytes of eight 1s and 0s, or a thousand times more than a gigabyte. Sixty-four terabytes is half the size of a big university library.) Now you can buy that drive for under $100. *The price has fallen ten thousand times*. Information about us doesn't disappear with time. It can be saved forever, cheaply, in lots of places. That's worrisome, but we also find it appealing. For about $175 you can bu a USB stick—also called a flash drive or a thumb drive—with sixty-four gigabytes (or "gigs") of memory. That's thirty-two million pages of text dangling at the end of a key chain. As we will see later, the ease of transporting huge amounts of data has dramatically changed the espionage trade.

FOLLOWING A SUDDEN explosion of Internet-enabled crime and the growing sense that our personal lives were exposed to strangers, Americans and Europeans began to search for ways to protect ourselves. Chiefly we have sought to regulate "personally identifiable information." [30] The European Community defines this somewhat more broadly (and vaguely) than do U.S. laws, but the phrase generally means data such as your postal and e-mail addresses and Social Security and credit card numbers, which can readily be associated with you. Companies like to tell you how carefully the protect this kind of information. But are these efforts effective?

The answer depends on the objective. The rules have undoubtedly forced companies and government agencies to tighten their handling of information about their own customers and employees. Whether they have had any effect in reducing fraud is doubtful, however, because the amount of personal information legally available is burgeoning, and the black market in such information is vast, as we'll see in the next chapter. But if the objective is to protect your anonymity, these laws have little effect—and may soon have none at all. That's because each of us can now be easily identified without reference to any of the usual categories of personally identifiable information. Strip it away—that's called "anonymizing" it—and data aggregators can put it back almost instantly.

Let's suppose I know your zip code and gender. If twenty thousand people live in your zip code, I can eliminate ten thousand of them by gender. Add in your age, and I can reduce the number much further. If I know what kind of car you drive, I can identify you with near certainty. Researchers at Stanford University were able to reidentify people by their Netflix viewing habits simply by comparing the company's carefully anonymized viewer ratings with publicly posted ratings on other Web sites that rated the same movies. Essentially, they showed the emptiness of the promises that Netflix and others make that you can do, watch, or buy whatever you like anonymously on their Web sites. Information scientists says they need only thirty-three "bits" of information—mundane things like your zip code or the make of your car—to identify you, and the information may have nothing to do with the legal definition of personally identifiable information. There are two possibilities for each bit (each bit must be a 1 or a 0), and $2^{33}$ is a very large number—more than 8.6 billion, which is more than the Earth's human population.[31] A firm called PeekYou has filed a patent application for a "computerized distributed personal information aggregator" that matches real names with pseudonyms used on blogs and social network sites like Facebook and Twitter.[32] It's becoming almost impossible to be anonymous anymore.

Many of us are uncomfortable with the proliferation and transparency of personal data, and some would like Congress to pass laws to stop it. But the law is chasing reality, not shaping it. (This is

another theme we'll see cropping up repeatedly throughout this book.) The law is not fundamentally altering the direction or speed of our society's movement toward the instant, universal availability of massive amounts of information that can be sliced, diced, and analyzed in microseconds—nor can it. You will have such data if you want it; your friends, enemies, and bank will have it too, and the government will either have it or be allowed to get it under certain legally defined conditions. We wi write some rules that make access somewhat more difficult, but those rules won't be able to hold bac an overwhelming tide.

There are aspects of this that I find wonderful; others strike me as distasteful or worse. It has led t massive increases in productivity and wealth. It has also created vulnerabilities of staggering proportions—vulnerabilities that now generate billions of dollars in criminal revenue, are exploitable and exploited by foreign intelligence and military services as well as by criminals, and that—if not better understood and mitigated—put our communications, our economy, and even our military at ris of failure. For both good and ill, this is what's happening. This is the glass house we live in.

# A PRIMER ON CYBER CRIME

JUST AS THE RAIN FALLS on the unjust and just alike, so aggregated data have value for thieves and swindlers as well as for law-abiding merchants and public health officials. Organized gangs of international criminals have moved eagerly into cybercrime, and often use it to fund other nefarious enterprises, because it makes more money than even the illegal drug trade.[1] Profits are high because crime on the Internet is cheap; e-mail is essentially free. The chance of scamming any particular individual for data is poor, but the chance of scamming one in a thousand is much better, and if I can get my hands on a million sets of records, my chances of running a successful scam become really good. This is why electronic crooks are systematically stealing large batches of data from places such as the University of Virginia, the Catholic Diocese of Des Moines, Citibank and the Royal Bank of Scotland, hospitals across the country, the Pentagon, the General Dynamics Corporation, and a slew of other agencies and companies .[2] In 2010 Verizon, a telecommunications company that tracks this market, reported that over nine hundred million sensitive data records had been stolen from Americans in the previous six years.[3] And an ominous new trend has emerged: The rate of theft by corporate insiders, who are in a better position to steal valuable information than are external hackers, has gone up.[4] In 2010, the incidence of electronically stolen data surpassed that of physical theft for the first time.[5]

The Internet crime business has become international. An identity thief in Tulsa, Toulouse, or Tunbridge Wells can buy stolen credit card numbers from a gang in Moscow that freely advertises its wares. He can e-mail those numbers to a counterfeit credit card shop in Guangzhou that produces cards that are indistinguishable from the real thing. And if that shop doesn't make driver's licenses—he'll want a fake ID before he goes shopping—he can get one from another counterfeiting shop in Minsk, in Belarus.

If you're a victim, you pay for this kind of theft directly in loused-up credit, months of aggravation, and possibly money you'll never recover. And all of us pay indirectly through higher prices. For example, our banks prefer not to talk about their losses from credit card fraud, because they don't want to scare us away from doing business on the Internet, which is highly profitable. That's why in the United States you pay nothing when someone makes a fraudulent purchase on your card, not even the fifty dollars the issuer could legally charge. Instead, banks prefer to make up the losses by charging you for transactions that used to be free or cheaper than they are now.

The cost of becoming an Internet thief is low—and getting lower. You can download user-friendly hacking tools for free. The cutting-edge tools cost money, but not much considering the potential rate of return. They are stealthy, innovative, and customized for the kind of information they target.[6] If you want one that searches out engineering drawings, for example, you can buy it. If you want one that searches instead for personal identification numbers (PINs) and bank data, it's available.

Thieves who know how to steal your data but may not know how to exploit it can sell it to a third