An Excerpt From

The Rise of the American Corporate Security State
Six Reasons to Be Afraid

by Beatrice Edwards
Published by Berrett-Koehler Publishers

THE RISE OF THE AMERICAN CORPORATE SECURITY STATE

SIX REASONS TO BE AFRAID

BEATRICE EDWARDS

Foreword by **JESSELYN RADACK**, National Security and Human Rights Program Director, Government Accountability Project

The Rise of the American Corporate Security State

Six Reasons to Be Afraid

Beatrice Edwards

Berrett–Koehler Publishers, Inc.
San Francisco
a BK Currents book

The Rise of the American Corporate Security State

Berrett-Koehler Publishers, Inc.
235 Montgomery Street, Suite 650
San Francisco, California 94104-2916
Tel: (415) 288-0260, Fax: (415) 362-2512
www.bkconnection.com

Ordering information for print editions
Quantity sales. Special discounts are available on quantity purchases by corporations, associations, and others. For details, contact the "Special Sales Department" at the Berrett-Koehler address above.
Individual sales. Berrett-Koehler publications are available through most bookstores. They can also be ordered directly from Berrett-Koehler: Tel: (800) 929-2929; Fax: (802) 864-7626; www.bkconnection.com
Orders for college textbook/course adoption use. Please contact Berrett-Koehler: Tel: (800) 929-2929; Fax: (802) 864-7626.
Orders by U.S. trade bookstores and wholesalers. Please contact Ingram Publisher Services, Tel: (800) 509-4887; Fax: (800) 838-1149; E-mail: customer.service@ingrampublisherservices.com; or visit www.ingrampublisherservices.com/Ordering for details about electronic ordering.

Berrett-Koehler and the BK logo are registered trademarks of Berrett-Koehler Publishers, Inc.

First Edition
Paperback print edition ISBN 978-1-62656-194-6
PDF e-book ISBN 978-1-62656-195-3
IDPF e-book ISBN 978-1-62656-196-0

2014-1

Interior design and production by Dovetail Publishing Services.

Cover design by Brad Foltz.

For the staff and clients at the Government Accountability Project, who never met a windmill that wouldn't tilt.

This page intentionally left blank

Contents

Foreword

By Jesselyn Radack

In the pages that follow, Bea Edwards shows the post-9/11 merger of corporate wealth and government power in the United States—beneath a thinning veneer of democracy. The book in your hands explains the way in which this private/public collaboration gives policy-making over to profit-seeking corporate interests, which then become a direct threat to our civil rights and our way of life.

Peace and financial stability are the first casualties. Increasingly, well-connected corporate directors, with their privileged access to military resources and the national treasury, placed the country on a permanent war footing even as they dismantled government regulation of their businesses. They made a series of decisions and actions that the public never considered, debated, or approved, even indirectly.

The Rise of the American Corporate Security State examines the way corporate power behaves when it takes a dominant role in government policy-making and explains the advent of endless war. For profit-seekers, war is desirable for three reasons:

1. It is extremely lucrative for some companies.
2. The withdrawal of civil liberties is simpler in wartime because people are frightened.
3. The public accepts greater official secrecy because the nation is under threat of attack.

War justifies the dragnet electronic surveillance of Americans; the government claims to protect us by searching for the terrorists among us. The government also justifies withholding information about its actions, citing national security.

To comingle private wealth and public authority, US elites are promoting an antidemocratic legal regime that allows the exchange of consumer information among the corporations that now own the nation's critical infrastructure—banks, power companies, transportation companies, and telecoms—and America's intelligence agencies. This new legal collaboration will provide certain private interests with the cover of legal immunity for their invasive surveillance. It will eradicate the remains of your privacy and deliver your personal data to the government. Should you protest or demand redress, you will find that you have lost your legal right to remedy.

As an attorney, I represent whistleblowers from the National Security Agency, who speak about the intrusiveness and illegality of bulk surveillance of Americans. And I, too, became a whistleblower at the Justice Department when I witnessed the slide of the US government away from the Bill of Rights into a morass of illegal detention and torture. In different ways, through different means, our government accused my clients and me of betraying the country. But the opposite was true. We remained loyal to the Constitution, while our government betrayed it. When we spoke up, the Justice Department turned on us. Every day, we experience firsthand the consequences of the government's unwanted attentions. We know what happens when your government suddenly notices you—and sees you as a threat.

Edward Snowden, of course, knows this, too. He is stateless because he exposed the extent to which our government has compromised our constitutional rights and promoted the joint operation of private and public sector surveillance—under the guise of counterterrorism. The significance of his disclosures cannot be overestimated. He is revealing the whole ugly antidemocratic project, and he came just in time. Bea Edwards's analysis explains why we must act on what he's showing us, and if we do, we can back away from the brink of permanent war and gross economic inequality where the Corporate Security State is leading us.

Preface

In the United States today, we have good reason to be afraid. Our democracy and our freedoms are impaired. Many Americans have lost their homes and jobs and will never get them back. Our pensions and our privacy are also gone. Most frightening of all, the Constitution that protected us for more than two hundred years from the tentacles of oppressive government and the stranglehold of private wealth is less respected every day.

After September 11, 2001, our government told us to fear foreign terrorists, so we did. To protect our national security, we submitted to unreasonable searches without protest; we surrendered our freedom of speech and association. At a staggering cost, we financed a permanent, mercenary military to patrol the world.

In September 2008, when the economy froze, the stock exchanges plunged and private firms began shedding jobs by the hundreds of thousands each week. The Treasury Department stepped in and transferred hundreds of billions of dollars in public assets to failing private financial institutions. The subsequent congressional inquiry determined that we were all responsible. We were guilty of irrational exuberance.

But now, taking stock years later, we have to recognize that no foreign terrorist shredded the Constitution. Nor did we, as citizens, bankrupt the nation. Powerful forces inside the country did. And worse than that: they intend to keep doing it. They have yet to be stopped. This is the real reason to be afraid: the rise of the Corporate Security State.

The Constitution gave us three branches of government to ensure that no one small faction could control the state. Each of them is failing us.

The agencies of the executive branch appear to be helpless before the rise of the Corporate Security State. According to the attorney general, the Justice Department cannot prosecute corporations that usurp our rights and rob us of economic security, and the Treasury Department is forced to protect these financial forces from the consequences of their own reckless "trades." The president, whoever he happens to be, releases triumphant photographs of himself saluting in a flight suit or watching a live feed of SEAL Team Six killing Osama Bin Laden. He gives speeches about America and its greatness and periodically runs for re-election in what is now a grotesque pageant of clowns.

The Congress is paralyzed by squabbles over the debt, much of it occasioned by endless, off-the-books warfare. In the fall of 2013, the whole thing shuts itself down, along with the rest of the government, for lack of funding, flounders toward the next political showdown, and finally produces a meaningless agreement with itself about the national budget. Increasingly, the American public despises the entire body, and one poll taken during the 2013 government shutdown showed that we preferred cockroaches, zombies, and dog doo to Congress.

The judiciary, which is the last to go, blesses the increasing intrusion of money in politics, and stands down before the revelations of a secret court operating behind a veil of national security.

The Corporate Security State is tipping the balance between the self-interest of a governing corporate elite and the rights of the rest of us to freedom, privacy, safety, and fairness. We can see the power shift manifest in six clear and evolving trends since 2001:

- **Average citizens are subject to ever-expanding surveillance by the government-corporate complex.**

  Intelligence agencies, working with private corporations, gather extensive private data on *everyone.* Outsourced government has created a complex of private national security contractors who capture approximately 70 percent of the bloated national budget for intelligence and surveillance.

- **Control of information by the government-corporate complex is expanding.**

  The Obama administration continues to overclassify information. In 2009 and 2010, the number of classification decisions exploded. Among the documents deemed secret is the one setting out the cost of our

national surveillance system and its unconstitutional domestic intelligence gathering capabilities. We are obliged to pay for it, but we have no right to know how much it costs or what it does.

- **The separation of powers established by the Constitution is eroding. Rights guaranteed by constitutional amendments are becoming irrelevant. Reporting a crime may be a crime, and informing the public of the truth is treason.**

  Since June 2013, we've discovered that the National Security Agency (NSA) has been routinely violating the First, Fourth, and Fifth Amendment rights of American citizens. The NSA has been doing this secretly for years, while the Justice Department uses the Espionage Act to prosecute national security whistleblowers as traitors when they try expose it.

- **The government-corporate surveillance complex is consolidating. What has been a confidential but informal collaboration now seeks to legalize its special status.**

  Legislation permitting the fluid exchange of information about citizens between the national intelligence apparatus and private financial and infrastructural institutions is moving through the Congress.

- **Financial reforms enacted after the crisis are inoperable and ineffective because of inadequate investigations and intensive corporate lobbying.**

  The major financial institutions, well-connected to the Congress, the Treasury Department, and the Justice Department, ensure that key regulations implementing reforms are either unfinished or ineffective.

- **Systemic corruption and a fundamental conflict of interest are driving us toward the precipice of new economic crises.**

  After the financial cataclysm of September 2008, the Justice Department's refusal to prosecute senior officials of the corporations that failed due to systemic fraud eliminated any deterrent. The deceptive practices continue, and the next collapse is only a matter of time.

The consequences of these trends and conditions are moving us toward a world like the one portrayed in the dismal post-apocalyptic movies churned out by Hollywood. We are submerged in wars that never end, and the wealth produced by and in the United States skews upward in

ever greater concentrations. We await the emergence of the world's first trillionaire and look forward to the fawning portrait of him in a glossy business magazine.

Such a country can only be maintained with greater repression of dissent and suppression of the truth. This is why the government is into deeper and broader surveillance. Instead of funding education and health care, clean air, and water, our taxes are paying for intrusive electronic monitoring—of us.

But the battle for equality and fairness is not yet over. Many of the laws that prohibit surveillance and unreasonable search and seizure are still in place. Although they are under attack, and they erode incrementally if we are not paying attention, we still have recourse to them. And they still protect us from domination by a faction—the danger most dreaded by the framers of the Constitution. We must aggressively defend them, and we must promote peace for the United States and the rest of the world. For the war we think we are fighting abroad is also being waged against us. If we deprive others of their rights in an effort to protect ourselves, step-by-step we forfeit our own rights, too. That's just how it works.

This page intentionally left blank

No truly sophisticated proponent of repression would be stupid enough to shatter the facade of democratic institutions.

—Murray B. Levin
Political Hysteria in America: The Democratic Capacity for Repression

PART I

The National Security State

The right of the people *to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*

—Constitution of the United States
Amendment IV

This page intentionally left blank

CHAPTER 1

The Government-Corporate Complex: What It Knows about You

Reason to be afraid #1:

Average citizens are subject to ever-expanding surveillance and data collection by the government-corporate complex.

Halfway across the ornate sitting room, Julian Assange stands with his back to the door, drinking a bottle of beer. It is early on a summer evening, June 22, 2013, and the Embassy of Ecuador in London is hosting a small party to acknowledge the one-year anniversary of his arrival in need of asylum. While Assange stands chatting calmly about the future of his anti-secrecy enterprise, Wikileaks, few people in the room know that he is worried. Sarah Harrison, his principal researcher and confidant, is only hours away from slipping out of Hong Kong with Edward Snowden, who, at that moment, is fast becoming the most hunted man in the world.

Close friends and supporters of Assange mill around the room, helping themselves to the buffet and arguing about software and the state of the world—in that order. Assange himself, with his longish white hair and black jeans, looks slightly out of place in the scene, bordered as it is by stiff-legged, gilt-painted settees. After a year, however, he's completely at home here, laughing and joking with the security guys, lawyers, and hacker guests, talking thoughtfully about the escalating struggle for control of electronic information.

"There's a completely new creation in the world," he says. "And the battle is on for access to it."

He's talking about the electronic "pocket litter" that each of us collects as we cruise the Internet and use our cell phones each day. Behind us, we leave a digital trail that reveals our interests, our politics, our friends, their friends, our health worries, our finances and fears. As he speaks, Assange is thinking of Snowden and what he had recently revealed about the practices of the National Security Agency (NSA) in the United States.

In the course of his highly classified contract work for the NSA, the US intelligence agency, Snowden uncovered unconstitutional surveillance programs that trace and store the electronic pathways etched across the Internet by hundreds of millions of Americans. NSA surveillance also sweeps up and archives the metadata associated with phone calls. Snowden discovered that Americans are subject to dragnet electronic domestic surveillance and have been for years.

His disclosure of NSA domestic surveillance caused a Washington tailspin, and the search for the source was on. After he identified himself in a video filmed in a nondescript Hong Kong hotel room, US political pressure ramped up on the Chinese government. The White House, the NSA, and the FBI closed in, and as a Chinese diplomat later confided, "You don't know what pressure is until you have those sons-of-bitches breathing down your neck."

Even if everything else the Chinese government said about its role in the Snowden affair was calculated, that statement was unquestionably spontaneous and true. Snowden had the secrets to the Corporate Security State that was quietly metastasizing through US federal agencies and corporate management suites after 9/11, and he was telling them to the world. He had to be stopped.

In the world of national security and surveillance, the evening of June 5, 2013, two weeks earlier, was frankly horrible. At about 9:30 Eastern Daylight Time, a story by Glenn Greenwald appeared on the *Guardian* website, linked to an order from the Foreign Intelligence Surveillance Court (FISC) of the United States.[1] In black and white, the document showed that, at the request of the FBI, the FISC ordered Verizon Business Network Services to submit all telephony metadata in its systems to the NSA. Only the data for calls originating and terminating abroad were exempted from the order, which, until the *Guardian* posted it, was secret. The order would not declassify until April 2038, twenty-five years in the future.

Telephony metadata, an unknown phrase for many of us until that night, includes the phone number called, number calling, routing

of call, phone number identifiers, time of call, and duration. Subsequently, we learned that the FBI gave similar orders to Sprint Nextel and AT&T. Through a secret and tortured interpretation of the Patriot Act, Section 215, the court allowed this data collection.

Moreover, Greenwald wrote the next day that the NSA used a program called PRISM to collect customers' data from Microsoft, Yahoo, Google, Facebook, and other online corporations.

Two months later, a new Greenwald article appeared, also on the *Guardian* website: "XKeyscore—NSA tool collects 'nearly everything a user does on the Internet.'" The article explained that the XKeyscore program sucks into its maw almost every electronic datum on the Internet about everyone in the United States. And more than that: analysts need no prior authorization to inspect the emails, Facebook pages and postings, tweets, and Internet browsing history of ordinary citizens suspected of nothing. Via XKeycore, analysts at the NSA:

> *[L]isten to whatever emails they want, whatever telephone calls, browsing histories, Microsoft Word documents. And it's all done with no need to go to a court, with no need to even get supervisor approval on the part of the analyst."*[2]

Imagine that.

Many Americans can't, really. "I'm not a terrorist," they shrug. "So why should I care?" Then they laugh at the absurdity of highly skilled intelligence agents reading their dopey emails. "Go ahead, but it's pretty boring" is the typical reaction.

I work for a small nonprofit organization law firm in Washington, DC, that defends whistleblowers: the Government Accountability Project (GAP). Ordinary people come to us after they report appalling things in the places where they work and are dismissed, disciplined, or demoted in retaliation. They're hoping we can tell the world what they told us (at the very least) and get them their jobs back (at best). Most of our clients are federal government employees. We work with food inspectors, for example, who report animal cruelty in processing plants and toxic chemical additives to your food. Our clients are UN police officers who witness and report rape and sexual abuse by peacekeeping forces. Office workers and agents at the FBI and the NSA come to us to document gross waste and abuse. As do traders and risk managers who see pervasive fraud at multinational banks and FDA officials who report

drug trials faked by pharmaceutical companies. At truly repressive institutions such as the World Bank, our sources remain anonymous, but they also contact us by phone and email.

As a result, at GAP, our emails are not boring, and we do not want the NSA collecting them, much less reading them. Since the Snowden disclosures, we ask our clients to meet us outside the office, downstairs, and around the corner at Starbucks. We have to talk face to face as if we were subversives. To be safe, whistleblowers facing retaliation must provide their evidence on paper now, not by email.

Journalists must do the same with their sources. Or they need complex, user-hostile encryption programs. The loss of freedom from unreasonable search and seizure that Snowden exposed means the loss of a free press and free speech, as well as a loss of freedom of association.

Those who shrug about all this are right in a sense. Most calls and Internet habits are attracting nothing more than routine attention. It is also true, however, that innocent behaviors can drop you into the NSA's net. You are suspect if you're communicating over email in a language other than the one of the region you're in or if you're using encryption (in other words, trying to protect your privacy). Dissenting actions will also attract attention: writing a critical blog, or book; becoming a vocal whistleblower, whether wittingly or otherwise; contacting someone who contacts someone else who appears to be suspect. And then you must consider that US intelligence agencies have on record virtually everything you have done for five years past.

You should know that whatever information about you the government lacks, private corporations probably can provide. Your bank, of course, controls your financial data: number of bank accounts, balance, history of deposits, how much and when, cash withdrawals, bills paid, and checks written. Everything you bought with your debit card is also on record. Of course, if your bank issued your credit cards, then your purchases and payments every day, every month, are collected there, too.

You may also have noticed that whenever you shop online for, say, a how-to book or a garden tool, however specialized, you begin to get emails advertizing different versions of these things. Pop-up ads seem especially tailored for you. That's because they are. Commercial websites use cookies that record the ads you click on so that targeting is extremely precise.[3]

Then there's the new industry of data aggregation led by corporations like Acxiom and ChoicePoint. In her book *Spying on Democracy*, Heidi Boghosian describes this growing enterprise, which collects information about you available from municipal service providers, voter registration lists, property files, and court records. Clients of these companies include financial institutions, telecommunications companies, and insurance companies, which buy profiles and records for direct marketing purposes.

The US government also contracts data aggregators. According to Bogoshian:

> *Consumers are largely in the dark about the extent to which their personal data is being shared among different industries and government agencies and for what purpose. What is known, however, is that businesses and other organizations expend more than $2 billion annually to purchase personal information on individuals.*[4]

This is what Julian Assange meant when he said that there is a new creation in the world, and the struggle is on for access to it and control of it.

On a Wednesday afternoon in the fall of 2011, Jesselyn Radack (GAP's National Security and Human Rights program director), Kathleen McClellan (GAP's National Security counsel), and attorneys from three nongovernmental organizations (NGOs) convene in the conference room at GAP. It is decorated with the customary law firm props: the long oval table, the speaker phone, and shelves of matching leather-bound law books that no one has opened since the advent of electronic communication. GAP's national security program clients (Tom Drake, Bill Binney, and Kirk Wiebe) are there, too. Like Snowden, they're NSA whistleblowers, but they preceded him and used internal reporting channels, all of which failed them and left them exposed to devastating reprisal.

This afternoon, at Radack's and McClellan's behest, they are explaining what has been happening to all Americans since 9/11. The lawyers sit along one side of the table, and the NSA guys sit along the other. Radack opens the meeting: GAP is making the NSA whistleblowers available to the group because their knowledge about the US government's invasion of Americans' privacy is fundamental to any meaningful overall defense of the civil rights of US citizens. Bill is the mathematician of the trio, she

explains. Tom knows IT and NSA management, and Kirk translates the math into the programming.

As the NGOs take notes, Bill and Kirk explain how NSA eavesdropping has evolved and what the government can do now. The US government, they say quietly, can collect every website visit, every phone call, and every email of anyone in the country. All of this information can be recorded wholesale and stored in massive databases, to be queried if and when needed.

Binney, looking the part of a bemused mathematician over his glasses, explains in lay terms the capabilities of the NSA. He names an apparatus the NSA operates: the Narus Insight equipment. It can process 1.25 million 1,000-character emails a second. The NSA has ten of them.

All web information is collected, regardless of whether the transmitters are of US origin, and all information is stored for a period of years by the government.

NGO lawyer X protests softly. "But that's illegal," she says. "They've testified in Congress that they're not doing anything illegal."

"They're lying," Drake answers, looking at her as if she's new on the intelligence beat.

"To Congress?" asks the NGO lawyer Y.

Wiebe laughs softly and nods.

"Yes," says Drake. "To Congress."

"Jesus," from NGO lawyer Z.

NGO lawyer Y comes back: "But the FISA court would never approve that."

Wiebe looks down at his hands and says no more.

The audience for this presentation is not made up of novices. These are lawyers who are not naïve about official commitment to respect for the Bill of Rights. Still, they're stunned, and as the shock wears off, Binney delivers the *coup de grace*: although the programs are both illegal and intrusive, they are not especially useful for purposes of counterterrorism.[5]

It's clear to everyone in the room that Bill Binney knows what he's talking about. He and Wiebe, with their colleague, Ed Loomis, and others on the signals intelligence (SIGINT) team recognize a worthless program when they see it. In contrast, they designed a valuable one: Thin Thread. A miracle of signals intelligence, Thin Thread could scan through the metadata on calls and messages, identify suspect connections based on past intelligence and current contacts, and throw the rest of the data away.

Besides its economy, Thin Thread had one other compelling feature: it was legal. In developing the program, Binney and his team solved one of the NSA's most sensitive and difficult problems. They structured Thin Thread to separate US calls and emails from the rest of the digital heap and automatically encrypt the data to avoid warrantless spying on US citizens. If Thin Thread found that a US-based phone number or IP address contacted a known terrorist suspect, the agency could go to the FISC for a warrant.

When the NSA tested Thin Thread, the program immediately identified targets for investigation and encrypted the identities of US callers.

"And then you know what happened?" Drake asked during the meeting at GAP.

"What?"

"They shut it down."

There was silence in the room.

"But why?" asked NGO lawyer X.

The three NSA whistleblowers looked at one another. Finally, Drake cocked his head, and a pained expression crossed his face. "Too many careers and contracts were tied to a different program."

Given the fact that 9/11 happened less than one year after the NSA shut down Thin Thread, there was nothing more to say. For his part, Binney was extremely disturbed about the NSA's failure to deploy the program. Thin Thread was ready to go months before 9/11, and he planned to apply it in Afghanistan and Pakistan, where it would be most effective: he was (and is) convinced that if the NSA had put Thin Thread online when it was ready, 9/11 would not have happened.[6]

Documents Edward Snowden began to disclose in June 2013 tell the whole sorry saga of the NSA and its corporate partners in the years after 9/11. Both what they have and have not done.

Back on its heels and lacking a mission after the Cold War ended, the NSA got new life with the advent of the Global War on Terror. Its budget more than doubled. Billions of dollars now disappear annually into intelligence contracts. Before Snowden told us in the summer of 2013, we did not know how much the US government spent on intelligence. Now we know: $52.6 billion annually.[7] Of that amount, 70 percent goes to private corporations.[8] Because, as taxpayers, we who fund the whole business have no right to know what we're paying for, the setup is ripe for waste and fraud.

In America, there's a curious disconnect between taxpayer concerns about the cost of social programs and the cost of security operations and war. It's as if politicians don't notice that Medicaid and the NSA are run by the same outfit—the US government. If the government wastes money on health care programs for poor people, which, by the way, are publicly and constantly audited, imagine what's going on at the NSA, the CIA, and the rest of them, where much of the financing is secret.

The possibilities for waste in government agencies with few budget constraints and little oversight are almost unimaginable, and the one agency where the budget is most generous and the external oversight is weakest is the Pentagon. When he ran the Army's Intelligence and Security Command, for example, General Keith Alexander, who later came to run the NSA, presided over the Information Dominance Center, designed by a predecessor to resemble the bridge of the Starship Enterprise from *Star Trek*. It had everything: hardwood paneling, odd trapezoidal chrome and glass cabins, and a huge TV screen on the wall so the little man in the glittery uniform could monitor the world while sitting in his great huge leather captain's chair. Those who have been there swore that the politicians Alexander invited to tour the place could also sit in the big chair if they wanted.[9]

All of this, of course, was assembled with public money.

The US government, which is huge and cumbersome and bureaucratic, is given to cronyism and ineptitude unless subjected to meaningful oversight. If no one is paying attention, public money can buy props and toys to shore up the egos of generals. This has been repeatedly exposed, and yet there is no effective watchdog for the intelligence world or the Pentagon. Their money and their programs are classified.

This is why war is so profitable. When the country's at war, the budget floodgates open and secret money pours out, funding black programs that lack accountability. And when we're at war, anyone who brings up even the possibility of fraud in the intelligence world feels the full weight of the Justice Department come to bear against him—or her. We know this because it happened.

On July 26, 2007, in the early morning, Bill Binney was taking a shower when he thought he heard a commotion downstairs. He couldn't be sure over the rush of water. He pulled back the shower curtain and found himself looking into the barrel of a Glock. The agent behind it wore a Kevlar vest that read FBI, and the gun was pointed directly at his head.

"Whoa," Binney flinched and dropped back. He waited a beat. "Do you think I could get dressed here?" he asked.

Binney dressed quickly and hurried downstairs. His wife and his youngest son were home, and he knew they would be terrified. He was right. They huddled in the living room as the FBI raided their house. By the time Binney got to them, the ransacking was well underway.

FBI Special Agent Paul Michael Maric, whom Binney had met before, broke away from a huddle in the hallway and presented him with a search warrant: a thick blue document with a long list of articles the team could confiscate. On the list was the book *State of War* by James Risen, a book that documented secret domestic surveillance.

Inspecting the warrant that morning, Binney, a long-time veteran of the Cold War and the battle against totalitarianism, felt a chill. The fact that it listed Risen's book confirmed for him that he was caught up in a leak investigation that many at the agency were watching warily. Published two years before, the book contained information about surveillance that the author should not have known. Agent Maric allowed Binney a few moments to inspect the warrant, and then separated him from his wife and son.

"Out back," Maric told him and steered him through his kitchen to the back porch. There, Maric told Binney to sit and began interrogating him.

Maric's questions were specific, and he brought up details about classified operations, describing NSA sources and methods in the unprotected space of the back porch. Binney became increasingly concerned. Here was the FBI, pursuing information about security breaches and leaks, openly describing classified operations without precaution. Binney, a high-level NSA specialist, knew that if anyone's house was bugged by a US enemy, his was. The FBI, however, on that particular day, didn't seem to care.

The questioning continued, and the day grew hotter. Maric wanted a name. The agents were after someone, but Binney wasn't helping. He couldn't. He knew there was a leak investigation, but he wasn't Risen's source. Finally exasperated, Maric yelled at him: "Tell me something that will implicate somebody in a crime!"

At that, Bill Binney shut down. This was a home invasion pure and simple by armed FBI agents. He was being attacked by his own government.

The attack that day was part of a coordinated raid on the homes of three NSA specialists, and Diane Roark, a senior staff member of the House Permanent Select Committee on Intelligence (HIPSCI). It was an attack many years in the making. For much of that time, Bill Binney, who headed a cryptographer team, worked with his group to develop Thin Thread and solve the NSA's primary problem during the 1990s. The analysts had to makes sense of the ocean of data pouring into the NSA daily, isolate real threat information, and protect the privacy of Americans. At a cost of about $300 million for full deployment, Thin Thread came in under budget, on time, and up to spec. Bill Binney, Kirk Wiebe, and Ed Loomis were pleased and planned to deploy it.

There they hit a wall, and nothing moved, even as they went higher up the chain of command looking for a green light. They spoke with Bill Black, the deputy director at the NSA, and finally with NSA director Michael Hayden. Neither would commit to anything.

In fact, Hayden didn't want Thin Thread and would never use it, although neither he nor Black would say so. Even as Binney sketched out for Hayden what Thin Thread could do, the NSA director was asking Congress for an additional $3.8 billion to develop another surveillance program: Trailblazer. Binney and Wiebe got orders to merge Thin Thread's data sweep with the embryonic Trailblazer, now to be produced by SAIC, Bill Black's former employer. The initial amount to be spent on Trailblazer was about $1.2 billion, $900 million more than full deployment for Thin Thread, without the fine-tuning that made it legal or the real time analysis that made it effective.[10]

At this point, Binney, Wiebe, and Loomis began to suspect that a financial force was driving NSA decision-making on security surveillance. In April 2000, they contacted Roark at HPSCI and briefed her. Reaction from NSA director Michael Hayden was swift and furious. He transferred both Binney and Wiebe to the technology division at the agency, where they had less access to congressional staff members.

At the same time, Hayden sent a memo to the "NSA Workforce," informing the entire agency staff that if anyone else decided to report his decisions to Congress, they would regret it.[11]

Seventeen months later, on a bright blue September day up and down the US east coast, a cabal of fanatics attacked the World Trade Center in New York and the Pentagon outside Washington with a coordinated hijacking

of commercial airliners loaded with passengers and fuel. The towers caught fire and fell. The Pentagon itself seemed mortally wounded, and the country froze. Like a scene from a sci-fi horror movie, lower Manhattan and downtown DC filled with panicked and fleeing office workers and then stood deserted. No one knew what came next. Across America, air traffic control grounded all planes, and the stock market crashed and closed as TV stations rebroadcast the second plane hitting the South Tower of the World Trade Center over and over again.

It's difficult to envision the complacency before and the panic just after September 11, 2001, in the management suites of the NSA. After the 1993 World Trade Center bombing, the jihadists had gone quiet here in the homeland, but that attack was enough of a scare to crank up the contract machine and bulk up the budget for electronic surveillance in an agency hurting from the end of the Cold War. By 2000, Hayden & Company weren't all that worried, they thought they could shut down Thin Thread and fool around for a few years with Trailblazer prototypes and PowerPoint presentations showing what SAIC was about to produce in exchange for $3.5 billion.

Then, with the shock of 9/11, the threat was suddenly real. Congress was asking questions, but Trailblazer wasn't ready and wasn't even scheduled to be for some years. So Hayden did the logical next best thing: he picked up elements of an espionage program that Binney had developed for surveillance of the Soviet Union and used them to spy on Americans. Because the 9/11 hijackers were based inside the United States, the NSA turned a program designed for foreign surveillance around and used it instead for dragnet domestic surveillance. The program soon had a new name: Stellar Wind.[12] And the alternative acronym for the NSA—Never Spy on Americans—was no more.

A precursor of the programs Edward Snowden revealed, Stellar Wind enabled wholesale surveillance of Americans beginning shortly after 9/11.[13] In effect, the NSA, with the blessing of the Bush White House and the Justice Department, secretly did away with the Fourth Amendment to the US Constitution just like that.[14]

The operation of the NSA after 9/11 is a cautionary tale about secrecy and profits. Senior managers made the wrong decisions consistently, and no one stopped them because no one who knew the whole

picture, and objected, could talk about it. Those who did know and who tried to object were silenced.

As the 9/11 Commission reviewed the lapses in US defenses that allowed the attacks to occur, the phrase "connecting the dots" entered the popular lexicon, as in "The intelligence services failed to connect the dots." Nonetheless, in the aftermath of 9/11, neither the CIA nor the NSA seemed to concentrate on more effective dot-connecting, which was exactly what Thin Thread would have done. Instead, the NSA wanted Trailblazer, a program that merely collected billions more dots. After years of this, the operative question is: just how many dots does the government have about each of us?

The answer is: too many because Stellar Wind was the real deal. Trailblazer, in the end, became a string of big-bucks contracts for SAIC that never produced a working program. Stellar Wind, however, unencumbered by privacy concerns, was sinister in the extreme. The program ran for years, sweeping up hundreds of billions of data points on US citizens, as if we were all plotting subversion. The Bush administration, which authorized it, and the NSA, which directed it, labored diligently to ensure that the American public remained ignorant of what was happening.

Very few people in Washington knew anything about Stellar Wind. In fact, no one outside a small circle of White House, NSA, and Justice Department officials did. Nor did anyone outside the circle really know how the program operated, until December 16, 2005, when James Risen and Eric Lichtblau published an article in the *New York Times* exposing the NSA's warrantless surveillance. The article opened with a dramatic statement:

> *Months after the Sept. 11 attacks, President Bush secretly authorized the National Security Agency to eavesdrop on Americans and others inside the United States to search for evidence of terrorist activity without the court-approved warrants ordinarily required for domestic spying, according to government officials.*[15]

On January 29, 2006, there was a second news bombshell. Although it was an ordinary mid-winter day for most Americans, it was a disaster for the cadre of NSA insiders managing Stellar Wind and concealing the Trailblazer losses. The morning dawned cold and clear on the Chesapeake Bay as the Sunday edition of the *Baltimore Sun* hit front walks and stoops

around the city with the most explosive story of the author's career.[16] Siobhan Gorman, then a reporter for the *Sun*, began publishing a series of articles that exposed the gross waste and incompetence attached to the nonfunctional Trailblazer surveillance program. Coming on the heels of the December 2005 *New York Times* article by Risen and Lichtblau, the Gorman exposé infuriated the upper echelons at the NSA.

At the Justice Department and throughout the intelligence community, the search was on for the whistleblower.

Ironically, the reaction of the Bush White House, the NSA, and the Justice Department to September 11 unfolded according to the classic terrorist strategy. Terrorist groups are relatively small scale when compared to their targets; their leaders realize that their isolated attacks—even one as spectacular as 9/11—cannot topple a targeted regime. The regime's own extravagant reaction to the attack, however, does the rest of the work. Struck by a bomb—or by an American Airlines plane—the liberal regime clamps down on dissent in ways that make it unpopular, until the formerly free citizens themselves protest. Then the regime spends its wealth on stiffening repression rather than on public goods, so that it becomes increasingly despised and hated. No longer does the government help finance jobs, education, and health care. Instead, it sends tens of thousands of previously harmless young humans to distant countries for obscure reasons, where they die ignominiously or return home useless and wrecked, needing a lifetime of care, which the government no longer provides, either.

This is, in all likelihood, exactly where we are.

This page intentionally left blank

CHAPTER 2

Official Secrets: Absolute Control

Reason to be afraid #2

Control of information by the government-corporate complex is expanding.

The top-secret world the government created in response to the terrorist attacks of Sept. 11, 2001, has become so large, so unwieldy and so secretive that no one knows how much money it costs, how many people it employs, how many programs exist within it, or exactly how many agencies do the same work.[17]

On July 19, 2010, the Washington Post published an investigative story by Dana Priest and William Arkin that revealed the expanding parameters of the security state. The information that the NSA and the Justice Department struggled for years to control was seeping out, despite the attacks on the NSA whistleblowers and the censorship and harassment of journalists.

The effort to conceal the government's secret surveillance programs undoubtedly ramped up after Alberto Gonzales had a brush with perjury three years before the Priest/Arkin story appeared. Bush's hapless attorney general nearly revealed in an open congressional hearing that there were more surveillance programs than the Senate knew about. Gonzales admitted to "other intelligence activities," beyond the so-called Terrorist Surveillance Program, in a testy back and forth with Senator Charles Schumer.[18]

The FBI raids on the homes of the three NSA whistleblowers and Diane Roark occurred two days after Gonzales referred to "other intelligence activities," and four months later, on November 28, 2007, the FBI raided Thomas Drake's house. Drake was the official who communicated with Siobhan Gorman at the *Baltimore Sun*.

The FBI incursion and search of the Drake house was the same drill as the attacks on the others: a dozen or so agents stormed across the lawn in the early morning. The raid lasted eight hours, and toward noon ABC News and Fox News drove slowly up the street outside and parked their large boom vans at the curb to film it. The episode was broadcast twice that night and the next morning. For weeks afterward, Drake had to explain to his friends and neighbors why the FBI treated him like a dangerous criminal, a spectacle they'd seen on television repeatedly the day it happened as well as the following day.

The FBI raids in 2007 were one of the first manifestations of the extreme steps the government would take to secure its secrets. After 9/11, the US Defense Department both expanded and tightened its security regime, but it took awhile to build it out and cover it up. According to investigative journalists Priest and Arkin, 1,271 government organizations and 1,931 private companies in about 10,000 locations across the United States worked on counterterrorism, homeland security, and intelligence.[19]

Despite the campaign promises in 2008, the Obama administration did not arrest the trend toward more security-related secrecy. In 2011, Obama's agencies made 92 million decisions to classify documents, a dramatic increase over years past.[20] The following year, the Public Interest Declassification (PID) board wrote the president about the dangers of increasing secrecy:

> *At its most benign, secrecy impedes informed government decisions and an informed public; at worst, it enables corruption and malfeasance.*[21]

The extent of information collected and stored at public expense—but withheld from the public—is astonishing. The PID board's 2012 report identified one government agency that was classifying one petabyte of new data every 18 months, the equivalent of 20 million filing cabinets filled with text, or 13.3 years of high-definition video.[22] Moreover, the cost of storing and safeguarding all of this is high: roughly $11.3 billion in 2011, up from about $4.7 billion in 2001.[23]

The knowledge we now have about the national security operations of the United States suggests that we've moved from an embryonic position—where data collection is voluminous and secret but disorganized—to a more

sophisticated state, in which the government's information about Americans is categorized, searchable, and centralized. The national security picture exposed by Edward Snowden in 2013 reveals a domestic surveillance system that is greatly advanced over the one Priest and Arkin described only three years before.

The government of the United States has two ways to withhold information from us, and they overlap for good measure. The first is to classify government documents as confidential, secret, or top secret for purposes of protecting national security. Classification withholds information from disclosure if requested under the Freedom of Information Act (FOIA). A second method is to invoke any of the nine exemptions or three exclusions of FOIA, one of which withholds classified information.[24]

Shortly after he took office, Barack Obama committed his administration to openness and transparency. In choosing him to be president, Americans effectively showed their displeasure with the arrogance of the Bush/Cheney administration, which concealed the machinations of governing behind a veil of secrecy and national security.

Obama was a Democrat, not a Republican. He was a progressive not a conservative, and he represented a younger generation than Bush and Cheney. He was to be different. He said as much in a statement released on his first day in office:

> *My administration is committed to creating an unprecedented level of openness in government. We will work together to ensure the public trust and establish a system of transparency, public participation, and collaboration. Openness will strengthen our democracy and promote efficiency and effectiveness in government.*[25]

It was not to be.

An assessment by the Associated Press (AP) in 2010 showed Obama using FOIA exemptions to withhold information more than Bush did during his last year in office, even though the Obama administration had received fewer requests for documents. The AP's review showed that after one year in office, the Obama administration had increased the use of virtually every FOIA exemption in order to withhold information.[26]

The record on the classification and declassification of documents is no better. Obama's own PID board wrote to him to say: "[P]resent practices for

classification and declassification of national security information are outmoded, unsustainable, and keep too much information from the public."[27]

Thirty-three civil society organizations supported many of the board's recommendations and also wrote the president to emphasize the importance of the issue:[28]

> *[T]ransformation of the classification system has become a democratic and security imperative, and the critical moment in this effort has now come."*[29]

That was April 23, 2013. The moment came and went.

Despite these consistent signs of growing secrecy in executive agencies and the regular warnings from sources familiar with government secrecy, the Snowden disclosures during the summer of 2013 occasioned an uproar among experts on national security law, cyber- intelligence, and document classification. People did not know what to think when the enormity of the revelations hit them. There is no precedent for what Snowden showed.

The disclosures came one after the other in digestible increments: metadata, PRISM, XKeyscore, illustrated with slides and official documents. Nothing was simply the opinion of the whistleblower. All of it was documented.

Thanks to Snowden, everyone who read or saw the news anywhere knew, for example:

1. The US national intelligence program includes sixteen spy agencies that directly employ 107,035 people.
2. For fiscal 2013, the classified "black budget" requested of Congress by the White House was $52.6 billion. The amount far exceeded what we previously thought to be true.
3. The CIA and NSA increasingly engage in massive cyber-operations to hack into foreign computer networks of both allies and enemies to steal data and sabotage infrastructure.

Perhaps most unsettling, the United States has spent more than $500 billion on intelligence since 9/11, an amount that exceeds equivalent Cold War spending levels.[30]

In brief, the Snowden disclosures show that the Constitution and the government of the United States have parted ways. We are no longer

a democratic nation of laws. That's new in America. We've had our differences about various presidents, and most of us have little respect for the Congress, but in general, the judicial system enjoys a certain deference, and the country—including our government—as a whole is the subject of devotion. We still place our hands over our hearts and pledge allegiance to the flag—and to the republic for which it stands. The perception that the machinery of the state—including the executive, legislative, and judicial branches—does not respond to the will of the people, actively conceals its law breaking, and when exposed, deceives in a coordinated and deliberative fashion, is a first in living memory.

The Watergate scandal of the 1970s was also a constitutional crisis, but it was confined to the executive branch. It was also confined to one president, Richard Nixon. When he was gone, it was over. The same is true of the Iran-Contra scandal. Ronald Reagan broke the law and defied congressional intent, but the legislature reacted when the news broke, and the secret program stopped.

This situation is far worse than that, taking in as it does Presidents Bush and Obama—two very different presidents—their respective Justice Departments and intelligence agencies, the Foreign Intelligence Surveillance Act Court and its judges, and the House and Senate Intelligence Committees. When looked at that way, it's difficult to name a strong actor with both the skills and the incentive to right the ship of state. No one in government is empowered to expose the totalitarian infrastructure at the heart of the democratic government of the USA.

The seepage of power from elected officials—such as the president—to the surveillance agencies appeared clearly in early September 2013, as Washington, DC, prepared for the October state visit of President Dilma Rousseff of Brazil. The White House planned a formal state dinner and a heavy schedule of meetings to showcase the close relationship between Brazil, the new powerhouse in the Americas, and the United States. The two governments also planned to consider an arrangement between Petrobras, Brazil's state-run oil company, and the US government to allow US companies access to oil deposits trapped under a salt layer in the Atlantic waters off the Brazilian coast.

On September 8, 2013, the Brazilian newspaper *O Globo* reported that the NSA had penetrated the internal computer network at Petrobras, according to documents released by Edward Snowden. The news

provoked a furious reaction in Brazil, as negotiators realized that US officials had outflanked them by peering into the Petrobras negotiating strategy. It added insult to injury because documents released by Snowden the week before showed that the NSA had hacked Rousseff's personal email and that of her close aides. As the conflict broke into the open, the White House released a weak and meaningless statement that did not acknowledge the NSA's invasion of the sovereignty of a friendly nation and did not commit to holding anyone accountable.[31] Rousseff cancelled the state visit with an angry public protest, and in the United States, the press highlighted the fact that the Defense Department's statement in August, denying that the NSA engaged in industrial espionage, was a lie.[32]

The Snowden documents have badly eroded the legitimacy of the US government both domestically and internationally. No one in government, from the White House to the Congress, has been able to state anything close to a reasonable and truthful case for the clandestine actions of the NSA.

After the *Guardian* released the FISC order to Verizon Business Systems, President Obama told an interviewer that the court is transparent and that it is part of a system of checks and balances. The statement, aired on broadcast television, was preposterous. The court order is secret, and it is based on a secret interpretation of the law—an interpretation that one of the law's principal author's asserts is a gross violation of congressional intent. In this one exchange, Obama damaged the credibility all three branches of government. The executive branch, in the person of Obama, is either ignorant or lying. The judicial branch is secretly defying the legislature, and the legislature, which is responsible for oversight, is not paying attention.

Deputy Attorney General James Cole tried to help the NSA out of its credibility hole in the early summer. In testimony before the House Intelligence Committee, he described the elaborate monitoring and oversight that kept the NSA in check. He did admit, however, that: "Every now and then, there may be a mistake."

Not long after Cole made this statement, we learned from the *Washington Post*:

> *The National Security Agency has broken privacy rules or overstepped its legal authority thousands of times each year since Congress granted the agency broad new powers in 2008, according to an internal audit and other top-secret documents.*[33]

This Material Has Been Excerpted From

The Rise of the American Corporate Security State
Six Reasons to Be Afraid

by Beatrice Edwards
Published by Berrett-Koehler Publishers

For more information, or to purchase the book,
please visit our website
www.bkconnection.com