# SKATING ON STILTS

## Why We Aren't Stopping Tomorrow's Terrorism

Stewart A. Baker

HOOVER INSTITUTION PRESS
Stanford University Stanford, California

# 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.

*The Hoover Institution on War, Revolution and Peace, founded at Stanford University in 1919 by Herbert Hoover, who went on to become the thirty-first president of the United States, is an interdisciplinary research center for advanced study on domestic and international affairs. The views expressed in its publications are entirely those of the authors and do not necessarily reflect the views of the staff, officers, or Board of Overseers of the Hoover Institution.*

*www.hoover.org*

**Hoover Institution Press Publication No. 591**

Hoover Institution at Leland Stanford Junior University,
Stanford, California, 94305–6010



First printing 2010
16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1

Manufactured in the United States of America

The paper used in this publication meets the minimum Requirements of the American National Standard for Information Sciences—Permanence of Paper for Printed Library Materials, ANSI/NISO Z39.48-1992. ♾

Cataloging-in-Publication Data is available from the Library of Congress.
ISBN-13: 978-0-8179-1154-6 (cloth)

ISBN-13: 978-0-8179-1156-0 (e-book)