PART ONE | THE ROAD TO 9/11

Introduction | The Gift

A cold drizzle is falling on the Pentagon parking lot. The memorial for those who died here on 9/11 was dedicated in 2008—just a year ago—but it's almost deserted. In nearly four years at the Department of Homeland Security (DHS), I never managed to visit any of the 9/11 memorials. Now that I'm out of office, along with the rest of the Bush Administration, I have time to pay a quiet visit.

I don't like the place. Flat and unadorned, it feels like an extension of the vast Pentagon parking lot. The trees are scrawny, and the grounds are a utilitarian expanse of gravel and rain-slick paving stones. Beyond the sparse vegetation and a concrete wall, traffic hisses and thrums on a highway.

I think I know what the designers had in mind. They wanted everything understated and austere. There's a bench and a lighted pool of water for each victim who died here. Each bench bears a victim's name. The benches and the paths trace the course that Flight 77 must have taken—smack into the massive west wall of the Pentagon that looms nearby, gray in the rain.

The site is all about good taste and minimalism. Security is tight. The grounds look as though they're swept clean each night to remove any trace of the day's visitors, their litter, their mess, their grief.

But I'm not in the mood for good taste. The place feels cold and runic. Some benches arc toward the building; others arc away. Some of the pools have names in them; most don't. The benches are arranged by year, from 1998 to 1930.

I've come for a memorial; instead I've found some kind of puzzle.

I practice law for a living, but off and on I've spent years in government. This last tour has been a tough one. DHS was a startup, begun in the wake of disaster and assembled on the fly. Two years in, DHS suddenly realized that it needed a policy office, and I got the job. A startup within a startup, the office had to be built from scratch.

Everything was up for grabs—policies, procedures, authorities, personnel. I knew that wouldn't last; slowly the demand for routine would crowd out innovation. So in the midst of chaos—uncertain budgets, borrowed staff, no backup—I felt the pressure to push new ideas and policies into place as quickly as possible. Early on, what matters is how good your ideas are. Later, what matters is whether your ideas have been vetted with every office that thinks it has a stake in the decision.

So all at the same time, I had to build the office, recruit great people, solidify the budget, and put a solid policy structure under much of what DHS did.

I did that. Now I'm tired. I need time to clear my head.

So here I am, thinking about the people who died a few yards away—the people whose deaths drove me back into government. I am taking stock of what I've actually managed to do for their memory.

The place is nearly deserted. A handful of other people wander the paths. Two youngsters skip up to me. They want to know where the broken limestone is.

I look around. The place is as sterile as a French park. There's no place for anything broken.

"It's here somewhere. We have to find it for our class."

Great, I think. A puzzle and a scavenger hunt. I try sitting on one of the benches. It's sopping. My pants soak through. I stand.

That's enough. Time to go.

But the puzzle nags at me. The dates are easy enough. They're birth years. The benches arcing toward the building are for the passengers on Flight 77. The others are for victims who died in the Pentagon.

I look for my birth year—1947. Eleven dead. More than any other year. That seems fitting. By 2001, we baby boomers had shaped the

United States to reflect ourselves. We were what the attackers hated. This is our fight.

I'd known that from the start. On the day of the attacks, I looked out of my law office window and saw the smoke rising from the Pentagon.

I felt at least a bit of responsibility for our failure to stop the attacks.

In the 1990s, after a term as the National Security Agency's top lawyer, I spoke out in favor of keeping a wall between spies and cops. The idea was simple enough. Agencies like the National Security Agency (NSA) gathered intelligence on a global scale, and they rarely observed the legal constraints that applied to domestic policemen. To protect the civil liberties of Americans, it only made sense to separate intelligence gathered in that way from evidence assembled in a criminal investigation. With a wall between the two, criminal investigators from agencies like the Federal Bureau of Investigation (FBI) would be forced to observe the legal restrictions that went with criminal investigative tools. They wouldn't be tempted to take the shortcut of using intelligence that had been gathered with less attention to civil liberties.

That was the theory, anyway. In practice, the wall crippled our last, best chance to catch the hijackers before September 11, 2001. In August of that year, the wall kept the FBI from launching a full-scale criminal search for the hijackers—even though all of our security agencies were expecting an imminent al Qaeda attack, and even though both the FBI and the Central Intelligence Agency (CIA) knew that two dangerous al Qaeda operatives had entered the United States. The failure to track those operatives down wasn't a matter of incompetence or a failure to communicate, at least not in the last weeks. FBI criminal investigators spent the last part of August begging for a chance to track the terrorists. They were shut down cold—by lawyers who told them the wall simply could not be breached.

I wasn't the most enthusiastic proponent of the wall. I thought that the civil liberties dangers it was supposed to ward off were probably

more theoretical than real. But I saw no harm in building in an extra margin of protection for civil liberties. If nothing else, the wall would reassure privacy advocates in the courts, in the newspapers, and on Capitol Hill that intelligence would not be misused. It was insurance, not just for civil liberties, but for the intelligence agencies themselves. For both reasons, I thought, it was best to keep the wall high.

It made eminent sense inside the Beltway.

Until the world outside the Beltway broke through, just a few yards from where I'm standing.

Slowly, as I wander back and forth among the rows of benches, the puzzle starts to fall into place. The oldest passenger was seventy-one; the youngest was three. The names of family members who died together are engraved in each other's reflecting pools. Husbands died with wives. Parents with children. Most of the passengers, though, died alone. Which would be worse, I wonder, facing death without a hand to hold or knowing that your spouse will die with you?

Close to the entrance is a knot of benches for children—two girls traveling with their parents and three eleven-year-olds without family. What was the hijacking like for these youngsters, I wonder, imagining the chaos as the passengers were forced into the back of the plane. At that age, I'd just assumed that adults were in control. They were the ones who made the rules, the ones who could always protect you when things got bad. For the first time, and the last, all those comfortable childish assumptions about the world had broken down.

The birth-year arrangement means that a long barren stretch of gravel separates the eleven-year-olds from the twenty-two-year-olds who worked in the building. Bereft of flowers and personal touches, all of the benches seem a little lonely; off by themselves, the children's benches seem lonelier still.

In the wake of the attacks, I recanted my support for the wall. I testified to the 9/11 Commission about the risks of overprotecting civil liberties. But that didn't seem like enough. I wanted to do more. I seized a chance to work for the Robb-Silberman Commission that

investigated our intelligence failures in Iraq; I helped make recommendations about how to keep weapons of mass destruction out of terrorists' hands.

And finally in 2005 I joined the brainy, hard-charging Michael Chertoff at the Department of Homeland Security (DHS).

Wiser career decisions have been made; at the time, DHS was being widely mocked as disorganized and obsessed with duct tape and color schemes for terrorist warnings. But I've never turned down a chance to work in government with someone I respect, and bringing order to DHS policy was a chance to undo some of the harm that the wall had caused.

I had to decide where DHS policy could make the most difference. One place where the Department of Homeland Security had sole responsibility was the border. In fact, the one unquestionably good idea at the core of DHS was uniting border responsibilities that had been split among three cabinet secretaries. Neglected by all three, border security had collapsed under the weight of ever-increasing jet travel. Border officials were waving more and more visitors through our immigration and customs checkpoints with only a cursory look.

Al Qaeda sent twenty hijackers to carry out the 9/11 attacks. All but one got past our border defenses. Even stopping that one hijacker took an act of courage on the part of the border agent; in those days, keeping a Saudi traveler out of Orlando could easily trigger complaints about discrimination and lost tourism.

We had to rebuild those defenses—but without discouraging international travel. That would require clarity and determination. Already, the toughest measures were being stalled.

Civil liberties groups, far from feeling abashed at the role their doctrine had played in 9/11, were loudly fighting DHS's new security measures. They had an eager audience abroad; in fact, our allies in Europe had already forced DHS to rebuild the wall between law enforcement and intelligence, at least as far as border data was concerned. The Europeans had threatened to withhold data on transatlantic travelers unless DHS promised to keep that data from intelligence agencies—and even from other parts of the department.

I am beginning to see the appeal of this austere, cerebral memorial. I don't know most of the victims, and neither will others who come here. The memorial is not meant for memory but for connection. It tells us nothing but the names and the birth dates of the victims, but I see now that those are enough to build a web of connections. Just those facts drain some of the anonymity from the dead. They are all that's needed to pull us out of airy sentiment and make us feel instead the concrete loss the victims and their families suffered.

It's not much, in fact it's sadly impersonal, but it's more than most memorials can convey.

With Secretary Chertoff's full support, I fought back against the determined resistance of airlines, foreign governments, and civil liberties groups; we put in place a coherent border inspection strategy despite them. We hadn't won every battle when I left, but we were winning, and it looked as though the new Secretary and the new administration would keep up the fight. That was satisfying.

But satisfaction was not what I was feeling. I've never understood political memoirs that are a long tale of successes. In my experience, government rarely offers clear victories. The more ambitious your goals—if you want to do more than enjoy the limo rides, if you want to solve problems and reshape policies—the more likely you are to fail. In ways that hurt so bad you'll never forget them.

Maybe other government memoirists are better at putting their failures behind them. But I can't, maybe because I fear that my failures will end up costing the country as much as the failures that led to 9/11.

The same exponential changes that undercut border defenses are at work elsewhere. Moore's Law, which has predicted decades of exponential growth in computer capabilities, is creating scary new vulnerabilities here at home; soon a host of criminal and military organizations will be able to leave individuals bankrupt and countries without power or a financial system. Similar exponential changes in biotechnology will empower a generation of garage hackers who may

or may not end up curing cancer but who will certainly end up making smallpox at home.

Unlike jet travel, these technologies have not yet been misused on the scale of 9/11. And without three thousand dead, business, international, and civil liberties groups have been ferocious in opposing any action that might head off disaster. I struggled to sound the alarm, to prepare the country for computer network and biological attacks, but I failed more often than I succeeded.

That's over now. I've been relieved. The new administration has embraced civil liberties rhetoric with enthusiasm. Some of them seem convinced that they have a mandate to roll back any security measure that reduced privacy or inconvenienced the international community. I don't think that will happen with border security, but the new administration's deference to privacy groups and international opinion will make it far harder to do anything about the new threats.

Maybe, I think, they're right not to pick those fights. Maybe Americans are tired of battle, tired of remembering 9/11, tired of its lessons. Perhaps the fight against the new threats will just have to wait until something bad happens.

The rain is growing heavier. The low clouds are darker. The lights in the pools have begun to glow. I'm ready to leave.

Passing a bench, I see something: a tiny dot of color in the vast, sterile park.

It's a bit of glass, like a clear blue marble left in the kiln too long and melted into an oblong. It's easy to miss. I've already walked past it once. But it wasn't dropped at random.

It sits centered at the end of one bench. In this scrubbed, cerebral monument, it looks almost defiant, an act of personal rebellion against the clean lines and uniformity.

The name on the bench is Ronald Hemenway, electronics technician first class. He died at work in the Pentagon. He was thirty-seven—the right age to have a wife and young children still feeling the pain of his loss eight years later.

I imagine mother and child sitting together on the bench. They glance carefully around and slip the blue stone from a pocket. A child's hand centers it at the end of the bench, just so.

A gift of memory. For a father. For a family.

For all of us.

It is memory that will save the changes DHS has made at the border. We remember what weak defenses cost us.

But the memory of 9/11 may not save us from the new threats. When catastrophic terrorism returns, the terrorists will use weapons that have already been deployed—by governments, by business, by all of us. Like jet travel, the weapons will be technologies we value. If we do nothing, these technologies and the new powers they confer will eventually be used against us in shocking new ways.

I tried my best to manage those new risks as aggressively as we were dealing with border security. But with the new technologies, that was a lot harder; privacy groups, business, and the international community resisted change with fervor. And too often they won, blocking our efforts to head off the greatest risks.

Those are the failures I most regret. The lesson I learned from the wall and 9/11 was simple: The civil liberties advocates of the time did not know where to stop. They only stopped campaigning for the wall after it had killed three thousand Americans (and some didn't stop even then). They couldn't see the line between reasonable protections and measures that crippled our effort to fight terrorism. And they still can't. They and their allies in business and international organizations are natural conservatives, opposed to any change that might help government fight terrorism in new ways.

I'd chosen not to fight these entrenched interests in the 1990s. When I left the National Security Agency, I'd written a long article that endorsed a wall between spies and cops. I've spent years undoing that mistake.

Now I am leaving government again, and writing again—and hoping to keep others from making the same mistake.

Call it a gift of memory.

1 Skating on Stilts

In a way, all truly popular technologies resemble the bicycle. A bicycle is an implausible thing. To see how implausible, take it out in the street and stand it up. Now let go.

It falls over.

Stand it up in the street and put a man on it; it falls over faster, and he's likely to skin his knee. The thing is utterly unstable.

So who would imagine that the way to solve the instability is to put a man on it and roll the bicycle down a long hill?

Nobody. It defies common sense that something so unstable could become more stable when it's moving. Perhaps that's why nobody imagined the bicycle, at least not for a couple of thousand years after it became perfectly possible to build one.

It took a lot to make the bicycle imaginable. In 1815, the Battle of Waterloo brought an end to nearly twenty years of European war. At the same time, the largest volcanic explosion in recorded history occurred, at Mount Tambora in what is now Indonesia.

The next year, summer never came. Snow fell in every month. Crops failed. Without the crops, pack animals died.

Everyone in Europe cast a wary eye on St. Helena, where Napoleon was imprisoned, and wondered how they'd fight a war without pack animals.

The following year, in 1817, a German official named Karl von Drais showed them how. He invented the bicycle. He demonstrated that soldiers could carry heavy weights quickly over long distances by riding and pushing a crude bicycle. His model weighed nearly fifty

pounds, was built of wood and had no pedals. But once he showed that it worked, others improved the design until by the turn of the century the bicycle as we know it was everywhere.

The Romans—perhaps even Alexander the Great—could have built a bicycle like Karl von Drais's, something with crude bearings and no pedals.

They didn't, though. Why not? Here's my theory: The whole idea was simply implausible. Who could imagine traveling at high speeds on a vehicle that can't even stand upright by itself?

But moving forward is the key to the bicycle's stability. A bike moving at one mile per hour is a lot more stable than a bike at rest, and at five miles per hour it's more stable still. At even higher speeds, the bike can adjust faster and roll over obstacles that will bring it to a dead stop at lower speeds.

Go faster and feel safer. We all remember discovering this amazing rule as kids. If 5 mph is good, 10 should be better. And it is! We remember how it ends, too. Fifteen mph is better still. And twenty. Everything is better on a bike when you go faster. Until, quite surprisingly, it's not.

That's when you discover that falling off a bike at 30 mph means something a lot worse than a skinned knee.

And suddenly the Romans don't look quite so dumb.

Lots of technology is like the bicycle. It seems implausible at first. As Arthur C. Clarke once said, "Any sufficiently advanced technology is indistinguishable from magic."[1]

Once we relax and learn to trust it, it really does give us new, nearly magical powers. It gets better and better, faster and faster.

Then it starts finding new ways to kill us.

In a way, that's what happened on September 11, 2001.

Technology—cheap commercial jet travel—made the attacks possible. In fact, it made attacks like September 11 more or less inevitable.

It may be hard to remember now, but air travel was once seen as the great technological achievement of the twentieth century. Futurists marveled at how it would change our world.

In 1907, as heavier-than-air flight was just becoming a reality, Alexander Graham Bell declared that it would not be long until "a man can take dinner in New York and breakfast the next morning in Liverpool."[2]

By the 1920s and 1930s, airplanes and air travel were to young men what computers became in the 1970s and 1980s—a way to revolutionize society, make a better world, and find a fortune. After World War II, the youngsters of the twenties and thirties set about building their dreams, and they succeeded.

As late as 1958, European flights were still a special event. That year, *Life* magazine ran a feature story "Off for Paris in Jet Time," describing a Pan American flight from Idlewild (not yet Kennedy) Airport in New York. Actress Greer Garson was in "deluxe" class, along with forty other passengers paying $909 for their round-trip tickets. Another seventy-one economy passengers, attired mostly in suit and tie, or dresses, also made the trip.[3]

Fifty years after Bell envisioned transatlantic travel, it was still remarkable enough to deserve a gushing feature in the preeminent magazine of the era.

That ended in 1959, when Boeing introduced its 707. The new jet cut flying time between New York and London from twelve hours to six. In an instant, international air travel went from luxury to commonplace. By 1965, 95 percent of transatlantic travelers were crossing in the fast jets of Pan Am and European airlines such as British Overseas Air.

In the seventies, Boeing introduced the jumbo jet. By then, jet travel had lost any resemblance to magic and had acquired an unfortunately close resemblance to, well, bus travel. Yet jet tourism kept growing. In 1950, air travelers flew about 28 billion kilometers. By 2000, that number had grown to three trillion.

In those years, international air travel had roughly doubled every five years. That's fifty years of exponential growth.

Any technology that grows so fast is going to have some unexpected effects. As it grew, jet travel brought a slow revolution to the border.

The U.S. border agencies now at the heart of the Department of Homeland Security were confronted with exponentially increasing international travel. As they watched, a rising tide of travelers slowly overwhelmed their 1950-era security measures.

Border checkpoints and searches, travel visas and printed passports—these things had changed little since the nineteenth century. Some were even older; written safe conduct passes for travelers go back to 1414 in England and the oldest, existing passport was issued in 1641 by King Charles I. Even the name "passport" reveals its antiquity. Passports were used to pass through the gate (the *porte*) in a medieval city wall. By the 1980s, though, the walls were down and the gate was open.

Border controls that depended on a serious inspection of individuals, their passports and their luggage, simply could not keep up. Security officials could not spend much time with each traveler. The lines at the border were getting too long.

By the 1980s, governments had begun to vie with each other to dismantle these border security measures. U.S. Customs abandoned individual inspection of travelers, allowing those with nothing to declare simply to stroll through the Green Lane. The United States also adopted the Visa Waiver Program (VWP). That program abolished our single most important restraint on foreign visitors entering the United States—the visa.

Visas are travel permits. Issued by a country's embassy or consulate abroad, they authorize the visa holder to travel to that country. The process of issuing a visa can be quite simple or quite elaborate, but it typically requires at a minimum that the applicant go to the embassy of the country he wants to visit to provide whatever information the consular official requires.

As a control mechanism, the visa is highly flexible. To discourage illegal economic migration, nations may grant very few visas in poor

countries—and those only to the well-to-do. They may also deny visas to potential troublemakers, criminals, or terrorists. They may insist that the local government vouch for the visa applicant. They may require that applicants fill out detailed forms, or provide fingerprints, to help in the clearance process.

These control mechanisms worked pretty well in the first half of the 20th century. But a flood of commercial jet travelers turned visas into costly barriers to casual travel—barriers that soon began to fall.

In 1988, the United States stopped requiring visas for nationals of Japan and the United Kingdom, and these governments did the same for Americans. The United States was certainly not alone. If anything, other countries moved further and faster. In 1985, for example, most members of the European Union began simply abolishing controls at their borders with other member states. In countries like Belgium, border inspectors were deployed only at international airports. Everywhere else, travelers were free to enter and leave the country without a glance from officialdom.

By the end of the 1980s, even the world's most notorious border barrier had fallen. The fortified iron curtain cutting Eastern Europe off from the West was broken—by governments and by crowds of citizens from East and West.

Soon, the retreat from border control measures became a rout. Thirteen years after admitting two countries to the VWP, we had opened our doors to two dozen. By 2001, half of all the foreign visitors to the United States—a million a month or more—were coming without visas. No American official laid eyes on these travelers, or even knew they were coming, right up to the moment they reached the immigration booth at LAX or JFK.

Even when visas were required, they were streamlined to eliminate the hassles, as well as the safeguards. In Saudi Arabia, for example, the U.S. State Department launched the Visa Express program in June 2001. The program allowed applicants to obtain a visa by submitting a two-page application to their Saudi travel agency instead of going to a U.S. consulate to provide visa information.

Commercial jet technology had triumphed. It had made mass international travel possible, empowering millions. And almost without noticing it, these millions of empowered travelers were eroding a system of border security that had existed for decades.

Border officials noticed, of course, but they could not resist the onslaught. If they insisted on the old controls, tourism and foreign investment would lag behind the rest of the world. As they saw it, they had only one choice: surrender the old control system or watch their country stagnate.

So they surrendered.

We all know what happened next.

Four years after the 9/11 attacks, I joined the Department of Homeland Security. Secretary Michael Chertoff asked me to create and run a policy office that would let DHS lift its head above the scrum of daily crises and think about its biggest challenges.

DHS was still a startup, barely two years old, and it had spent those two years getting organized, finding desks and office space—and at the same time frantically trying to build defenses against an unseen enemy. No one had had much time to think about the future. That was one of the reasons we needed a policy office, or so I thought.

I wanted to think about 9/11 in a new way. It seemed to me that it was an event driven as much by technological change as by evil men and government errors. Sure, there were evil men, and there were errors. But we had to get beyond the immediate mistakes and focus on the long-term trends that had made the attacks possible in the first place.

When we started tracing the roots of the 9/11 attacks, we realized how jet travel and a growing flood of travelers had wrecked our traditional border defenses. That's when we began to ask what other technologies might have in store for us.

Technologies like jet travel are seductive. That's why we flock to them. They give us more choices and more reach. Commercial jets allowed us

to work or play on any continent in a matter of hours. More recently, computers and the Internet gave us instant access to knowledge that once was available only to a handful of librarians. Biotechnology, a new, explosively exponential technology, gives us the power to create and design life itself.

Giving individuals the opportunity to use these tools, with the choices, reach, and power they confer, is a great thing—much of the time. It's like skating on stilts that get a little longer each year. Every year we get faster and more powerful. Every year we're a little more at risk. We are skating for a fall, and the fall grows worse every year we put it off.

Technologies that empower ordinary individuals also empower people like Osama bin Laden and Unabomber Ted Kaczynski. Commercial jet technology had been around for nearly half a century before nineteen men were able to use it to kill three thousand. But the possibility of something like 9/11 was inherent in the technology from the start.

The 9/11 Commission (formally known as The National Commission on Terrorist Attacks upon the United States) criticized officials for a failure of imagination in the run-up to the attacks. Even those who knew al Qaeda was planning an attack did not imagine domestic jet hijackings that ended in suicide attacks on national symbols. I resolved when I joined DHS to keep that failure in mind. Where else was our imagination failing us?

Once I began to look for other emerging threats, I realized that jet travel is not the only technology that puts Americans at risk. Computer technology and bioengineering are more recent. Their power to change our lives is still growing, and their future is harder to predict. But if we wanted to get ahead of tomorrow's terrorism, DHS had to begin thinking about future risks as well.

Based on my own experiences, I knew of two that were bearing down on us fast.

For decades, information technology has been driven by Moore's Law. One version of the law holds that the number of transistors that can

be cheaply placed on a chip doubles every eighteen to twenty-four months.

As chip capacity grows, the cost of computer power falls. A computer that cost $1 million in 1970 could be duplicated for $500,000 in 1972 and for $10,000 in 1984. By the end of the 1980s, personal computers were giving individuals capabilities that were once available only to government and the Fortune 500; electronic spreadsheets, word processors, contacts files, and email began expanding the capabilities of all.

Surely one of the oddest results of going to work for NSA was my initiation into the vanguard of this trend. The agency controlled encryption, and especially exports of encryption technology to other countries. But as cheap home computers made the Internet a potential source of mass electronic commerce, Microsoft and other software companies wanted to build encryption into their products. They rightly saw a need for more security if computer networks were going to carry large transactions.

"We're going to put encryption in your toaster," one Microsoft representative told me, invoking a day when every kitchen appliance would have its own Internet address.

To defend NSA's encryption policy, I had to understand this Internet thing and the changes it would bring. While I never fully accepted the techies' encryption policy proposals, I came to believe that they were right about the Internet. A revolution was coming. After leaving government I built a law practice around that insight. I represented dozens of Silicon Valley firms, including Netscape in the days before its IPO helped to launch the Internet revolution.

So I had a ringside seat as Moore's Law worked its magic. By the late 1990s, computing power that had cost $1 million in 1970 could be had for a hundred dollars.

Cheap computing and telecommunications (not to mention a gradually softening policy on encryption exports) did indeed create a mass market Internet. We were able to search the accumulated wisdom and folly of humanity in seconds. We could download books,

music, and movies—what we wanted when we wanted it. We could bank, play games, trade securities, salute friends, trash enemies, gossip, build businesses, lose and find lovers—all online.

Oh, and a few more things: we could be defrauded, robbed, extorted, and blackmailed—with stolen secrets—online, too. The industry push to incorporate strong encryption into their products turned out to be a red herring. Government did get out of the way, but even the strongest encryption didn't provide the security the techies thought it would. Crooks easily found ways around it.

But, as with commercial jet travel, the bad news about information technology arrived late—long after the technology had become indispensable. We were up on our stilts and skating hell for leather before we even noticed there might be a problem. It wasn't until the 1970s that some of the first hackers discovered they could obtain free phone service by fooling AT&T's computers, and it took until 1988 for the first computerized "worm" to clog the Internet. Computer viruses also emerged in the 1980s, passed from disk to disk. They were an annoyance, but little more. Most were written simply to show off the skills of the author.

But as we moved our lives online, criminals followed. Hackers discovered that there was money in compromising other people's computers. Spammers could use those machines to send messages without fear of being shut down. Online networks allowed foreign criminals to reach across borders without leaving home as Nigerian spammers learned to defraud gullible men and women in the United States and Europe.

Networks of compromised machines were marshaled into vast zombie armies that could attack a single website together, knocking it off line. For some sites, being off line even for an hour was so costly that they'd pay extortionate fees to stop the attack.

Exploiting computer security holes wasn't the cyberspace equivalent of spray-painting graffiti on subway cars anymore. It was a new form of organized crime. It paid well enough to attract real talent. And that talent found new ways to make computer hacking pay.

Compromising the computers of credit card processors and merchants allowed identity theft and credit card fraud on a massive scale. Sending booby-trapped emails to known individuals, in contrast, might only compromise a single machine, but it would allow the criminal to steal every name and password used on the machine—and to empty the bank account of the victim.

As the criminals demonstrated what could be done online, governments followed their example. Governments didn't steal money, though. They stole secrets. Protected from prosecution and motivated by patriotism, government hackers turned out to be even more effective than the crooks. Countries that depended on computer networks began to wonder whether they had any secrets left.

Bad as it was to lose secrets, that wasn't the worst threat from government hacking. Once a system has been compromised, the attacker can choose its fate; he can keep the system alive and milk it for its secrets; or he can kill it—shut it down for as long as he likes. This was great for government attackers; they could exploit their adversary's systems for intelligence purposes for years, and then, in a crisis, they could shut the systems down.

The tools to infiltrate information systems grow more sophisticated every year. The United States is the most at risk. It is probably among the top five intelligence targets of every government on earth. Why? Because our unique global military reach means that no government on earth can safely ignore the likely U.S. reaction to its actions. Put another way, every tin-pot president-for-life who wants to attack a neighbor has to worry first about whether he can beat his neighbor and second about whether the United States will choose to stop him. So every government wants to know how we will react to what it does, and ideally it wants a weapon that can persuade us not to get in its way.

For many governments, hacking U.S. information systems serves both purposes. Hostile nations can gather intelligence about our view of them while they plan attacks on a neighbor. And once the attack is launched, if the United States interferes, the code that was used

to spy on us can be deployed to shut our systems down. Electricity, aviation, communications, and banking can be disrupted, perhaps even sabotaged irreversibly. Without a shot being fired, without even a clear sense of who the attacker is, much of the United States could find itself living in post-Katrina New Orleans, but without hope of a rescue anytime soon.

How effectively this weapon could be deployed today is in dispute. But there is little dispute that the attackers have been gaining on the defenders by leaps and bounds. Two nations, Estonia and Georgia, have already suffered serious, coordinated cyberattacks originating in Russia during disputes with that country. The attacks were effective, but not crippling. So perhaps foreign nations cannot use information technology to kill or harm Americans on a large scale today. But it seems likely that they will have that capability soon. Just as it took decades for terrorists to figure out how to cause catastrophic failures in the air transport system, so it may take decades for attackers to find and exploit the most damaging holes in our information networks. So far, there is no sign that the spies and the crooks who are trying to do that are running out of ideas or money.

And what are we doing as this threat gathers?

More or less what border officials were doing in the 1980s. We are embracing information networks with the same enthusiasm we have displayed since the 1970s, and doing very little to close the security holes this technology opens.

We are up on the bike and flying downhill. Only now, as the scenery begins to blur, are we starting to understand that maybe this technology, too, will find a way to kill us.

If jet travel and computers were the ghosts of technologies past and present, biotechnology is a specter that haunts the future. It became my personal nightmare while working for the Robb-Silberman Commission. The United States agreed to give up biological weapons in the 1970s, and stopped all work on them at that time. The Russians signed the same treaty but, if anything, they expanded their biological

weapons programs, continuing to make ever more loathsome and unstoppable diseases. Little wonder then that their client states and allies, like Iraq, also had biological programs.

Most troubling from an intelligence point of view, our spies had little or no insight into these programs in Russia or in Iraq, at least not until defectors revealed them. It was just too easy to hide them, in medical or insecticide factories, say, or in anonymous laboratories on the outskirts of obscure cities.

The death and demoralization that biological weapons cause can be equivalent to a nuclear detonation. That makes it crucial that we do a better job of tracking foreign governments' illicit biological programs, as the Robb-Silberman Commission recommended.

But that wasn't the scariest part of what I learned while serving the commission. What scared me most was how rapidly the ability to make biological weapons is being democratized. Biotechnology is growing as fast as jet travel and computers. The cost and difficulty of biological engineering is being reduced at an exponential rate.

This means that scientists' ability to build dangerous organisms is also increasing exponentially. In 2005, that progress allowed scientists to rebuild the deadly 1918 flu virus from scratch. Worse diseases can be revived in the same way. Although smallpox has been eradicated in the wild, it has become more dangerous to humankind than ever now that vaccinations have stopped. It has not been synthesized, at least not that we know of. But the failure to recreate smallpox is now a matter of choice, not capability. Larger and more complex organisms than smallpox have already been created, and the cost and difficulty of assembling such DNA sequences keeps dropping.

In fact, the current state of the art has moved from viruses to bacteria. In 2008, scientists assembled the entire DNA sequence for a small bacterium that causes urinary tract infections. It was substantially larger than the sequence for smallpox.

Of course, you have to be really sophisticated to assemble a sequence that large. Only a handful of labs can accomplish that feat today. But Moore's law will do soon for DNA synthesis what it did

for mainframes. DNA experiments that were once the province only of big institutions with sophisticated staffs will in a few years be the playground of smart high school kids.

Indeed, that's the dream of a lot of influential and wealthy industry leaders. The people who grew rich from the information revolution would like the biotech revolution to be a straight replay—complete with DNA hackers operating out of their parents' garage, DNA synthesis IPOs, and "open source" DNA coding languages. Those who advocate a "wet" replay of the information revolution are not concerned that biotech and synthetic DNA haven't really delivered big improvements in human health yet. Massively democratizing computer power was good for all of us, they say, pointing to the results of the personal computer and the Internet. Why shouldn't the mass democratization of DNA synthesis also produce an outpouring of creativity, playfulness, and unexpected progress? Besides, they conclude, it's going to happen whether we like it or not, so we might as well get on the bandwagon.

But you don't have to be Cassandra, or Ned Ludd, to see that a world where millions of people can make smallpox from scratch might turn out to be a dangerous place.

That's not just a future that might kill you by mistake; that's a future that could kill you in a fit of adolescent pique.

As the risks of future misuse emerged, a failure of imagination started to look pretty good compared to actually, you know, *having* an imagination. At least a lack of imagination lets you sleep at night. Because the question for DHS was what were we going to do about these risks now that we saw them.

I knew one thing. We couldn't call time-out. We couldn't turn our backs on the technologies and walk away from the harm they can do.

Tokugawa-era Japan is famous for giving up firearms in the early 1600s, a hundred years after guns had been introduced by the West and widely adopted throughout Japan. For the next 250 years, it is said, Japan was ruled, and wars were fought, by the sword, even though guns were acknowledged to be more effective weapons.

But Tokugawa Japan is famous because its story is so uncommon (indeed, some say it isn't true). Certainly no other nation is known to have denied itself an important technology for so long and survived. That's especially true for technologies like synthetic DNA. Manmade diseases wouldn't stop at our borders just because we decided to discourage biotechnology. We could let other countries take the handlebars, of course, but we'd all take the same fall in the end.

If we couldn't give up the latest technologies, we knew, we would have to find ways to manage their risks. We'd have to begin now to think about how to guide the rising curve of exponential change, how to steer it away from the most deadly consequences. Could we do that? We weren't sure. But we started with travel—the technology whose exponential adoption had already caused so much death on September 11, 2001.

The problem of jet travel, at its heart, is that everything happens so fast—life-and-death decisions are a matter of seconds.

And not just while the plane is in the air. When international flights arrive at our airports, DHS can spend no more than thirty seconds with each traveler. In those thirty seconds, we have to decide who should be waved through and who should get more detailed attention. Indeed, thirty seconds is probably longer than we can afford to spend; anyone who has experienced the lines at JFK or Dulles when many international flights arrive at the same time knows that they are dehumanizing and exhausting—not exactly a welcoming ceremony.

Our solution was to use information about the traveler more effectively. First, we had to find out, in advance, who was coming here. We sought information from the airlines about the passengers they were carrying; and in the end we asked all international travelers, even those for whom visas weren't required, to provide information about themselves before they traveled.

We also needed more information about risky travelers if the system was going to work. We had to knock heads in the bureaucracy

to ensure that each agency was contributing to a single list of known or suspected terrorists. More importantly, we needed better data to help decide who was risky. And not just from other U.S. government agencies. We needed information from other countries; if you want to know who the terrorism suspects are in Hungary, chances are that the Hungarian authorities have better sources than the Federal Bureau of Investigation or the Central Intelligence Agency.

We also needed information that would help us spot new recruits who hadn't yet come to the attention of the authorities. Aussie ranchers call their unbranded calves "clean skins." Their intelligence agencies have borrowed the term to describe terrorists who don't yet have a record. They are every terrorist group's dream and every government's nightmare. But no terror recruit is perfectly clean—with the right information, subtle clues often reveal connections that identify risky travelers, even if we've never seen them before.

That was the heart of the solution. If we got data in advance, we could identify the tiny fraction of suspicious travelers who should be pulled aside for additional screening. The thirty-second interview in the booth was no longer our only chance to find bad guys. Instead, it would become a backstop—a chance to double-check work that had been done in advance.

In theory, that should have been enough. If you know whom you're worried about and who's coming, you can do the sorting on that basis. But terrorists aren't always so obliging, or so stupid. If the government screens travelers based on who they are, then the terrorists will try to defeat the system by changing identities.

So we had to lock travelers to a single identity, and we did, raising security standards for passports around the world and recording travelers' fingerprints so that terrorists couldn't use different passports to enter the United States. Even if they managed to fool another country into issuing a passport in a false name, they wouldn't be able to fool us.

At this point, some readers must be wondering what the fuss is about. Surely this approach to border security is obvious. There's nothing

especially groundbreaking or high-tech about a passenger-screening program that uses data to improve decision making.

Well, yes and no.

Yes, it's easy to *imagine* such a border control system. It was easy to imagine such a system in the 1980s, too. But governments didn't implement it. They did the opposite. They surrendered to the tide of travelers.

Why, we wondered, did they make a choice that seems so foolish now? We soon found out that we would have to fight for our new border strategy. And it wasn't at all clear that we would win—even though the new approach moved most travelers as fast as before, and even though the old approach had produced a disastrous failure and left three thousand dead.

It didn't matter. We were in for a bruising political and diplomatic battle with powerful groups that weren't used to losing. To them, our new approach was a threat greater than terrorism. They had defended the border status quo against past efforts to improve security, and they didn't think the unfortunate events of 9/11 were a reason to change course.

The first and most obvious opponents of change were the businesses whose profits depended on the status quo. Our new strategy was going to shake things up. For example, in the old days, to encourage travel, the United States had told a number of countries in the Western Hemisphere that they could come to the United States without a passport. That put a big hole in our security strategy, but when we filled it by requiring that all international air travelers have passports, industry howled.

Tourism, travel, and airline executives wanted to keep riding the exponential growth in jet travel. They didn't want innovations in government security on the border. The industry couldn't be sure that the measure would improve security, but if the measure made travel less attractive, they knew they'd be hurt. So the safe course for industry was to always advocate less control, not more. And that's what they did. We had to jam the requirement through over their resistance.

The second opponent of change was the privacy lobby. In the United States, left-leaning groups like the American Civil Liberties Union (ACLU), the Electronic Frontier Foundation, and the Electronic Privacy Information Center (EPIC), joined with right-leaning libertarian groups like the Eagle Forum and Americans for Tax Reform. In Europe, the privacy advocates were government agencies—privacy bureaucracies. They could usually count on support from journalists who shared their views. Throughout our tenure at DHS we faced claims from all of these groups that using data to screen travelers was somehow an abuse of personal information. Privacy watchdogs in the United States and Europe didn't like it when government got access to any information for any purpose. If the data was collected at all, they agreed, its use must be restrained in the most stringent manner. They wanted suffocating controls on what we gathered and how we used it.

I started to believe that some of the privacy groups just objected in principle to any use of technology that might help catch criminals or terrorists. The example I remember best was when the police at Logan Airport got handheld computers. The computers were connected to public databases so they could check addresses and other information when they stopped someone. It was pretty much what any businessman could do already with a Blackberry or iPhone.

The American Civil Liberties Union went nuts. The executive director of the Massachusetts chapter called the handhelds "mass scrutiny of the lives and activities of innocent people," and "a violation of the core democratic principle that the government should not be permitted to violate a person's privacy, unless it has a reason to believe that he or she is involved in wrongdoing."[4] Another ACLU spokesman piled on. "If the police went around keeping files on who you lived with and who your roommates were, I think people would be outraged," he told *USA Today*. "And yet in this case, they're not doing it, but they're plugging into a company that is able to do it easily."[5]

Remember, the handheld computers only tied to public databases that any citizen could search. "It's nothing we don't have access to already," Lieutenant Thomas Coffey told the *Boston Globe*. "Instead of

me having to go down to the registry of deeds in a particular county, I can now access this information via a BlackBerry," he added.[6]

If the ACLU considered that a civil liberties disaster, I remarked, we'd better not tell them that we also have access to the White Pages.

Still, "no" was the privacy community's default answer to any improvement in law enforcement technology. The rest of us can use Blackberries, Google, and Facebook all we want to gather information about our friends, our business associates, and even our blind dates. But the ACLU seemed to think that law enforcement should live in 1950 forever.

So it's no surprise that privacy groups challenged our passenger screening time and again, in the press and on Capitol Hill. Each time, they found sympathetic ears in the establishment media. They forced us to justify our plan over and over again. Without the strong, consistent support of Secretary Michael Chertoff, a superb policy advocate in his own right, and his willingness to take on the *New York Times* and the ACLU, our strategy would have been chipped away bit by bit.

Business and privacy groups are conservative by choice in this debate. The third player—the international community—is conservative by nature. Other countries just don't like it when the United States changes policies. And our new border strategy was a change. The Canadian ambassador to the United States was vocal in questioning our plan to require passports for all travelers, questioning whether we were really ready to carry out our plan, and predicting disaster if we did. He pressed us many times to postpone the requirement, and the Canadian government would have been delighted to see it delayed forever.

It makes a kind of sense that other nations would line up against change. After all, the travel and tourism businesses are often multinationals, as are some of the privacy groups. If new U.S. border measures make Americans safer but put a burden on Lufthansa, European officials may feel it's their job to represent the interests of Lufthansa.

Sometimes it's hard to separate that motive from a less attractive one. Unfortunately, anti-Americanism is now an institutionalized part of the politics of most Western nations. Practically all developed

democracies, particularly in Europe, have a party that is anti-American and a party that is not.

There are a lot of reasons for this. They may blame us for changes in the world that aren't exactly our responsibility. (We blame Hollywood for the skewed values taught by the movies; Europeans blame us. We blame globalization for the excesses of the market; Europeans blame us.) Europeans may also have felt slighted or ignored as the United States put its post-9/11 policies together. Certainly President Bush's moral certainty after 9/11 did not wear well abroad; he was cast as a trigger-happy cowboy in a tale of American unilateralism and disregard for world opinion.

Even with a new president, and a Nobel Peace Prize-winner at that, I don't expect much change in this institutionalized anti-Americanism. Saying "no"—or "yes, but"—to the United States is the diplomatic default position of virtually every foreign ministry across the globe.

And that is indeed what the diplomats of the European Union said when DHS began to implement a data-based screening system. Borrowing arguments from both their travel industry and their privacy advocates, European officials set out to thwart DHS's new policy and to roll back the clock, to take us back as close as they could get to the old, failed status quo.

As we'll see, they very nearly won.

Even if al Qaeda disappears tomorrow, the temptation to terrorism will not go away. And tools that can give new power to terrorists are being improved every day. Terrorist attacks using these technologies are completely foreseeable.

But I also know now just how hard it is to head off foreseeable disasters. Anything government does to steer the course of an exponential technology, any suggestion that we apply the brakes or put on a helmet will face diplomatic, privacy, and business resistance.

These constituencies will fight for the status quo. It's a strange kind of status quo that they want—constant, exponential acceleration. But acceleration can feel very stable.

For a while.

I'm proud of what DHS was able to do about terrorism at the border. It was a revolution. It took years of hard fighting to put in place security solutions that worked with new technologies instead of against them. Truth be told, it took three thousand deaths, too. Without those deaths, not much would have changed at the border, even today.

I'd like to think that we can apply that lesson to other technologies. Maybe this time we can change course a few degrees before we suffer a catastrophe. I'd like to think we can build prudent, imaginative security measures into information networks and biotechnology, just as we did with our border procedures. I'd like to think that we can do that before there's been a disaster.

But, really, I'm not sure we can.

That's what the rest of this book is about.

2 Atta's Soldier

If you want to understand how difficult it can be to change security policy in the face of privacy, international, and business opposition, the best place to start is in the months before September 11, 2001.

The entire government knew an attack was coming—somewhere. And yet so entrenched were civil liberties and international interests that it took an act of individual courage to keep even one hijacker out of the United States in the months before the attack.

Worse, that kind of courage was missing when the time came to look for known terrorists within the United States.

For years pockets of the FBI had waged a stubborn insurgency against the civil liberties strictures created by the court that administered the Foreign Intelligence Surveillance Act, or FISA. Unlike most agencies, the FBI had both intelligence and criminal authorities, and its agents often shared information with each other without much regard for the court's effort to build a wall between the intelligence and law enforcement. But in August 2001, just as sharing was needed most, the FBI's resistance was finally stamped out, and the last chance to stop the attacks was lost.

It's a long flight from London to Orlando, and in August it only takes a touch of Florida's afternoon heat and humidity to leave jet-lagged passengers slumped and rumpled in the line for immigration control. But in early August 2001, there was nothing slumped about Mohamed al Kahtani. He was a small man, but he stood in the line like a soldier.

That's what he was. He had come to Florida on a martyrdom mission for al Qaeda. At that moment, Mohammed Atta was waiting upstairs, on the other side of border control, talking to al Qaeda's man in Dubai on a pay phone, demanding to know where the new arrival was.

But Atta's soldier had a problem. When he strode to the immigration booth for what should have been a thirty-second interview, Kahtani told the officer he spoke no English. He left his customs and arrival form blank. Little things, but they made the officer suspicious. In four years at Orlando airport, this was the first Saudi she'd encountered who did not speak at least a bit of English.

She sent him to secondary inspection, where an experienced border official would be able to ask a few more questions.

That's when Kahtani met Jose Melendez-Perez.

Melendez-Perez is a quiet man with glasses and a mustache. He'd been in the military himself—twenty-six years as an enlisted man in the Army before starting a second career as a border inspector.

Melendez-Perez called Kahtani into the interview room. The man was "well groomed with short hair, thin mustache, black long-sleeved shirt, black trousers and black shoes," Melendez-Perez remembers.[1] Kahtani stood about five-feet-six and was in "impeccable shape . . . He had a military appearance," Melendez-Perez told the 9/11 Commission.[2] As soon as they made eye contact, though, Kahtani began behaving oddly. He gave the inspector a long stare with more than a hint of arrogance in it. Kahtani wasn't happy. He'd been cooling his heels in secondary inspection, and he was already impatient. As he sat down for the interview in a windowless room, the temperature in the room seemed to drop. Kahtani was giving off an air of menace.

Melendez-Perez launched into the interrogation, waiting for the translator on the speaker-phone to repeat the questions in Arabic. (In this book, conversations that are paraphrased or reconstructed from paraphrases are marked with dashes rather than quotation marks.)[3]

—Why don't you have a return ticket? Melendez-Perez asked.

Kahtani showed anger. He resented the question. And the finger he waved in Melendez-Perez's face didn't require translation.

—Where are you going when you leave the United States? Melendez-Perez asked, unfazed.

—I don't know; a friend is coming to the U.S. to travel with me. He is making the travel arrangements.

—And when will the friend arrive? Melendez-Perez asked.

—In three or four days, said the Saudi.

—And what is the purpose and length of your visit?

—I'll be here for six days. I'll travel around the United States with my friend, said Kahtani.

Melendez-Perez thought the whole thing was fishy. Why wait around for his friend for three or four days if the whole stay is just six days?

"It was clear that he was upset," Melendez-Perez recalled to me later. "He didn't have answers to my questions, so he started to get aggressive."[4]

The Saudi's anger and sense of entitlement were unusual.

"This was the first time anyone had done that in a secondary interview," Melendez-Perez told me. "Usually, you know, people try to stay calm and persuade you they're good people who should be admitted."[5]

Melendez-Perez kept pressing.

—And where will you stay?

—At a hotel.

—Won't it be hard to stay at a hotel if you don't have a reservation and don't speak the language? Melendez-Perez asked.

—I've got a friend upstairs waiting for me, Kahtani told him.

—And what is your friend's name? Melendez-Perez asked.

—Actually, I'm going to call my friend once I've found a place to stay.

Kahtani's story was changing.

—So, what's your friend's phone number, then? Melendez-Perez pressed.

—That's none of your business, said Kahtani. It's personal; there's no reason for you to contact him.

—How are you going to pay for your hotel and your travel and your flight home? Melendez-Perez asked him.

Kahtani had $2,800 in cash and no credit cards. A return ticket would use up most of that.

—My friend is going to bring me some money, Kahtani said.

—Why would he bring you money?

—Because he is a friend, said Kahtani.

—How long have you known this person?

—Not too long, said Kahtani.

By now, Melendez-Perez had spent more than an hour with Kahtani, growing less and less comfortable with the hostile and evasive Saudi. It felt to Melendez-Perez almost as though Kahtani had received counterinterrogation training.

Kahtani must have known that his answers weren't satisfactory, but he didn't seem to care. In the end, he expected to be admitted no matter what he said. After all, his papers were in order. A search of his luggage had turned up empty. Melendez-Perez had nothing concrete, just a bunch of answers that he didn't like.

That would have been enough to turn most travelers away. But Kahtani was a Saudi. And as far as Melendez-Perez knew, no Saudi had ever been turned away by a border inspector.

The Saudis who came to the United States "knew they were going to get taken care of," Melendez-Perez told me.[6]

"When I started work in Miami, I got instructions about arriving flights with Saudi passengers. We were told 'Don't do anything to offend Saudi passengers.' When a flight with a lot of Saudis would arrive in Miami, the line supervisors would get nervous. They would tell the officers, 'Make sure you treat these people well and follow protocols for them.'"[7]

In Orlando it was the same.

"Even the supervisors were nervous about how Saudi passengers are greeted," Melendez-Perez said.[8] The special treatment could be seen as simple cultural sensitivity. For example, if a female passenger accompanies a male, and the man doesn't want her to show her face to

the male officer, the female would be sent to secondary to be seen by a female officer.

But the supervisor's nervousness sent an informal message, too: "No one was into refusing Saudis," says Melendez-Perez.[9]

If he had any doubt about that, it didn't last long. Melendez-Perez stepped out of the interview room to check Kahtani's computer records. And to warm up. Just being in the room with the Saudi was chilling his blood. He'd been in there a while. The whole office must have realized what was happening.

As he stood by the computer, one of his coworkers walked by, a stack of immigration forms in hand.

"Hey, you're trying to refuse a Saudi? Are you crazy? You'll get in trouble for that," his colleague said without breaking stride.[10]

"He gave me the wrong answers. I can refuse anyone for that," Melendez-Perez retorted.[11]

But he knew that wasn't true.

"I didn't really have the authority to refuse Kahtani. But I could recommend refusal. The question was, 'Would that fly?'"[12]

The problem wasn't the inspector's instincts. "I had a good record. Sometimes officers recommended refusal and it didn't stand up, but I had built up credibility."[13]

The problem was the nationality of the man he was trying to send home. The United States wanted Saudis to feel welcome when they came to the country. They were good for business; and anything that made them uncomfortable would provoke criticism from the tourism industry. And they had clout. Saudi Arabia had paid much of the cost of the first Gulf War. Its diplomats were wired in Washington, and unhappy Saudi tourists were quick to call the embassy. In fact, Washington had already made the front-line border supervisors nervous about anything that hinted at cultural insensitivity or discrimination.

Melendez-Perez was determined, though. This guy was bad. He took the problem to his supervisor, who had the authority to approve his recommendation. Listening to Melendez-Perez, the supervisor

must have wondered how he'd justify the refusal if the Saudis—or the U.S. ambassador to Saudi Arabia—decided to complain.

He'd say, "Well sir, my inspector's intuition told him the guy was up to no good. He didn't like the way Mr. Kahtani stared at him and Kahtani's answers to his questions seemed arrogant and strange." Could the diplomats make that sound like ethnic prejudice, or cultural insensitivity, or just an arbitrary bureaucratic power trip? Sure they could. He had no grounds for excluding Kahtani that would stand up to second-guessing.

The supervisor was willing to back his inspector, but only if he could find someone to back *him*.

—Let's take this higher, the supervisor said.

He put in a call to the assistant director of the port. Melendez-Perez listened nervously as his supervisor laid out the case to the assistant director. Then the supervisor fell silent. He handed the phone to Melendez-Perez.

The assistant director wanted to talk to Melendez-Perez directly. He had a lot of questions. He wanted to know why Melendez-Perez was pushing the issue so hard.

—When he looks at me, said Melendez-Perez, I feel a bone-chilling cold. The bottom line is, he gives me the creeps.

Now it was the assistant director's turn to squirm. The call was his. And so was the blame if the decision blew up into a diplomatic mess. He needed something more, a clear bureaucratic line of defense, not all this talk about Kahtani's "chilling" demeanor and unconvincing answers.

But the assistant port director had an idea. He quoted the Immigration and Nationality Act: "An applicant for admission may be required to state under oath any information sought by an immigration officer regarding the purposes and intentions of the applicant in seeking admission to the United States."[14]

"Put him under oath and ask the questions again," the assistant director ordered. "If he won't answer, he's in violation of the law. Then you can refuse him."[15]

The stakes were high as Melendez-Perez walked back to the windowless room where Kahtani was waiting. If Kahtani refused to answer, he would be on the next plane home. But if he just repeated what he'd said before, Melendez-Perez's boss—and his boss's boss—would be in a tough spot.

Melendez-Perez administered the oath. And he began asking the same questions Kahtani had already answered. Kahtani could see what was happening. They were covering the same ground all over again. The officer wasn't even trying to disguise the repetition. Kahtani had had enough. He balked. He was sick of the whole thing.

Melendez-Perez breathed a sigh of relief. That was it. They wouldn't have to rely on his intuition if they were called on the carpet. Kahtani had blundered into a flat violation of the law. Now he could be sent home.

Ninety minutes later Melendez-Perez and another inspector were on the jetway of a Virgin Atlantic flight to Heathrow with Kahtani between them. The plane was empty. Kahtani would be boarding before anyone else.

Before boarding, though, Kahtani had one more thing to say. He was standing erect, almost cocky, in the door when he turned to the inspectors.

"I'll be back," he said.[16]

For the first time all day, he spoke in English.

He was right. He would be back. But not in time to meet Mohammed Atta, who left the airport that day without his soldier.

And not in time to meet the other hijackers, either. Five weeks after Kahtani was sent home, Flight 93 took off with four hijackers on board. Every other hijacked flight that day had a team of five. As it turned out, the missing man made all the difference. Organizing quickly, the passengers attacked the shorthanded crew of hijackers. Unable to keep the passengers out of the cockpit, the hijackers were forced to crash the plane in an empty field near Shanksville, Pennsylvania. It never got near its likely target, the Capitol in Washington, D.C.

When Kahtani did return, it would be in shackles. He was captured in Afghanistan as an enemy combatant in 2002.

There's a good chance that the Capitol was spared thanks in part to the determination and imagination that Jose Melendez-Perez and his superiors showed. Melendez-Perez turns aside praise for what he did.

"That's why I was getting paid," he says.[17] But, in fact, he managed to do his job in part because he and his bosses found a way to protect themselves from bureaucratic second-guessing.

A few months earlier, though, in New York and Washington, it was second-guessing that triumphed. As a result we lost our best chance to save the World Trade Center and the Pentagon.

3 To the Wall

March 9, 2001, was cold and gusty in Washington. No one without a clearance even knew that Royce Lamberth, the chief judge of the Foreign Intelligence Surveillance Court, had sent a letter that day to John Ashcroft, the recently confirmed Attorney General of the United States.[1]

But almost immediately, the letter set off the worst turmoil ever experienced in the clubby world of foreign intelligence wiretaps. For the first and only time in its history, the FISA court was disciplining an FBI agent, singling him out by name and barring him from any appearance before the court. Even papers that he signed would be rejected. Why? Because the court no longer trusted his assurances that the FBI was observing the elaborate set of rules that the court had erected to protect the civil liberties of terrorist suspects.

This could not be tolerated. The court was determined to bring the FBI to heel; this ruling would show just how seriously the court took its civil liberties procedures.

Widely described inside the FBI as a contempt order, the ruling looked like a career killer. Indeed, the court's letter seemed to accuse the agent of making false statements to the court, a felony under federal law. That's how the attorney general saw it. The Justice Department's Office of Professional Responsibility was called in to consider what other sanctions might be proper.

This was the beginning of a years-long nightmare for the agent. But in the secret cloisters of intelligence law, it would not be his nightmare alone; it would spread and spread, like ripples on a still lake.

It sent a chill of fear first through the FBI counterterrorism machinery in Washington, then deep into the warrens of the National Security Agency at Fort Meade.

In August, though, the chill had not yet engulfed the FBI counterterrorism squad in New York. They were champing at the bit, having just learned that an al Qaeda terrorist had recently entered the United States. They didn't know for sure that he was planning an attack, but they'd been hearing all summer that a big one was coming. If a major-league terrorist was in the United States it might be real trouble. They geared up to go looking for him.

That's when the nightmare reached them, too. They shouldn't have the information, they were told, and were forbidden to act on it. They could end up like the other agent, censured for breaching the civil liberties protections erected by the court. They were stopped in their tracks.

A few days later the nightmare became America's.

Spies and Cops

The letter Judge Lamberth sent John Ashcroft on March 9 was a long time in the making. In fact, it marked the climax of a decade-long undercover battle over civil liberties and intelligence wiretaps. The basic story can be teased out of official documents, particularly a staff report of the 9/11 Commission that was not declassified until 2009 and a Justice Department Inspector General report from 2004, and many of the participants are now willing to talk about those events.

The March 9 letter had its roots in the difference between law enforcement and intelligence wiretaps. Law enforcement wiretaps are heavily regulated. They can only be initiated if other investigative techniques have failed; they can only be carried out for a limited time. They require constant supervision and review. They are approved only for specific kinds of crime. Wiretaps that don't keep producing new criminal evidence must be halted. And once a criminal case begins, the defendant can see transcripts of the wiretaps and challenge their

legality. If the law enforcement agencies have gone beyond the law, the courts will exclude the evidence, and the defendant will likely escape justice. Everyone in criminal justice understands that and conducts himself accordingly.

Intelligence wiretaps are different. They don't have to pay off right away, and they can be renewed repeatedly. Sometimes they're left in place for years before they reveal something useful. And they aren't triggered by suspected criminal activity. Any representative of a foreign government is fair game for an intelligence tap. The rules that apply to law enforcement taps just aren't appropriate for intelligence wiretaps. So, in 1978, when the United States embarked on the experiment of putting intelligence wiretaps under judicial oversight, it wrote a special statute for them. FISA sets much more flexible rules for wiretaps aimed at agents of a foreign power than the law sets for law enforcement wiretaps.

Once Congress had created two parallel wiretap statutes, civil liberties conflicts were nearly inevitable. Usually, there wasn't much overlap between the two. Law enforcement wiretaps were for organized crime and politicians. Intelligence wiretaps were for foreign spies and the like.

But espionage is both a crime and an intelligence matter. We usually expelled foreign government spies without prosecution, but we could prosecute Americans when we caught them spying. Which raised the question whether the suspected spy should be wiretapped using FISA or the law enforcement wiretap law.

Civil libertarians and judges had nightmares about such cases. They feared that law enforcement agencies would game the system, picking and choosing the wiretap law that gave them the most latitude. If they couldn't persuade a court to grant a law enforcement wiretap, they'd just use a FISA wiretap instead.

The intelligence agencies had a similar nightmare. What if they found an American spy while conducting an intelligence wiretap and Justice decided to prosecute? As soon as the accused spy got in front of a judge, he would claim that his privacy rights had been violated.

He'd claim that the government had played a shell game, using a FISA tap to catch him when it should have used a law enforcement tap.

If the court agreed, the wiretap could be declared illegal. The spy could go free—but first, he'd likely get a chance to read transcripts of all the government's wiretaps and to figure out how they were done. Years of intelligence gathering could be put at risk.

Even worse, there was no way of knowing when the line had been crossed. It might take years before an intelligence wiretap was put at issue in a criminal trial. By the time a judge told them the intelligence agencies were out of bounds, it would be way too late to fix the problem.

They had to know where the line was. But the law was sparse. The courts had given a few hints. They seemed to say that a proper intelligence wiretap would morph into an improper law enforcement wiretap when the primary purpose of the tap shifted from intelligence gathering to building a criminal case. If the main reason for the tap was gathering evidence, the prosecutors would have to get their own wiretap and live by the rules that the law set for those intercepts.

So if the intelligence agencies wanted to stay out of court and out of legal trouble, all they had was a rule of thumb: The less contact the better between the agencies running the intelligence taps and the prosecutors and investigators handling the criminal case. That reduced the chances that the courts would think that there'd been a shell game in progress. Or, to put it in terms the *New York Times* might have used, the less contact there was between prosecutors and intelligence wiretaps, the less likely it was that American liberties would be eroded by the misuse of FISA for criminal justice purposes.

For a while, the concern was mostly theoretical. When FISA was adopted in 1978, no Americans had been prosecuted for espionage since Julius and Ethel Rosenberg more than a quarter-century earlier. But 1985 turned out to be the Year of the Spy. A dozen Americans were caught spying for foreign governments. They were legitimate FISA counterintelligence targets. They could also be arrested and prosecuted.

But if the authorities were getting ready to prosecute someone, shouldn't they use ordinary wiretaps with all their built-in privacy and civil liberties protections? Suddenly the intelligence agencies' nightmares seemed to be coming true. A solution had to be found. And it was. The two investigations would be kept separate. FISA taps could be used to keep track of likely spies for years, waiting for their tradecraft to slip. When it did, if criminal prosecution looked like an option, the case could be handed off to the prosecutors, who would have to meet all the usual criminal standards if they wanted to carry out wiretaps or other searches. The two things would be independent of each other. The prosecutors didn't need the details of the intelligence. All they needed was a tip that they should begin a separate criminal investigation.

The first course of the wall had been laid, but it seemed to work. The Department of Justice successfully prosecuted several of the spies caught in 1985. America's spies and cops had found a way to live together.

Until the wheels nearly came off.

It was 1993. Janet Reno had taken the helm at Justice as attorney general. She had not brought a contingent of loyalists with her to the department. But she did bring Richard Scruggs, once her boss in Miami, who had come north to handle national security matters for her. Reno was comfortable relying on the career professionals. At first. But within months of arriving, she'd relied on them in approving a raid on the Branch Davidian compound at Waco, Texas, that had gone badly wrong. Dozens of cult members died in a fire, and later investigation cast doubt on much of the advice she'd been given before the raid.

Now it looked as though the career professionals had let her down again. Scruggs could barely contain his disbelief. Shortly after the Waco disaster, he and the attorney general had been briefed on the worst espionage case the United States had seen in a generation. Aldrich Ames, a CIA operative with intimate knowledge of the agency's Soviet sources had sold them all to the Soviets for several million dollars.

To move its investigation forward, the FBI asked the attorney general to personally approve a physical search of Ames's home. Because the search was done for foreign intelligence purposes, the FBI told her, no court-ordered warrant was required. It felt odd to tell the police they could break in to an American's home without going to court for a warrant, but she had relied on the professionals. This wasn't a criminal matter.

Or was it? Scruggs had heard a rumor, and he wanted the truth. He called the two top criminal division prosecutors in national security cases to his office.

—Has the FBI been briefing you about the fruits of their foreign intelligence search of Ames's home? Scruggs demanded to know.

They had.

Scruggs exploded.

—And how are we going to explain that at trial? he asked. How can we tell the court that the attorney general personally authorized the FBI to break in to an American's home without a court order and that the evidence was then turned over to the prosecutors?

It was a debacle, and a civil liberties windfall for Ames. Almost as soon as he was arrested, in early 1994, his lawyers began making precisely the argument that the intelligence agencies and Scruggs had feared. Ames had betrayed the identities of nearly a dozen men. They had almost certainly paid for his treason with their lives, and he could have faced the death penalty if his case had gone to trial. Instead, he was able to negotiate a quick plea for himself and his wife that kept him alive and allowed her to leave prison in 1998.

The Ames case opened a chasm in the little community that understood intelligence wiretaps. For the intelligence agencies, the case was a bullet dodged. The plea deal had kept the courts from deciding whether intelligence techniques violated civil liberties when they were used to help prosecutors. But the intelligence agencies didn't think they could dodge many more bullets like that one. The rules of the road had to be clarified so they could steer clear of retroactive second-guessing by the courts.

As NSA's top lawyer, I was part of the intelligence community at the time, and I shared its concern about privacy claims. In 1994, after I left NSA, I argued in a *Foreign Policy* article[2] that intelligence and law enforcement should be strictly separated. The privacy risks that came from blurring the lines between intelligence and law enforcement might be more abstract than real, I thought, but they had to be taken into account: "However theoretical the risks to civil liberties may be, they cannot be ignored."[3] Foreign intelligence gathering is intrusive, harsh, and deceitful—and should be. I didn't think the courts would or should tolerate the application of these qualities to ordinary criminal defendants. And so I argued for an approach that "preserves, perhaps even raises, the wall between the two communities."[4]

I had plenty of allies in that little world. The FISA court had its own reasons for wanting strong civil liberties protections. Since its creation, it had been incessantly attacked by civil liberties groups as being too secretive and too friendly to the government. It was called a rubber stamp court because it almost never turned down a wiretap application.

The slurs hurt. "I have struggled with the perception for years that we did whatever the government wanted and were rubber stamps," said Judge Royce Lamberth, who became chief judge of the FISA court in 1995. "That was not and is not true."[5]

But making that case was an uphill fight. The court's proceedings were so highly classified that the judge could do little to rebut the charge. Perhaps he felt he had a little more to prove than most. A Republican appointee and a former prosecutor, Lamberth was a colorful, aggressive judge. When not on the bench he sometimes attended sober Washington events in a cowboy hat. A tribute to his Texas roots, he says. Truth in advertising, say some of the lawyers who've appeared before him.

Whatever the truth, Judge Lamberth didn't want anyone to mistake his court's commitment to civil liberties. That was Job One. "We worked to protect civil liberties while protecting the country itself. The judges asked themselves: Are we going to lose our liberties if we

approve this kind of surveillance?" Lamberth told one reporter. "We knew that the country has not always done things right."[6] But those days were over; the FISA court was on the job.

In its mission to head off civil liberties objections, the FISA court had an ally—an obscure but powerful Justice Department office. The Office of Intelligence Policy and Review (OIPR) was the liaison between the court and the executive branch. No paper was filed and no word was spoken in the FISA court without the approval of the intelligence review office. As the guardian of intelligence wiretaps, OIPR wanted to make sure there were no civil liberties abuses on its watch.

When I was at NSA, I had worked with Justice's intelligence review office. It was a small office, and for a generation it had been run by a legend. The counsel for intelligence policy was Mary Lawton, a tiny, tough-talking, hard-smoking spinster with a fine legal mind. She had taken over soon after the intelligence scandals of the 1970s. She believed strongly in the intelligence mission, and especially in her boys at the FBI. She usually found a way to justify the wiretaps and other operations they wanted to carry out.

But she had sharp elbows and a keen sense for the politics of survival. No one talked to her court but her. She was almost as effective at keeping others from talking to the attorney general about classified matters. In government, there's almost nothing that can't be accomplished if you're the only person in the room with the decision-maker, and Lawton knew that.

She also knew how to deal out punishment for bureaucratic offenses. From time to time, someone would cross a line with Lawton. FBI agents would complain to the director about a ruling. Or I'd raise doubts about her refusal to make a particular argument to the FISA court.

The punishment was always the same. She'd stop taking our calls. We'd be referred to her deputy, Alan Kornblum. Bald, bullet-headed and energetic, Kornblum meted out the punishment. He would demand endless rewrites of the same documents. They were never good enough. He wouldn't send the applications to the court without changes. And the changes weren't good enough either. Finally, desperate at the prospect that we'd miss the deadline and have to drop an

important wiretap, I'd call Mary and surrender. Then she'd help us get our paperwork filed in time. Lesson learned. It was a small world, but she ruled it absolutely.

Then, in 1993, Lawton died suddenly. Shaken by the near miss in the Ames case, Attorney General Reno asked Richard Scruggs to take over. Scruggs decided immediately that the tension between law enforcement and intelligence could not be allowed to fester any longer.

He wanted tough new civil liberties guidelines, including a "Chinese wall" between criminal prosecutors and investigators on the one hand and intelligence operations on the other. There would be no more casual mixing of investigations like the Ames case. Instead, the informal understanding would become formal. If the intelligence agencies found a spy, they could use FISA to watch him for as long as they liked, identifying his contacts and drawing a bead on what he had compromised. But they'd have to do all that without any help from the prosecutors.

At some point, the intelligence community would see no value in continuing to watch him, or the case would begin to look like something that could lead to an arrest. Then they could tell the law enforcement agents what they knew. The prosecutors could seek a law enforcement tap and use it to gather the evidence they'd use to prosecute. The earlier work by the intelligence agencies would stay out of the case; no one could say the prosecutors had misused a FISA tap they barely knew about.

Scruggs's relationship with the attorney general was strong. She was determined to avoid another civil liberties debacle of the sort that only a plea bargain had avoided in the Ames case. And he had the solution—a wall in time between intelligence gathering and criminal investigation. It seemed to the lawyers of the intelligence review office, and of the intelligence community, that we had found a safe place to stand, protecting both civil liberties and intelligence sources.

But no sooner had we taken a stand than the ground began to slip from under our feet, like sand in a withdrawing tide.

We had reckoned without the determination of al Qaeda—and the machismo of America's prosecutors.

Prosecutors and Terrorists

While the lawyers argued nice points of civil liberties doctrine in Washington, Islamic extremists had begun to target New York City. We had granted an immigrant visa to a vicious Islamist ideologue. Omar Abdel-Rahman, also known as the blind sheikh, was allowed to stay as a "religious worker" spreading his faith. And spread it he did, preaching death to Americans with enthusiasm and to great effect.

Shortly after his arrival, his allies and acolytes had killed the radical Jewish activist, Meir Kahane. The case was handled by FBI agents and prosecutors based in Manhattan. These offices saw themselves as a criminal justice elite, the center of criminal justice excellence in the country. The U.S. attorney for the Southern District of New York only occasionally accepted guidance—and certainly never direction—from Washington, where the office was known as the "Sovereign District" of New York. The FBI office in Manhattan had a similar esprit. In Washington, agents made coffee; in New York, they made cases. Big ones.

But they had booted the Kahane case, wrapping it up quickly in a trial that portrayed the shooter as a lone nut. In fact, he was part of the blind sheikh's Islamist circle, and the blind sheikh was planning on much more than a one-off murder.

Indeed, his acolytes were just getting started. Soon, they would set off a huge car bomb in the World Trade Center, hoping to bring the whole complex down. While the elite of federal law enforcement was struggling with that case, the blind sheik's allies planned an even more ambitious attack. Their scheme was eerily similar to the assault on Mumbai that would take place in 2008. Bombings on the bridges and tunnels to Manhattan would isolate the island one evening; in the confusion, several luxury hotels would be seized by terrorists disguised as kitchen workers. Mass executions would follow.

The first plot succeeded, though the buildings did not fall. The second plot failed; it was thwarted by an informer. But the plotters' contempt for the authorities was plain. The cream of federal law

enforcement had overlooked the blind sheikh's organization the first time. Now they took the new attacks personally.

The commitment today of the Obama administration's Justice Department to prosecuting terrorists like common criminals in civilian courts can be traced back to those early years. Prosecutors were riding high. They had indicted a sitting head of state, Manuel Noriega of Panama, in 1988, and the country had invaded Panama to bring him to justice. Prosecutors are to the Justice Department what fighter pilots are to the Air Force. The most talented ones have a bit of a swagger, and there's nothing they think they can't do.

Islamic terrorists, the Southern District's prosecutors believed, had messed with the wrong people. Southern District prosecutors and investigators weren't afraid of international conspiracies. They had convicted over a dozen Mafioso in the "pizza connection" cases of the 1980s. Now, spurred by a mix of shame and outrage, they marshaled their full resources against the terror plotters.

And they delivered. By 1995, nearly fifty extremists were on trial for the Mumbai-style plot.

But this wasn't the Mafia, playing by well-understood rules. In the middle of the trial, the hunted became the hunter. The judge, prosecutors, and witnesses all received death threats. The prosecutors put criminal wiretaps in place. They came up dry. Mary Jo White, the ambitious head of the Southern District, called for FISA wiretaps to keep the coverage up.

Now the fat was in the fire. It was too late to follow the old practice of closing any intelligence taps before opening a criminal case. There were several ongoing criminal investigations into Islamist terrorism in New York. Worse, law enforcement wiretaps had already been tried and failed. It looked as though the prosecutors were doing exactly what civil libertarians and the intelligence review office has always feared—using FISA because criminal wiretaps weren't producing enough information.

Scruggs's OIPR offered a simple solution that would protect defendants' rights fully. If Mary Jo White wanted intelligence taps,

all she had to do was drop the criminal case. Either that, or she could stop asking for intelligence taps in a case that had clearly gone criminal long ago. If FISA taps were launched now, the FISA court would think that its broad authorities were being hijacked to serve the prosecutors of the Southern District. To protect against civil liberties objections, the court would reject the wiretap applications. Or, worse, it would grant them, and the whole thing would come crashing down later, when the wiretaps were reviewed by the trial court in the middle of a high-stakes terrorism prosecution.

But the fighter jocks of the Sovereign District weren't used to taking orders from a no-name intelligence aide like Scruggs, no matter how close he might be to the attorney general. The prosecutors wanted intelligence wiretaps, right now, and they wanted to know everything the taps were producing. After all, if the intelligence community couldn't go looking for a foreign conspiracy to kill American officials, what good was it?

They argued for the greatest possible sharing of intelligence and the narrowest possible view of the civil liberties problem. They wanted anything that might help them make a case.

And what about civil liberties? The prosecutors were used to the claim that they were violating defendants' civil liberties. That's what practically every criminal defendant says these days. The prosecutors could take the heat, and they expected to win in the end. The intelligence guys, they thought, were being nervous nellies. They should just grow a pair.

OIPR's effort to save FISA from civil liberties attack was suddenly at risk.

The Intelligence Review Office Takes on the Prosecutors

In the spring of 1995, Richard Scruggs went to New York to face off with Mary Jo White. Scruggs took Alan Kornblum, who remembers that White was assisted by a well-regarded junior prosecutor named

Patrick Fitzgerald. Fitzgerald would eventually become famous in his own right as the man who prosecuted both Scooter Libby, Vice President Cheney's chief of staff, and Illinois Governor Rod Blagojevich.

White rejected Scruggs's demand that she choose between FISA taps and her criminal case. Kornblum says White wanted a new kind of procedure that would keep the intelligence and criminal cases technically separate while permitting information to slip across the boundary. The intelligence review office rejected the idea but, as he remembers, Deputy Attorney General Jamie Gorelick forced the two sides to agree on something close to White's proposal: An intelligence investigation, complete with FISA wiretaps, would be opened. But to ensure that the wiretap did not become an end run on the civil liberties protections that applied to law enforcement taps, the prosecutors would have no control or direction over the intelligence investigation. Intelligence memoranda would only be given to prosecutors with the permission of the intelligence review office. A single prosecutor would have full visibility into the intelligence "take," but no say in shaping the operation.

Most fateful was the way the deal treated the FBI. The bureau's investigators were divided into criminal and intelligence teams; the criminal team would not be allowed to influence the course of the intelligence investigation.

The wall had arrived. What had been a wall in time—first do the intelligence investigation, then do the criminal investigation—was now a wall between investigators.

The deal made sense as a way to protect civil liberties. Without it, there was a risk that intelligence taps would be influenced by the evidentiary needs of the criminal investigators and prosecutors. If the government was serious about making the criminal investigators turn square corners, there had to be restrictions on how they dealt with the intelligence gatherers.

But it made no sense in terms of countering terrorism. How could two sets of federal agents hunt the same Islamic terrorists without

working together? No one was entirely happy. In OIPR's view, the wall would only protect civil liberties if it were strictly enforced. The procedures sounded good. In theory they kept intelligence intercepts separate from criminal investigations.

But the intelligence review office feared that the prosecutors might win the fight in practice. After all, a prosecutor would see everything the intelligence agencies turned up as soon as it was gathered; he could talk to the intelligence side freely, and if he were as good as Fitzgerald was rumored to be, he'd have no trouble giving the agencies hints about how to improve the criminal case. In the same vein, there were separate FBI teams for intelligence and criminal work. But they all worked for the same bureau; it would be impossible to keep them from talking to each other. The prosecutors were surely counting on exactly that.

Who had won depended on how strictly the wall was enforced. The intelligence review office soon began to fear that it would lose the enforcement battle. The deal with the Southern District only resolved matters for that office. In July of 1995, Deputy Attorney General Gorelick released department-wide guidelines for cases where intelligence and criminal investigations ran parallel. The basic rules were hard to argue with. Prosecutors could have information from the intelligence operation but no control over it. Prosecutors were expressly prohibited from exercising any direction or control over intelligence taps that intersected their criminal investigations. If the intelligence taps turned up evidence indicating the commission of "a significant federal crime" it had to be reported to the Justice Department's Criminal Division.[7] These guidelines were adopted by the attorney general in July of 1995.

But the details made the intelligence review office antsy. Its lawyers feared that the prosecutors wouldn't really respect the wall that was supposedly protecting the rights of defendants. Sure, everyone agreed that prosecutors could not control or direct intelligence taps. And the intelligence officials knew that, like every federal employee, they were obliged to report evidence of a crime to the Justice department.

But the attorney general's guidelines went well beyond reporting of crimes. They didn't just call for a report; they required a detailed description of the facts and circumstances of the crimes, and ongoing consultation. This seemed to stretch "crimes reporting" to the point of artificiality. ("Hello, Justice? CIA here. I'm calling to report a crime. You won't believe it, but al Qaeda is *still* plotting to kill Americans in gross violation of federal criminal law. Here's today's detailed evidence of exactly how they're planning to do that.")

Sure, the guidelines said that prosecutors couldn't direct or control the intelligence tap, but the temptation to cheat would be strong. The intelligence review office and the intelligence community's lawyers all feared that prosecutors would ask questions that were really hints about what the intelligence agents should do next. And that eager-to-please intelligence agencies would turn the informal guidance into their own direction. The FBI criminal investigators, many of whom were experienced lawyers in their own right, could informally lobby their intelligence colleagues to shore up the weak spots in the criminal case. Everyone would get along famously, chiseling away at the wall and the rule that criminal defendants can't be wiretapped without intense judicial supervision.

It would all be good—until the music stopped. Then some judge would put everyone under oath and pull the whole story out of them. At which point the intelligence wiretaps would be held to violate the defendants' civil liberties, with incalculable consequences.

Then the prosecutors who had boasted of their *cojones* would stand before the judge like naked men in an arctic gale.

Or, even worse, when the risk of a bad ruling became clear, the prosecutors would turn against the intelligence agencies, displaying the mix of self-righteousness and flop-sweat that replaces the prosecutors' swagger in the weeks before trial. Nothing would be more important to them than winning the case. Not classified information, not future intelligence operations. Nothing. Suddenly, to ensure victory, the prosecutors would become fierce internal advocates for whatever civil liberties rules they thought the judge was likely to want.

The only way to avoid this, the lawyers of the intelligence review office thought, was to keep the wall high from the start. That meant putting them in the middle. They had to act as chaperone and gatekeeper, overseeing the exchanges between intelligence collectors and prosecutors. Before anything could get across the wall, the intelligence office would have to approve it. The office, after all, was exquisitely responsive to the FISA court and the civil liberties risks. If it could police the wall, it would keep overeager prosecutors and over-cooperative agencies from sliding into forbidden territory.

The only problem was that the attorney general's guidelines didn't give the intelligence review office a chaperone's role. They left the wall in place as a technical matter, but they didn't give OIPR the tools to enforce it.

The attorney general had made her decision. But as far as OIPR was concerned, that was just the beginning of the fight.

Within two years, the attorney general's decision was a dead letter. Whatever the guidelines might say, the FBI was refusing to share intelligence wiretap information with criminal prosecutors without the permission of the intelligence review office.

How did that happen? Put simply, the office had outmaneuvered the prosecutors.

It had the FBI over a barrel. All of the bureau's FISA wiretaps had to go through the intelligence review office, which controlled their drafting and filing. They were always on a tight time frame. And Alan Kornblum had learned one lesson well. Delay was OIPR's trump card.

If the intelligence review office said the documents weren't ready for filing, then they wouldn't go to the court. That meant the wiretaps would lapse, or never be set up. The targets, who might be extraordinarily dangerous terrorists or spies, would escape surveillance. OIPR could punish any FBI agent who talked too much to the criminal division by threatening to wreck his investigation.

But wasn't that a violation of the guidelines? Couldn't the FBI go to the attorney general and object? Sure, if the intelligence review

office was dumb enough to say that it was punishing the bureau for too much cooperation with prosecutors. But FISA filings are immensely complicated. If the intelligence office thought an FBI unit needed disciplining, it only had to send the applications back at the last minute with a host of research to do and changes to make. The unit would have to work nights and weekends and still might lose the tap. If it complained, the intelligence review office could simply say that the office had done an unprofessional job of preparing the application. There was no recourse.

Proud as it was, the bureau had to capitulate. And it did. No one would be allowed over the wall without a chaperone.

The prosecutors soon realized what had happened. They sent complaint after complaint to the attorney general; report after report declared that the guidelines were being flouted. If the intelligence review office and the FBI wouldn't provide information more freely, the prosecutors argued, then the guidelines needed to be revised. A drumbeat began, from the Southern District to the Criminal Division. The guidelines would have to be rewritten to take the intelligence review office out of its "babysitter" role. The prosecutors had to have access to FISA information, free from OIPR's oversight.

This was serious. Prosecutors didn't usually lose battles in front of the attorney general, who was after all the nation's chief prosecutor.

In 1998, the prosecutors showed their power by cutting the intelligence review office's Kornblum down to size. He had turned down several FBI requests for applications to conduct surveillance of Wen Ho Lee, a suspected Chinese nuclear spy at Los Alamos National Laboratory. He didn't think they met the legal standard under FISA, and he knew they'd likely end up being challenged if Lee were arrested and tried. True to type, he had sent them back time and again for more work, never quite saying no. Eventually, the agents shelved the requests. Later, when the government's lethargic handling of the matter blew up into a political scandal, they managed to tag Kornblum with much of the blame.

Also in 1998, the intelligence review office got a new leader. Frances Fragos Townsend (later George W. Bush's homeland security adviser) came from the prosecutor's side of the house. She had spent time in the Criminal Division and the Southern District of New York. When she arrived, she quickly pushed the wounded Kornblum aside, taking him out of the direct line of communication to the court and bringing in a new deputy to handle FISA applications.

Now OIPR's back was to the wall. It seemed only a matter of time before the wall had been eroded as a practical matter. But once again, the wall's defenders had a hidden trump card, and it was time to play it.

As designed by Mary Lawton, the relationship between the FISA court and the intelligence review office was uniquely tight-knit. FISA judges were appointed to seven-year terms from the ranks of existing federal judges around the country. Most had no intelligence background whatsoever before being appointed. They had no familiarity with the immensely complex statute governing intelligence wiretaps. There were no reported cases to read and evaluate. Everything was classified. They were deeply dependent on the OIPR lawyers who guided them through the applications. They thought those lawyers "were top-notch, very impressive," says Judge Lamberth, remembering his first impression.[8] The intelligence review office, in turn, worked hard to earn the court's trust by not taking a traditional litigator's approach to the court.

"Historically," Fran Townsend remembers, "we had more a comfortable than an adversarial relationship with the court."[9] So it was only natural that Chief Judge Lamberth would have been fully briefed on OIPR's fear that the prosecutors would never be satisfied until they had undone the intelligence review office's strict view of what civil liberties required.

And so, as the prosecutors circled, the FISA court itself began to stir.

The FISA Court Stages a Coup

The issue came to a head in 1998. Al Qaeda's bombing of two U.S. embassies in East Africa had put the Southern District's latest criminal investigation of the group into overdrive. But it also put the wall front and center. As with other al Qaeda cases, the criminal investigation was practically inseparable from the ongoing intelligence monitoring. So what rules would govern this investigation?

The intelligence review office did not want to return to New York for another chest-bumping showdown over the wall. The prosecutors were winning. If the guidelines had to be reworked for the East Africa cases, the intelligence review office would go into battle with half the department arrayed against it.

Staring defeat in the face, the intelligence review office finally played its trump card—the FISA court. Judge Lamberth remembers Kornblum suggesting that the guidelines be turned into FISA court orders. "He felt, and we agreed, that if you have rules, you should follow them," says the judge.[10]

The idea had understandable appeal from a civil liberties viewpoint, too. Unlike the attorney general, who was, after all, a prosecutor at heart, the court would be an honest broker. It could give the rights of defendants their due weight, without a conflict of interest and without yielding to the importunings of the prosecutors. And so it was done. The FISA court simply annexed the attorney general's guidelines, making the wall a matter of court order.

It was as simple as that; a quiet coup on the top floor of the Justice Department. From now on, the court would decide what was needed to prevent misuse of FISA taps, and the rules it settled on would simply be imposed as a condition on any antiterrorism wiretaps approved by the court.

For the prosecutors it was check and mate. The FISA court had the department over a barrel. The government had to keep the wiretaps up; an attack could occur at any time, and the government could

not afford to be deaf to the planning. If the department wanted the taps, it had to accept that the FISA court was making the rules.

In theory, this court order could have been appealed. There was a pretty good reason to think that the court's action was inconsistent with the law. The Justice Department did at last appeal the wall orders in 2002, when the FISA court insisted on keeping them in place despite the investigative debacle they ultimately caused. The department won easily. The review court was scathing in its assessment of the legal basis for the FISA court's judicial coup, saying that the FISA court had "mistakenly categorized" the 1995 guidelines as statutorily required procedures "and then compelled the government to utilize a modified version of those procedures in a way that is clearly inconsistent with the statutory purpose."[11]

At the time, though, Justice didn't utter a peep. The intelligence review lawyers had no interest in overturning their own bureaucratic triumph, and they controlled all appearances before the court. But even the prosecutors must have seen that an appeal would be a nightmare for Justice. The prosecutors would have had to ask the intelligence review office to assemble the first appellate review panel in FISA history, something that would not have been done quietly. The appeal would have turned into a major civil liberties *cause célèbre*. The newspapers would have treated it as an effort by Justice to cut back on the protections for defendants created by criminal wiretap law. One can imagine the headlines turning the FISA court into an unlikely civil liberties hero: "Revolt of the Rubber Stamp Judges" might have been among the milder ones. Many in Congress as well would have seen the issue through a civil liberties lens, and hearings could have been expected, perhaps even legislation to write the wall into law. Civil liberties groups would have filed amicus briefs, as indeed they did in 2002. And, in the end, there was no certainty that the appeal would succeed, at least in the atmosphere that prevailed before 9/11.

Once the applications had been signed and the opportunity for appeal had passed, the wall was law. Neither the attorney general

nor the Sovereign District of New York could defy or modify a court order.

There was a new civil liberties sheriff in town.

For advocates of defendants' rights, the court orders were a triumph. The wall was now far beyond the reach of the prosecutors. But salvaging the wall was only half the battle. The real key was making sure that the wall was enforced. The FBI had been forced to accept the intelligence review office as the gatekeeper between its intelligence agents and the prosecutors, but how could the court be sure that the FBI itself was enforcing the wall between the intelligence and criminal teams that were both pursuing al Qaeda? The members of each team were FBI agents and analysts, after all; it only made sense for them to pool information and resources. But that process could allow criminal investigation motives to infect the intelligence wiretaps. And that would lead to disaster in a later criminal trial. It would look as though the wall had been honored mainly in the breach.

This was no idle worry. FBI agents are tough, proud, and tribal. To them, the intelligence review office was just another Justice office full of lawyers who didn't understand the street. The agents pursuing al Qaeda shared a common bond, and they needed each other's help. It was crazy, they must have thought, to deny information to each other. As long as investigative cooperation could slip cross the wall informally, from one agent to another, it would continue, no matter what the intelligence review office said. Bringing the FBI to heel would not be easy.

But now the civil libertarians had the FISA court in their corner. "If you have rules, you should follow them," Judge Lamberth believes.[12] Soon the FBI would learn just how firmly he held that view.

Several al Qaeda members had been arrested in the East Africa bombing cases, and by 2000, their trial in the Southern District of New York was drawing near. Patrick Fitzgerald was again at the center of the case.

As Fitzgerald prepared to defend the East Africa FISA intercepts against a suppression motion, he noticed something troubling. The FBI affidavits that led to the FISA orders had dutifully mirrored the FISA court's new guidelines, affirming that there had been no contact between the FBI's criminal and the intelligence teams. But Fitzgerald knew the investigators, and he knew that wasn't true. The FBI teams overlapped.

This was a big problem. There was no evidence of deliberate misrepresentation. The affidavits had described the world that the intelligence lawyers thought existed. But, stuck behind the wall, they had evidently not pressed for the actual facts. And in the end, deliberately or not, the affidavits described a world that didn't exist.

It was a nightmare not just for the intelligence office but for the prosecutors. The Sovereign District was on center stage with this latest prosecution of al Qaeda; but its case was suddenly at risk because of problems with the FISA orders. A suppression hearing loomed. The judge overseeing the criminal trial would have to be told of the mistakes. And the judge would surely ask whether the FISA court had been told of the false statements. According to Judge Lamberth, Fitzgerald eventually announced that the clock had run out; if the attorney general didn't tell the FISA court about the error by the end of the day, Fitzgerald would have to disclose it himself.[13]

In a way, it was just what the intelligence review office had always feared. A prosecutor with a case to protect was suddenly claiming that defendants' rights had been jeopardized by the FISA process and was forcing action that could disrupt the functioning of FISA.

The Wrath of the Least Dangerous Branch

Not long after, Judge Lamberth got an unexpected call.

It was Attorney General Reno.

—I'd like to come see you, she said. I need to tell you something.

—All right, Madam Attorney General, the judge replied, but I know you've got a busy schedule. Much more crowded than mine. I'd be happy to come see you.

—No, no, Reno said. My mama always told me that when you're in trouble, you're the one who goes to see the judge. And I'm in trouble. I'm going to come to you.[14]

Taking a seat in the judge's chambers a few hours later, the attorney general confessed to the errors. It was bad. As many as seventy-five orders had been affected by false affidavits.

Judge Lamberth was not a retiring sort of judge. When he thought the government was not living up to its obligations, the chief judge was relentless. In other cases, he has threatened to hold two Interior secretaries in contempt of court and accused federal officials of racism and bias. Whether he was called a straight shooter or a loose cannon, everyone who appeared before him knew that Judge Lamberth was heavy artillery—especially when he thought he'd encountered government wrongdoing.

He certainly brought out the big guns now. He demanded an investigation of the alleged failure to adhere to the wall. Justice's Office of Professional Responsibility was assigned to track down any evidence that the agents who prepared the applications had committed misconduct.

Judge Lamberth was assisted in his work by a new legal adviser. Alan Kornblum had grown tired of his isolation at the intelligence review office and had joined the FISA court as its first clerk in decades. He brought with him the old, uncompromising OIPR view that the only way to preserve FISA's value for intelligence gathering was to maintain a strict separation of criminal and intelligence functions. So, while the affidavit errors were an embarrassment for OIPR as an office, it might in fact serve the office's long-term strategic interests. This was a chance to make sure that the wall was enforced for real. At last even the FBI could be brought to heel.

The court and its new legal adviser set about constructing new enforcement mechanisms. In October, Judge Lamberth reinforced the court's oversight of who got to see FISA wiretaps. From that point on, every agent who had access to FISA-derived intelligence would have to sign a special certification, promising that none of the information

would be conveyed to criminal investigators without the FISA court's permission.

The election of 2000 eventually brought George W. Bush to power and John Ashcroft to the attorney general's suite, but this did nothing to diminish the FISA court's clout or ambition. As a senator, the new attorney general had been notably supportive of civil liberties, playing to an antigovernment, libertarian strain of Republicanism that had grown strong in opposition to the Clinton administration's centrist support for more law enforcement authority. Attorney General Ashcroft had no interest in picking a civil-liberties fight at the start of his term. Quite the reverse.

According to published sources, Judge Lamberth met early with the new attorney general and gave him one piece of advice. If he wanted to mend fences with the FISA court, Townsend had to go.

She had lost the confidence of the court. Some say the problem was how close she was to the prosecutors, others that the affidavit fiasco had left her damaged.[15]

Not long afterwards, Townsend got word from the attorney general. Her services would no longer be needed. She departed, to head the intelligence office of the Coast Guard.

In early 2001, the FBI sat unknowing in a civil liberties bull's-eye. Many of its field agents were still doing what they had always done—informally sharing information about terrorists. They had a job to do and inside the bureau, at least, sharing with other agents was part of getting the job done.

But the ground had shifted. The FBI had no allies. The judicial coup that incorporated the wall into the FISA court's orders had forced the prosecutors to change sides in the fight over information sharing. Now the prosecutors were demanding that any assurances submitted to the FISA court be strictly accurate. So was the court. And so was the intelligence review office. The assurances looked like boilerplate, but they had become deadly serious, especially for the agents who signed them.

How serious soon became clear. In early 2001, OIPR told Judge Lamberth that it had found another group of investigations where the FBI had not observed the wall. These investigations had nothing to do with al Qaeda, so the FBI teams at work on them had not been touched by Fitzgerald's lash. Sharing across the wall had continued despite the flap in the Southern District. More than a dozen applications had been compromised by false assurances that the wall was in place.

It was the last straw for the FISA court—and for the FBI. The court would insist on an investigation, of course, but that would take months. Judge Lamberth's term would end in a year, and he was determined to strictly enforce the civil liberties protections he had put in place. The court's rules had been broken, and someone was going to pay. Now. Not months from now.

All seven members of the FISA court assembled and agreed. According to Judge Lamberth, one of the seven said, "If I discovered that an affiant in my court had made false statements, I wouldn't spend too much time worrying about whether the false statement was negligent or deliberate. I'd bar him from the courtroom immediately. Why don't we do that?"[16]

It made sense to Judge Lamberth. On March 9, 2001, he sent a letter addressing the attorney general in the bluntest possible terms. "I was disturbed to learn this week that we now have another series of cases in which the FBI affidavits contain information that is not true," he said.[17] The affidavits had been signed by a supervisory agent who was widely viewed as a rising star at the bureau. Not anymore.

At least not if the FISA court had anything to say about it. Effective immediately, Judge Lamberth declared, "the court will not accept any affidavits" from the agent.[18] (The agent was later identified by the *New York Times*, but when I tracked him down, he asked me not to use his name in this book, and I'm honoring his request.) Judge Lamberth also demanded that the intelligence review office "must immediately conduct an inquiry and verify the accuracy of the pleadings in these cases, and explain how such inaccurate information came to be presented to the court."[19]

In the end, Justice's Office of Professional Responsibility expanded its investigation to include the FBI agent's actions. Given the court's harsh language, the investigation wasn't likely to come out well for the agent. OIPR had already decided that the statements were false. The only question seemed to be whether the agent had deceived the court negligently or deliberately. Sanctions could be imposed either way, and if worse came to worst, the agent was at risk of a felony prosecution for making false statements to a federal official. (In fact, years later, after the wall had been discredited by the 9/11 attacks, the investigators would find that the misstatements were simple negligence.)

"The agent was crushed," Townsend remembers.[20] The bureau thought the order would put an end to the agent's career. So did the intelligence review office.

The effect on the FBI was immediate. It did all it could to undo the order. According to Judge Lamberth, "everyone was lobbying me to back off."[21]

The attorney general asked him to reconsider. Separately, FBI Director Louis Freeh "came over and begged me to rescind the order, everything under the sun that could be done about that order."[22] So did the head of FBI counterintelligence and other friends and colleagues of the agent. The disciplinary action was causing turmoil in the bureau.

But Lamberth simply dug in harder. He later told a reporter, "We never rescinded it. We enforced it. And we sent a message to the FBI."[23]

What message was the court sending? That the agents should "tell the truth"[24] about enforcement of the wall, said Judge Lamberth.

Maybe so.

But that wasn't the message FBI agents heard.

What FBI agents heard was a little more pointed and a lot more frightening: Nothing was more likely to end their careers than failing to observe the wall.

Caught between the prosecutors, the intelligence review office, and the FISA court, they had nowhere to hide. If they didn't follow

the civil liberties protections set out by the court to the letter, they would be punished, and harshly. Whether the mistake was negligent or intentional "didn't really matter," in Judge Lamberth's words.[25]

Even after that message had been sent, the court was determined to underline it. In April 2001 the court decided to put every supervisory agent with responsibility for an intelligence team on notice. Each one was required to sign the FISA applications filed by their offices. They had to confirm all of the facts that the applications set forth. Assistant U.S. attorneys were required to do the same.

With the lesson of the disciplined agent still reverberating through the institution, the new requirement was a reminder. What the FISA court had done to the first agent it was quite prepared to do to the rest of them. The new requirement forced every agent and every Justice official to double- and triple-check their compliance with the wall. Any error, any misstep could lead to sanctions.

In the confusion, with new players having to flyspeck the massive FISA applications and triple-check their compliance with the wall, the government began to miss deadlines for submitting wiretap applications. The offices just couldn't process the bulky filings under the court's new civil liberties standards fast enough. For the first time since FISA was enacted in 1978, FISA taps had to be dropped, not for substantive reasons but simply because the old orders had expired before new ones could be requested and approved.

That meant lost coverage. Suddenly, known terrorists could make plans and exchange information without the government learning what was going on. The biggest impact, according to published reports, came in the cases that inspired the court to write the new protections—the investigations of al Qaeda.

As many as twenty al Qaeda wiretap orders were reportedly dropped in the year leading up to August 2001—just as preparations for the 9/11 attacks were reaching a crescendo. Honoring Osama bin Laden's right to be free from unlawful criminal wiretaps was turning out to be costly. Enforcement of the wall was protecting his operatives

from scrutiny at a critical time, just as preparations for the September 11 attacks were at their most intense.

All through this period, the intelligence system was blinking red. Everyone feared and expected a spectacular al Qaeda attack. The director of Central Intelligence was urging greater effort to find out what al Qaeda was up to. Even the FISA court knew that something big was in the works.

But the FBI and other intelligence agencies had something more important to deal with. They were in the grip of a full-fledged bureaucratic panic. Law professors might call the judiciary "the least dangerous branch" of government; FBI agents had a different view.

"FBI personnel involved in FISA matters feared the fate of the agent who had been barred," says one declassified Joint Intelligence Committee report on the 9/11 attacks.[26] FBI intelligence agents "began to avoid even the most pedestrian contact with personnel in criminal components of the Bureau or DOJ [Department of Justice] because it could result in intensive scrutiny by [OIPR] and the FISA court."[27] If a star agent could be held in contempt, it could happen to anyone, they believed. The personal certifications were a constant reminder of the peril faced by anyone investigating al Qaeda.

The wall was getting higher every month.

End Game

On August 22, an FBI analyst named Donna got a call that could have stopped the looming attacks cold. The call came from an FBI detailee at the CIA. The detailee had discovered that a major al Qaeda operative entered the United States in July. This couldn't have been an accident. Something was up, and it was serious.

The last, and most promising, opportunity to halt the plot had opened up. Stopping it should not have been hard. Khalid al-Mihdhar had been living under his own name in California and could have been found there before September 11 if the bureau had moved quickly.

But Donna had a lot to do, and it wasn't until August 28 that she sent an alert about al-Mihdhar, including a related NSA report, to the FBI's New York office.

The NSA report was valuable, but it posed a complication. Less than a year earlier, NSA had begun adding a special "caveat" or legend on the face of reports derived from FISA wiretaps. The caveat said that information in it could not be shared with law enforcement unless special permission had been granted.

This rule, too, was part of the wall. NSA carried out fewer FISA wiretaps than the bureau, and it had always been more independent of the intelligence review office; still, it was dependent on both the office and the court. When those offices grew more demanding about policing the wall, NSA had to follow suit.

Donna wanted to stay within the rules set by the FISA court. She therefore sent the alert only to her intelligence contact on the bin Laden squad.

But as if to underscore the risk of unauthorized sharing that the court had been fighting for over a year, the intelligence investigator sent the alert to his supervisor, who ignored the NSA's caveat and sent the intelligence about terrorists in the United States to the entire criminal investigative team responsible for bin Laden.

One of the squad members, a criminal investigator by the name of Scott, was immediately galvanized. The team investigating the Cole bombing was already up and running. It had resources and manpower. He wanted to put those resources to work right away to find al-Mihdhar.

Donna was alarmed. She knew a violation of the new rules when she saw it. She insisted that Scott destroy the alert. It should not have gone to him under the rules as she understood them.

But Scott was not deterred. Known terrorists had entered the country. This was too important to leave to an undermanned intelligence team.

He argued that his criminal investigators could devote more agents to the search. The criminal investigators, he said, could use

grand jury subpoenas and other law enforcement tools that were far quicker than those available to the intelligence side of the Bureau. They had all the resources they needed inside the United States. The intelligence guys didn't.

He was right. At this time, the FBI's intelligence arm was notoriously underfunded and sometimes even disrespected by the rest of the bureau.

Even so, Donna insisted, the resources could not be used. The wall prevented the mixing of criminal and intelligence investigations.

Scott must have been the bravest or the most clueless agent in the bureau. He ignored Donna's advice and kept pressing.

Donna appealed to the FBI general counsel's office for a ruling. That office knew the score. Its lawyers had seen the FISA court's crusade to reinforce the wall up close. The FBI's general counsel, Larry Parkinson, would later tell the 9/11 Commission staff that the disciplined agent's fate was "'a big deal' for a lot of people." It "spooked" them, and they "became less aggressive."[28]

Spooked, the lawyers certainly were. They sided with Donna. Scott was out of line. He was risking a civil liberties scandal that would put his career and theirs in jeopardy. The search would have to be done by the thinly staffed intelligence arm of the bureau. Scott and his resources were off limits.

Even after this definitive ruling, Scott refused to go quietly. He protested in eerily prescient terms: "Someday someone will die—and wall or not—the public will not understand why we were not more effective and throwing every resource we had at certain 'problems.' Let's hope the [lawyers who gave the advice] will stand behind their decisions then, especially since the biggest threat to us now, UBL [Usama Bin (sic) Laden], is getting the most 'protection.'"[29]

From Washington, Scott's fight to get criminal resources into the search for al-Mihdhar looks like an act of courage that borders on the foolhardy. He had already received intelligence in violation of the wall, and now he was kicking up a fuss, bringing in lawyers, drawing

attention to the violation, and advertising his disagreement with the FISA court's rules.

It was as brave in its way as Melendez-Perez's decision to send Kahtani home based on little more than intuition. But unlike Melendez-Perez, Scott got no help from his higher-ups. The wall had become a maze of walls. And in the end, one agent's determination to do his job was not enough to overcome all the walls—the complex civil liberties rules, the harsh enforcement regime devised the intelligence review office and the FISA court, the lurking machinery of scandal.

Scott had nowhere left to go. He did what he was told. He left the job of finding al-Mihdhar to Donna and the understaffed FBI intelligence unit.

They were still looking when September 11 dawned, bright and crisp.

4 Never Again

It was the kind of day that made Melissa Doi want to dance. But then, most days did. At 32, she knew she'd never realize her dream of becoming a ballerina but Melissa was still a dancer at heart. "She would get happy and just dance," said a friend and former classmate. "Salsa, kick lines, everything."[1] And what a day it was for dancing—the first break from summer's muggy heat. Plus, it was Tuesday, and on Friday, Melissa was planning to take her mother to Italy.

There was a lot to do before then. She was already at work at IQ Financial Systems on the eighty-third floor of the World Trade Center when the plane hit.

She called 911; the transcript was released years later.

> Melissa: Holy Mary, mother of God . . .
>
> Operator: Hi there, ma'am how are you doing?
>
> Melissa: Is it . . . is it . . . are they going to be able to get someone up here?
>
> Operator: Well, of course ma'am, we're coming up for you.
>
> Melissa: Well, there's no one here yet, and the floor is completely engulfed. We're on the floor and we can't breathe . . . And it's very, very, very hot . . .
>
> Operator: Ma'am listen, everybody's coming, everybody knows, everybody knows what happened, okay? . . .
>
> Melissa: . . . It's very hot, everywhere on the floor . . . It's very hot. I see . . . I don't see any air anymore . . . All I see is smoke.
>
> Operator: Okay dear, I'm so sorry . . . stay calm with me . . .

Melissa: I'm going to die aren't I?

Operator: No, no, no, no, no, no, no say your, ma'am, say your prayers.

Melissa: I'm going to die.

Operator: You gotta think positive . . .

Melissa: Please, God.

Operator: You're doing a good job ma'am . . .

Melissa: No, it's so hot, I'm burning up . . . Stay on the line with me please, I feel like I'm dying.[2]

Melissa Doi didn't speak again.

I felt an almost personal sense of responsibility. After all, I had supported the wall. I'd done my best in government and in my writings to influence the tiny community of lawyers who had debated the issue over the years. I thought the risks to civil liberties were hypothetical, but I also thought it couldn't hurt to add a few extra safeguards to the process. I never imagined that it would end with three thousand deaths.

I saw things differently after that. The lesson of 9/11 and the wall was clear: It's foolish to write rules for government to protect against hypothetical civil liberties or privacy abuses, and even more foolish to enforce those rules as though they matter more than the security mission. Rules that restrict intelligence gathering are never cost-free; sometimes they impose very real costs in terms of lives lost.

I grew deeply skeptical of efforts to write new privacy limits on government in the absence of demonstrated abuses that required new limits. We should not again put American lives at risk for the sake of some speculative gain in civil liberties.

I thought that would be obvious to everyone. In the wake of a tragedy like 9/11, it would be unseemly and divisive to blame the people who helped create the wall for the failures that occurred in August of 2001. No one knew then what the cost of building such a separation would be. But we should know now, I thought; we can't prevent every imaginable privacy abuse without hampering the fight against terror, risking more attacks and more dead.

I thought then that everyone—from the privacy groups to the prosecutors and intelligence agencies—would join in a more realistic view of civil liberties rules after the attacks. And for a while it seemed to be so. Few people blamed the civil liberties groups for what happened on that day. The USA PATRIOT Act[3] was put together quickly to override the wall and to make a host of other small changes to the rules governing terrorism investigations. After detailed negotiations between the Bush Justice Department and the Senate Judiciary committee run by Sen. Patrick Leahy (D-VT), a compromise bill was taken to the floor. It was a modest set of changes in the right direction, and I thought it would set the tone for future civil liberties debates.

Boy, was I wrong. Within a year or two of passage, civil liberties groups began treating the USA PATRIOT Act as a symbol of overreaction. Privacy groups argued, without much evidence that I could see, that civil liberties had been put at risk by the response to 9/11. They began to attack new programs, like the TIPS program to encourage citizens to report suspicious conduct, or Admiral Poindexter's Total Information Awareness program, which would have developed new data analysis (and privacy protection) tools to identify terrorists. And they soon found success. TIPS was quickly canceled, and in January 2003, Sen. Ron Wyden (D-OR) attached an appropriations rider that dropped funding for Admiral Poindexter's effort.

It made me uneasy. I knew Poindexter. He was tone deaf to politics but smart about technology. What he hoped to do was exactly the kind of research that DARPA (the Defense Advanced Research Project Agency) had been doing for forty years—pushing the envelope of what was possible in the hopes of finding new solutions to hard problems. Understanding that a technology was possible was not the same as deploying it, and Poindexter was alert to privacy risks, which he also hoped to head off with new technologies. He even invited several privacy groups to an early briefing to reassure them of his good faith.

But the privacy groups were merciless. Immediately after they were given the conciliatory briefings, they leaked the story, putting

the worst possible spin on its every aspect. This didn't seem like the new, more cautious civil liberties lobby, attentive to the importance of security as well as privacy, that might have been expected in the wake of 9/11.

Nor did it seem likely to create a new, more balanced atmosphere in the halls of government, where it did not go unnoticed that John Poindexter was the only person forced from government because of the events surrounding 9/11.

There was worse to come.

A key failure of August 2001 was the inability of an undermanned FBI intelligence unit to find the two hardened al Qaeda killers that they thought might be in the United States and planning a major operation. Yet all the data necessary to find the ringleaders, and most of their accomplices, was readily available in private computer systems.

If they had obtained access to the data in airline reservation systems, even Donna and the undermanned FBI intelligence team could have immediately found the two terrorists they were looking for. And they could have broken the rest of the plot wide open by finding the links between those two and the other hijackers.

For example, three other hijackers, including Mohamed Atta, the plot's operational ringleader, used the same addresses as the two known terrorists.

Another hijacker used the same frequent-flyer number as al-Mihdhar. And five other hijackers used the same phone numbers as Mohamed Atta. That's eleven out of nineteen—all linked by simple data from the airline reservation system.

The information necessary to prevent 9/11 was in plain sight. But there was no easy way for government to obtain reservation data on domestic flights, and certainly not *before* a crime had been committed. (Officials could also have found a twelfth hijacker in an INS watch list for expired visas, and the remaining seven could have been flagged through him by matching the addresses of people who lived with him or his co-conspirators.)

Just to make this failure particularly excruciating, that same reservation data was routinely gathered on a voluntary basis by customs officials for international flights, so the government had tools for analyzing passenger lists. It had simply never applied those tools to domestic flights.

The government was determined not to let that happen again. First the Justice Department and then DHS, after its creation, launched an ambitious program to gain access to domestic airline reservation data. The creaking air security regime was being overhauled. A system that simply looked for weapons and the handful of people on the "no-fly" list wouldn't cut it anymore. It was obvious that reservation data could help identify risky passengers for closer inspection. To build a system that would do this, DHS launched CAPPS II (the second-generation Computer Assisted Passenger Pre-Screening System).

Privacy groups quickly rose to the attack. It was less than eighteen months after 9/11, but the groups had already won two victories, and now they were shifting their targets. Instead of going after half-formed (and arguably half-baked) programs, now they would try to kill a program that responded directly to the failings of August 2001.

Buoyed by past victories, they spared no hyperbole. "This system threatens to create a permanent blacklisted underclass of Americans who cannot travel freely," an ACLU legislative counsel, told the Associated Press in February 2003.[4] Recalling Admiral Poindexter, the ACLU's Barry Steinhardt declared that CAPPS II would "give the government an opening to create the kind of Big Brother program that Americans rejected so resoundingly in the Pentagon."[5]

By June 2003 the organization had filed suit to block the program. The ACLU and other left-leaning privacy groups built an alliance with libertarian-conservative groups like the American Conservative Union, the Eagle Forum, and Americans for Tax Reform. "You name it, we've gone into bed with them," an ACLU spokeswoman told the press.[6] By August this left-right coalition was lobbying heavily against CAPPS II.

And by September, the privacy groups had won.

Congressional appropriators stopped the program dead in its tracks, prohibiting implementation of CAPPS II and any similar program until the General Accountability Office certified that ten strict conditions had been met. The professionally dissatisfied auditors at that office were unlikely ever to certify that the conditions had been met. The conditions seemed to be a prelude to killing the program entirely.

I was growing more and more disillusioned with the privacy groups. They seemed to have lost any sense of responsibility, either for past disasters or for future security. Supported by the *New York Times* and the rest of the establishment media, they were now opposing any new security measure as an intrusion on civil liberties—even if the risk to civil liberties was entirely hypothetical.

By December of 2003 when I testified before the 9/11 Commission, I was worried enough to make the point explicit:

> Perhaps it isn't fair to blame all the people who helped to create the wall for the failures that occurred in August of 2001. No one knew then what the cost of building that wall would be.
>
> But now we do know. Or at least we should. We should know that we can't prevent every imaginable privacy abuse without hampering the fight against terror. We should know that an appetite for privacy scandals hampers the fight against terror. And we should know that, sooner or later, the consequence of these actions will be more attacks and more dead Americans, perhaps in numbers we can hardly fathom.
>
> We should know that. But somehow we don't . . .
>
> [B]it by bit, we are again creating the political and legal climate of August 2001.
>
> And sooner or later, I fear, August will again lead to September.[7]

I still believed in protecting privacy and civil liberties. I had served on a task force created by the Markle Foundation to find ways to use technology and data to fight terrorism while protecting privacy. And I urged the 9/11 Commission to adopt the Markle task force's

recommendations, which called for expanding both the use of data and the use of electronic audits to create accountability for any actual privacy abuses that might occur. (There's a longer description of my still-evolving thoughts on how to protect privacy without sacrificing security in Part Four of this book.)

I can't say that my testimony to the 9/11 Commission made many converts. When it came time to question me, Commissioner Ben-Veniste opened with a speech praising "those who are vigilant in protecting our constitutional rights and civil liberties against overreaching in times of national crisis . . . because they are courageous in the face of what's seen to be a popular demand."[8]

Courageous? By then I'd had enough.

"I have a different definition of courage than Commissioner Ben-Veniste," I responded when it was my turn to speak. "I don't think it takes any courage in this town to agree with the *New York Times*."[9]

In 2004, determined to do more than simply manage a prosperous law practice while the government dealt with the terrorist threat, I accepted an invitation to become general counsel of the Robb-Silberman Commission.[10] The commission's first job was to investigate intelligence failures concerning Iraqi weapons of mass destruction. But it was also charged with determining how to avoid such failures—and how to improve our intelligence about WMD in the future. I was in charge of the drafting team, and I was happy with the final report, which represented a bipartisan consensus on the commission and resulted in numerous changes in government practice.

As the Robb-Silberman Commission was winding down in 2005, Michael Chertoff asked me to come over for a talk. He had just become the new Secretary of Homeland Security.

Created two years earlier, DHS had started with nothing—no offices, no furniture, no copiers. And from day one it had been in the spotlight. Its first secretary, Tom Ridge, had managed the remarkable feat of cobbling together a working agency on the fly, but occasionally the baling wire broke or the chewing gum gave out.

The first thing the Chertoff team did when it geared up was to conduct a review of how the department was working and what it needed. More than anything, they decided, it needed a policy office that could bring coherence to the department's sprawling components. They needed an undersecretary for policy, and Secretary Chertoff was offering me the job.

I went to DHS headquarters for the interview. The department was housed in an old girls school, and it still felt like one. "Salve Regina" said the carved stone lintel over the entrance to the secretary's suite. The building was in a nice neighborhood; across the street were the Swedish embassy and the campus of American University. But the place itself was a testament to the haste with which DHS was created.

The U.S. Navy had taken it from the headmistress of Mt. Vernon Seminary in 1941 (literally—they kicked the students out, moved in, and dared her to sue). They hadn't updated some of the dorms since then. When DHS was looking for space, it found that the navy was planning to move out, and they claimed the grounds. But the navy was in no hurry to move. So they gave DHS some of the less attractive space and kept the best offices for themselves.

Chertoff's office still had the worn couch and ragged industrial carpet installed for the GS-15 who'd occupied it before him. That unprepossessing office was symbolic in my mind of the department's plight. DHS had several huge components to coordinate. Agencies like the Coast Guard, Customs and Border Protection, and the Secret Service could trace their origins back more than a hundred years. Each had built for its leader an office that was far more impressive than the office of their new boss, the secretary of DHS. In the same way, the components' beefy, multibillion-dollar budgets and staffs allowed the components to set their own course with little risk of oversight by Secretary Chertoff's limited staff.

But Chertoff was not worried about his quarters. He was determined to make the department run, and to his cadence. A gaunt, intense man—a runner with a deep competitive streak—Chertoff had aced law

school. (He was the model for some of the most intimidating characters in Scott Turow's first book, *One L*, about his experience at Harvard Law School.) Chertoff had clerked on the Supreme Court, prosecuted mobsters in New York and New Jersey, run the criminal division at Justice, and been appointed to a federal court of appeals. Exactly the career he must have hoped for when he was a law student.

But the federal bench is a slow place after all that action. The phone never rings. And Chertoff loves action. Now, after two years of judging, he was rested and eager to get back in the fray. DHS was a startup, a department with no tradition, and no one to say "we don't do it that way here." He was offering me a chance to join him in writing on that blank slate. The policy office would be brand-new—a startup within a startup. The good news was that the office could be whatever I wanted to make of it. The downside was that I'd have to assemble it from scratch.

I had a general idea how hard that might be. I had helped start the Department of Education for another federal judge, Shirley Hufstedler. Unlike private startups, government startups aren't created out of whole cloth. They're assembled from bits and pieces of other agencies, and their creation is supposed to demonstrate that their mission now has a new and higher priority. But the other agencies don't see it that way. For them, the new department is an interloper that is stealing a piece of the old agencies' turf. Since turf stealing is the bureaucratic equivalent of cattle rustling, the agencies that are losing bits and pieces of their organization show no mercy. The Health, Education, and Welfare leadership that contributed most of the Department of Education did its best not to leave us even working furniture, let alone a working agency or employees. It took years to build a functioning Education Department, even though the bulk of the Department was simply the "E" in HEW.

DHS was far bigger. (Today it is roughly the size of the Department of the Army, larger than Navy or Air Force, and in fact larger than any department other than Defense and Veterans Affairs.) And unlike Education, it had no core. Its seven main components came

from four cabinet agencies. The Secretary and his staff would have to get these proud, independent agencies pulling in the same direction, using only the tools put together in two years by Secretary Ridge. My assignment would be the hardest government job I had ever undertaken. But also the most rewarding. Chertoff would turn out not only to be as smart as his résumé suggested, but also willing to make tough policy decisions and to stick with his people when those decisions turned out to be unpopular with the *New York Times* editorial board. Like me, he had lived with the wall and knew how a fear of hypothetical privacy concerns had crippled cooperation between agencies. He, too, was determined not to let Americans go unprotected again.

"When can I start?" I asked.

Just about the first order of business for the new DHS policy office was figuring out how the United States could control international travel. During the year before 9/11, twenty hijackers had slipped into the United States. And so had several hundred million other travelers. Finding twenty terrorists in a stream of hundreds of millions of entrants sounds impossible. In fact, our border officials did stop one of them, a remarkable feat given the technology and standards of the day.

But a 5 percent success rate in stopping terrorists is not a passing grade. We had to do better.

In the immediate aftermath of 9/11, the government tried going back to the methods of the 1950s and 1960s. Every car was stopped. Every air passenger was interviewed and searched. The results were predictable. Soon, the wait at the Canadian border was measured in hours and miles, not minutes and yards. At airports, the lines grew longer and crawled to a halt.

It became clear why these methods had been abandoned nearly everywhere by the 1980s. They required that we give up the benefits of modern travel. We simply could not inspect every person crossing the border. And bad as 9/11 had been, we weren't willing to give up travel because of it.

By the time I came on board, DHS had begun to feel its way toward that path. The department was playing by ear. But a solution was beginning to emerge. The role of my policy office was to crystallize it.

We knew we couldn't inspect every passenger at the booth. We didn't have time. But if we could get enough information in advance, and analyze it quickly, we could conduct a "virtual inspection" before the passenger had even arrived. We could use what we knew about travelers to separate the business travelers who crossed the Atlantic every Sunday from travelers who needed a much closer look.

We didn't need to find terrorists using their travel data. We just needed to identify those travelers who ought to get more attention. They would be sent for a "secondary" inspection that more or less resembled what everyone went through at the border in 1950. They'd be interviewed at length and, if necessary, their luggage could be examined. It was the secondary inspection of Kahtani that kept him out of the country and off American Flight 77. With a bit of information about who was coming, and a clear sense of whom we wanted to keep out, we could supplement our officers' intuition, flagging suspect travelers and waving through the rest. We could concentrate our inspectors' talents on a smaller pool of more likely prospects.

We'd be diverting the growth of jet travel just a bit. We couldn't bring back the old system, but we could use new technology ourselves to restore a measure of security.

This was new. In the first half of the twentieth century, we couldn't have screened passengers before they arrived. Border systems then relied on personal interviews, visas, and passports because they had to. But now information technology was doubling in capability even faster than travel volume did. Data once was costly to retain, store, and analyze, but now it was becoming cheaper and easier every day.

What's more, the airlines whose passengers were overloading the old border system were using new technology to identify and manage the travel of those same passengers. If we could use *their* data to identify the handful of risky passengers who needed an interview, we could do our screening while the plane was in the air.

What information did we need? We boiled it down to three things.

First, we needed to know in advance who was coming to the United States. In theory, we could wait until the passenger showed up at the front of the line and presented his passport. We could then run his name through our computer systems to see what we already knew about him.

But in the real world, that would never work. Computer systems are never instantaneous, and the more information they process the slower they run. Everyone understands this. None of us turn on our computers and sit with our fingers on the keyboard while Windows boots up. We go and pour a cup of coffee, and when we return, our data is ready.

DHS needed the same thing—time to let the computer run before the passenger showed up for inspection. We couldn't afford to add any more time to primary screening. After all, with 90 million passengers arriving by air each year, adding even ten seconds to the average interview would add ten thousand extra days of waiting into the system. We also needed to process information in advance to avoid mistakes. The fewer decisions we forced border officers to make in thirty seconds or less, the less risk there was of error.

DHS already had some ways to find out who was coming to the United States. For countries where the visa requirement still applied, we knew which travelers had been given visas. We could prepare for those travelers before they showed up.

Things were worse if the travelers were coming from one of the two dozen countries for which we'd abolished the visa system. For these "visa waiver" travelers, we didn't know they were coming at all until they showed up at the booth in JFK in New York or Dulles Airport in Washington. Since half of our overseas travelers were from visa-waiver countries, this was a big hole.

We filled it by tapping the information systems the airlines were already using. In addition to the passenger manifests for each flight, we wanted information from the system the airline uses to keep track

of travelers' reservations. This system usually contains a bit more information—such as whom the passenger is traveling with, the name of his travel agency, emergency contact information, and payment details. The data is not especially sensitive (it had better not be, since it is shared widely among airline personnel). But as the example of the 9/11 hijackers showed, travel reservations could be crucial to making connections between the travelers we were already aware of and their accomplices about whom we know nothing.

That was our answer to the first question: Who's coming?

And that begs the second question: Who shouldn't come?

Again, in the aftermath of 9/11, much progress had been made in answering this question. The shocking lack of coordination among the agencies tracking potential terrorists had ended. The consular officials who issue visas had access to the same consolidated list of potential threats as the DHS border officials, the CIA counterterrorism agents, and the FBI investigators.

That's important. But really, if you wanted to know which French travelers posed the greatest risk, would you ask the CIA? Or would you ask the French security agencies?

The right answer, of course, is "why not ask both?" We did. Unfortunately, the French weren't talking. Although the United States had made concerted efforts after 9/11 to get agreements with other countries to share lists of suspected terrorists, practically none acquiesced. We had a handful of agreements with close allies, but even countries like France and Germany had not signed up.

Outside of information about terrorism suspects, cooperation was even worse. We had practically no information about criminals crossing our borders. If a thirty-five-year-old British man showed up with a ten-year-old boy who was traveling with him, and DHS officials became suspicious of the relationship, they had no way of finding out whether the man had been convicted of molesting children in the UK. The Brits didn't share that information with us. Neither did any of our allies, with the exception of the Canadians.

Oddly, the Canadians would not give DHS a list of suspected terrorists, not even those living minutes from our unguarded border. But, perhaps because Canadian troopers stop Michigan drivers for speeding every day and need to know whether they're wanted, Canada and the United States have long exchanged data on the criminal records of their citizens. That was our only international criminal data exchange.

Whether a traveler's crimes were raising funds for a terrorist organization or smuggling drugs or both, and no matter how relevant they might be for the scrutiny he should get at the border, the traveler left his crimes behind him when he boarded the plane to the United States.

We were going to need more. We didn't have to take as gospel everything foreign governments said about their citizens, but we did need to know what they thought. Because if *they* were worried about a particular traveler, that was reason enough to ask him some questions before letting him into *our* country. We could make up our own minds, but we needed to get the information first.

The hard question was how we'd do that. Other countries weren't firmly opposed to sharing information. After all, that would make their border officials more effective, too. But sharing information with the United States was bound to meet some political resistance at home. Our allies needed help in overcoming that resistance.

In theory, the answers to the two questions "Who's coming?" and "Who shouldn't come?" make a complete screening system: We know who's coming, and we know who shouldn't be let in without a close look. But we have smart, adaptable adversaries. If our defense depends on knowing the names of the bad guys, the first thing that bad guys will do is change their names.

That leads to our third and last question: How do we know who is who? How can we be sure that the name on the manifest list and the passport is the right one?

We could start with better passports. Congress had already started us down a path to more secure passports. After 9/11, it declared that countries would lose their visa-free travel privileges if they did

not adopt passports with improved security features, including an electronic chip to hold biometric data securely. Countries were also required to promptly report the identification numbers of lost and stolen blank passports so we could watch for what would otherwise be perfect forgeries made from official blanks.

The deadline for meeting these requirements would occur on our watch. If we held firm, we could radically reduce the risk of identity fraud. That in turn would bolster the effectiveness of our identity-based screening program.

But Tom Ridge's team had gone one step further to attack the identity theft problem. They had begun fingerprinting foreign visitors to the United States. Initially, they took only two fingerprints, because the main purpose of the prints was to tie a person to his name and passport biometrically. We couldn't necessarily stop all identity theft with the prints, but we could guarantee that, once a traveler presented himself and his passport under one name, he'd never be able to use a different name or passport without setting off alarms.

On examination, this was the most solid of the three legs on which a new approach to border security would rest. The Ridge team had launched many good initiatives designed to lock travelers to a single identity. It was up to us to bring them home successfully. We had to press our allies to adopt better passport technology and to report lost and stolen passports, using the leverage of the visa-waiver program. And we had to implement the fingerprint program successfully at a time when some countries were taking umbrage at the very idea. (Brazil had announced that it would fingerprint Americans in retaliation and then had jailed an American Airlines pilot who offered his middle finger to the officers administering the process.)

We ended up expanding these identification programs in several ways. We switched to gathering ten prints instead of two. This didn't add to the protection against identity theft, but it did give us a new way to identify those whom we wanted to keep out of the country. The Defense Department had begun to gather fingerprints in safe houses and even from the remnants of roadside bombs in Iraq and Afghanistan. We didn't know exactly whose prints they were, but if

anyone who left prints on a roadside bomb ever showed up in the United States, we were sure we wanted to talk to him.

And rather than simply play defense in other countries, we went on the offensive, urging other countries to adopt compatible fingerprint systems for screening purposes. The more countries there were who had locked a person to his passport, the harder it would be for him to take on a new identity. By the time I left office, Japan had already begun implementing its own prints-at-the-border system, the UK was using prints for asylum applicants and was testing a border fingerprint system, and the European Union had announced plans for a similar system. Implementation, meanwhile, went so smoothly that protests petered out as travelers realized how little the process resembled being booked for a crime.

When we finished constructing the new border strategy, we were pleased. Commercial jet travel had completely overturned the border control measures that the United States and other countries had relied on for much of the twentieth century. And by the 1980s, border controls were under siege, collapsing as international travel continued to double each decade. But we didn't have to abandon control of our borders if we used information technology prudently. We could build a screening system that told us who was coming and whom we should look at closely, and we could satisfy any reasonable privacy concerns.

In fact, we were well down the road, thanks to Congress and our predecessors. The "who's coming" measures were already online, and so were the measures to lock travelers to a single identity.

As long as we kept these two initiatives on course, we could devote our main effort to getting data that would allow us to identify suspect travelers. Of course, doing that wouldn't be easy. We'd be fighting all the defenders the status quo could muster.

In the end, it would take a massive diplomatic effort, multiple international negotiations, a harsh battle with other departments and the National Security Council.

And a game of chicken with the entire European Union.