SKATING ON STILTS

Why We Aren't Stopping Tomorrow's Terrorism

Stewart A. Baker

HOOVER INSTITUTION PRESS
Stanford University Stanford, California

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.

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)