PART TWO | FLIGHT AND FACTS

5 Europe Picks a Privacy Fight

Jonathan Faull was laying down the law. Trim and articulate, Faull was a director general in the European Commission—the highest-ranking career official in Europe's executive branch.

We sat opposite each other in an Arlington high-rise with striking views across the Potomac to the Washington Monument and the Mall. A phalanx of other European officials was arrayed across formica tables from their DHS counterparts.

It was the first meeting of the U.S.-EU Policy Dialogue on Border and Transportation Security since I had become head of policy for the Department of Homeland Security.

And it wasn't going well.

The policy dialogue was a fancy name for regular meetings between top officials at the Department of Homeland Security and the European Commission. It had been advertised as a good way to work with like-minded countries. Why go to twenty-seven European capitals, the commission had argued, when you can come to Brussels and talk to all of Europe? But we were constantly surprised at how contentious the dialogue seemed to be. Weren't we allies? Wasn't the fight against terrorism something we all shared? Somehow that didn't make the talks less combative.

Today, as so often recently, the contention focused on airline reservation data. The European Union, Faull said, had now completed its review of DHS's compliance with the rules for how to handle airline reservation data. European inspectors had sent DHS a questionnaire

to complete, had reviewed DHS's operations in the field, and then had spent a day quizzing DHS officials about their practices.

The European Union was not completely satisfied. The inspectors had found substantial compliance with the rules, Faull acknowledged, but this compliance had come too slowly, and there was plenty of room for improvement in the department's handling of reservation data. Faull made it clear that the commission would be watching closely in future. And next year, he promised, there would be another inspection and another report.

Faull is a formidable man. He had served in important positions throughout the European Commission—overcoming by sheer ability the innate suspicion that all British officials must endure in Brussels, where Brits are viewed as not truly committed to the European project. Despite this handicap, Faull had risen to the top of the European Commission's fastest-growing directorate—the directorate of Justice, Freedom and Security.

That wasn't helping him today. Perhaps it was just his accent or the continental tailoring of his suit, but to the Americans it seemed that a whiff of condescension hung in the air.

DHS was being schooled. The department may have passed its midterm exam, but by European standards it was not a particularly good student. "The U.S. gets a B," the German who led the review told one DHS official. Europe would expect a better performance next time.

If the department did not meet European standards, Faull made clear, the European Commission could declare that United States privacy law was not "adequate." That in turn would cut off the flow of airline reservation data that DHS was using to keep terrorists out of a still-traumatized United States.

The threat was deadly serious.

The roots of this conflict could be found in the rubble of the World Trade Center. In the weeks after the attacks, Americans asked how we could have missed the evidence that attacks were being planned on American soil.

Our attention soon focused on the wall between the intelligence agencies looking for terrorists and the law enforcement agencies charged with investigating crimes. Appalled at the failure to connect the dots, lawmakers asked why the wall had been raised so high between investigators with a common mission. There was no evidence that the wall had ever done much to protect civil liberties, but evidence of the harm it could do was still smoking in two American cities.

Backed by Congress, the Bush administration immediately acted to tear down the wall. Three separate laws passed between 2001 and 2004 required the sharing of all terrorism data among intelligence and law enforcement agencies. After that, Congress must have thought, there could be no barriers left; information on terrorists would have to be shared throughout the United States government.

At the same time that the wall and its costs were being publicly debated, a second lesson from the attacks was circulating quietly through the administration. An analysis of the hijackers' airline reservations showed that the entire plot could have been broken up if authorities had simply gotten access to the airline's travel reservation systems.

Remember the two terrorists the FBI was looking for but could not find in August 2001? It turned out that they could have been found easily if the government had simply had access to airplane reservation data. And, once the two were found, reservation data would have exposed links to nearly a dozen of the other hijackers, who shared addresses, phone numbers, or frequent flyer numbers with the known terrorists.

Though this analysis was not widely discussed in public, it had an immediate effect on Congress. Less than two months after the September 11 terrorist attacks, in the Aviation and Transportation Security Act of 2001[1], Congress required all air carriers to provide airline reservation data for travelers flying into the country. The data, known as "passenger name records" or PNR, would supplement information drawn from the passenger manifest for each flight. (Airline manifests contain basic information on all passengers and crew on a

particular flight.) By requiring that the airlines turn over PNR and manifest information for all passengers arriving from overseas, Congress ensured that border authorities would be able to perform the analysis that was not done in the days before September 11.

When DHS took over border management, it expanded the information systems used to screen arriving passengers. And we had made passenger travel data central to our new strategy. It told us two things: who was coming and who was risky. Knowing who was coming from Western Europe was especially important. Because no visas were required to travel from Western Europe, without the airline information we would be left in the dark until the passengers showed up at the customs booth. The data was also useful in figuring out who was risky. As the 9/11 hijacker data showed, we could sometimes find risky travelers because the reservation data exposed hidden connections among the passengers.

That's certainly what it did in June 2003.

It was an unseasonably cool day at Chicago's O'Hare international airport. DHS border inspectors were busy but not overwhelmed. The U.S.-led war to topple Saddam Hussein's Ba'athist regime in Iraq had been launched a little less than three months earlier. Fear of terrorism had kept some would-be passengers from the skies, but O'Hare was still operating at a fairly brisk pace.

A Jordanian man named Ra'ed al-Banna was among the throng of passengers who had just arrived on KLM flight 611 from Amsterdam. After waiting in line, al-Banna presented his passport to a U.S. Customs and Border Protection officer.

Without the computerized targeting system and data drawn from airline reservations and past travel, the officer would have had less than a minute's worth of information with which to make a decision about al-Banna. He could look at al-Banna's passport, and he could ask him a question or two. Unless there was something distinctly odd about the passport or the answers, al-Banna would be waved along, just like the mass of international travelers queuing behind him.

Al-Banna had a legitimate Jordanian passport; he held a valid visa that allowed him to work in the United States; and he had visited the United States before for a lengthy stay.

Short, dark, and good-looking, he was entirely comfortable in the West; he spoke English well and knew Nirvana from Nine-Inch Nails. On a quick look, there was no reason not to admit him; his paperwork was in order.

But on June 13, 2003, the data in the system called for a closer look. Al-Banna was sent to secondary inspection, where officers could inspect his luggage and documents and question him more closely. They asked him about his past travel to the United States, and the longer he talked, the less comfortable the officers became. They weren't satisfied that he was being completely truthful in his answers. They decided to refuse him admission. They took al-Banna's picture and fingerprints and put him on a plane back to Jordan.

So far it was a fairly routine day at the border. Not until nearly two years later did events in Iraq give it a new and troubling significance.

On February 28, 2005, at about 8:30 in the morning, several hundred police recruits were lined up outside a clinic in Hilla, a city in the south of Iraq. With no warning, a car drove into the crowd and detonated a massive bomb. One hundred thirty-two people were killed, and about as many were wounded. It was the deadliest suicide bombing Iraq had seen, and the death toll remains one of the highest of the war.

The driver was Ra'ed al-Banna. It wasn't easy to identify him. But when the authorities found the steering wheel of his car, his forearm was still chained to it.

A few days later, his father in Jordan got a short phone call from Iraq. "We congratulate you on the martyrdom of Raed," the caller said. To this day, the family insists that they had no clue when al-Banna decided to join the extremists.

The al-Banna case is the one DHS officials talked about most often, but it wasn't the only one. Every port of entry has a story about terrorist suspects turned away or smugglers identified using reservation data.

In Atlanta, for example, DHS officials at the airport spotted a member of a Pakistani extremist organization flying in from South America. The man had previously been identified conducting surveillance of the American ambassador to Argentina and trying to enter the U.S. Embassy under the guise of official business. That was a victory for the automated targeting system. Even better, the DHS officers found that the extremist's travel reservations linked him to two other travelers. Without that data, these previously unknown radicals would have entered the United States easily. With it, DHS officers quickly got them to admit that they were traveling together.

In Minneapolis, DHS officials acting on a tip from the unit that evaluates targeting data stopped a Qatari student with a valid visa. On inspection, it turned out that his laptop contained clips showing various improvised explosive devices exploding against soldiers and vehicles as well as a manual in Arabic on how to make the devices. Perhaps most troubling, the file also contained images of the student reading his will and quoting the Koran. Charged criminally based on his statements during secondary inspection, the traveler pleaded guilty to visa fraud.

In Newark, DHS officers noticed a woman returning from the Dominican Republic with her children. That didn't seem unusual until the officers examined her travel reservation data. Then they discovered that she hadn't taken the kids with her on the outbound flight. After more digging, they found that the woman had made many trips to the Caribbean island nation. Each time she left without children; each time she returned with them; and each time they were different children.

More research in the system uncovered links between this woman and other travelers. It turned out that many of them had the same travel patterns—they would leave the United States alone and come back with children. The travelers were members of an international child-smuggling ring, and reservation data was the key to taking it down.

The value of reservation data was well-established. And its privacy impact was small; this wasn't especially sensitive information, and it

was already being shared by travel agents, airlines, baggage handlers, and the like.

So why, I wondered, was Jonathan Faull trying to put limits on its use to fight terrorism? How did Europe come to enlist in such an unlikely privacy crusade?

In the summer of 2002, less than a year after the 9/11 attacks, the last of the debris from the World Trade Center had just been removed. The final steel girder standing—the Stars and Stripes beam—had been cut down in a moving ceremony. The remaining recovery workers scrawled messages on it; some touched it as though it were a coffin.

But Europe's attention had already focused on how to roll back the measures the United States had taken to protect itself from repeat attacks. That summer, the European Commission approached the United States and lodged a formal objection to the gathering of travel reservation data on passengers flying from the European Union.

U.S. rules for handling the data were simply not "adequate," the European Union declared. Unless the United States accepted European limits on how travel information could be gathered and processed, Brussels said, European airlines would be forbidden to supply the information.

The Europeans had just fired the first shot in an international privacy war—a war between countries that ought to have been on the same side.

Oddly, the road to confrontation began with a moment of transatlantic convergence. In 1973, as computerized records began to spread through government, a U.S. government advisory committee recommended a code of fair information practices. The code prohibited secret data systems, gave all individuals the right to find out what information had been recorded about them and to correct erroneous records, and insisted that information obtained for one purpose must not be used for other purposes without the individual's consent.

In 1974, the U.S. Congress enacted the Privacy Act[2], which enshrined these principles and more in law. European nations were

equally eager to regulate in the field. A British advisory committee recommended similar guidelines. Sweden, France, and Germany all enacted data protection laws in the 1970s, and all of them contained similar principles. By 1980, the Council of Europe and the Organization for Economic Cooperation and Development (OECD) had both recommended a similar set of guidelines to all developed nations.

The American policy initiative seemed to have sparked a remarkable confluence of laws across the Atlantic. It's the sort of thing that ought to make an internationalist's heart grow warm—the laws of nations gradually growing together as international dialogue produces transnational consensus.

No such luck. What these broadly parallel laws in fact yielded was three decades of bitter transatlantic conflict.

Part of the problem was cultural. Americans, with their suspicion of government, had been quick to apply the privacy principles to government databases but slower to apply them to the private sector. In Europe, where government was more trusted than the private sector, privacy laws were written more broadly to cover all personal data in private hands. To enforce the rules, privacy bureaucracies sprang up across the continent.

But the deeper problem was European unease about the growth of data processing, and the transfer of data across national borders. Labor unions in Europe feared that their jobs would move to the United States, where it was often cheaper to process data during the 1970s and 1980s. One French justice official saw even broader implications saying in 1977 that, "Information is power, and economic information is economic power. Information has an economic value and the ability to store and process certain types of data may well give one country political and technological advantage over other countries. This in turn may lead to a loss of national sovereignty through supranational data flows."[3]

Against this background, the new data-protection laws were a godsend for European policymakers. If U.S. law could somehow be characterized as inadequate to protect European data, then the data

could not be sent to the United States. The data processing jobs would stay in Europe, as would the "political and technological advantage" the French justice official worried about.[4]

In the end, European authorities didn't have much trouble deciding that U.S. laws were inadequate. They focused on the limited nature of U.S. privacy regulations for the private sector. In Europe, to take one example, it was unlawful for companies to sell their customer lists to junk mail companies; in the United States it was not. So if those lists were sent to the United States, European authorities thought, no law would prevent them from being used to send junk mail to Europeans. To prevent such an end run on European law, the authorities declared, the data would have to stay in Europe.

The United States, in turn, saw the ban on exporting data to "inadequate" countries as simply a clever bit of protectionism. In a wide variety of international forums, the United States argued that personal data should be freely transferred among jurisdictions as long as the data-protection regimes were comparable. The debate festered for nearly twenty years.

Then in 1995 the European Commission stopped debating and acted; its new directive on data protection made the export ban official EU policy. No personal data could be transferred, the directive declared, to countries that do not provide an "adequate" level of protection. To be deemed adequate, countries would have to adopt laws that more or less parroted the language of the European directive. Everyone knew that the United States would not simply adopt laws written in some other capital. A confrontation seemed inevitable until, in 1998, the United States and the EU found a compromise. They agreed that, under a "safe harbor" arrangement[5], U.S. companies could promise to follow EU law even while processing data in the United States and that the United States would enforce the companies' promises. In return, Europe agreed to allow "safe harbor" companies to transfer their data freely across the Atlantic.

From a European point of view, this was a great symbolic victory. The EU had branded the United States an inadequate defender

of personal data, and it had used a combination of economic clout and moral suasion—European soft power—to make the charge stick. Europe's "adequacy" requirement was gradually forcing countries and companies around the world to adopt European privacy standards. Perhaps the EU could hear a faint echo of the old days, when statutes written in a European capital automatically became law in many distant lands. That one of those distant lands might be the United States seemed particularly satisfying. The EU liked how the privacy conflict was playing out.

All of the conflict had so far centered on regulation of the private sector. For good reason. The United States had not been slow to apply privacy principles to government. Indeed, its enthusiasm for imposing privacy limits on government exceeded that of the Europeans. And there was no history in Europe of restricting data transfers to countries whose *governments* might misuse it.

But that was about to change.

America marked the first anniversary of the September 11 attacks with candlelight vigils and memorial ceremonies. Near Washington, construction crews raced to finish rebuilding the Pentagon. In New York former Mayor Rudolph Giuliani and a host of other officials joined in reading every victim's name at Ground Zero.

In Europe, meanwhile, the attack on U.S. antiterrorism policy was well underway. A working party of data protection officials was putting the finishing touches on a report that slammed the United States for gathering travel reservation data without "adequate" safeguards. The report acknowledged that "sovereign States do have discretion over the information that they can require from persons wishing to gain entry to their country."[6] But, it went on, U.S. sovereignty could not trump European data-protection standards. The U.S. proposal to collect travel data, the privacy officials declared, was inadequate because the data "could be used for routine purposes related to immigration [and] customs as well as more generally for US national security and may at least be shared amongst all US federal agencies."[7]

The European commission member responsible for the internal market, Frits Bolkestein, was even more blunt: "It is the sovereign right of the United States to determine the conditions under which people may enter its territory. But it is Europe's sovereign right to insist that personal data concerning its citizens enjoy adequate safeguards when transferred to other countries."[8]

At the time, a privacy assault on DHS's travel reservation program seemed like good politics on both sides of the Atlantic. While Congress had authorized access to travel reservations for overseas flights, it had not authorized DHS to review domestic flight data, and support for domestic access was eroding. As we'll see in Chapter 8, the ACLU and other privacy groups had targeted the domestic program for defeat, and they were close to winning. DHS was embroiled in claims that JetBlue and other airlines had violated privacy standards when testing the domestic program. Bolkestein welcomed the flap.

"I may be just about the only person who felt reassured after reading about how JetBlue surrendered passenger records to a firm working for the government," Bolkestein declared, because "I am confident that publicity for cases of this kind and the understandable outrage that they provoke will help to ensure that reasonable counsels in Washington prevail as regards the limits that must be set on the security-enhancing uses of passenger data."[9]

Bolkestein was accurately reading the mood in Washington. Congressional unease about the domestic travel data program grew rapidly in 2003. Sen. Ron Wyden (D-OR) took the lead in raising questions, and by the fall of 2003, he had successfully inserted language into the DHS appropriations bill imposing harsh new restrictions on implementation of any domestic travel data program.

Under siege on the Hill and facing hard lobbying from a financially strapped air industry, DHS had no stomach for a fight with Brussels. It buckled, agreeing to European demands and setting limits on how it would handle travel reservation data. In return the European Commission declared DHS's revamped program "adequate."

The agreement, negotiated during 2003 and early 2004, was meant to put the travel data debate on ice. It didn't. Reservation data was still a point of contention when I arrived almost two years later. Many Europeans politicians felt that they hadn't extracted enough concessions from DHS; they wanted a rematch. At the same time, the more Secretary Chertoff and I studied the deal, the less we liked it.

Chertoff was a former prosecutor. He'd sent a lot of people to jail after trials in which the defendants claimed that the prosecutor and police had violated the defendant's civil liberties and privacy. Every good prosecutor has developed a thick skin for such claims. And I'd been general counsel of the National Security Agency. I, too, had gotten used to separating responsible privacy claims from irresponsible ones.

What's more, both Chertoff and I had personal experience with the wall between law enforcement and intelligence. We were appalled at the idea that foreign governments would reimpose such a catastrophic policy on the United States within a few years of 9/11.

But that's what the agreement did. Pursuing its own notion of what privacy requires, the EU had insisted that that the Customs and Border Protection agency (CBP), and only that agency, would have access to reservation data. The FBI, the CIA, NSA, and the National Counter Terrorism Center, even other parts of DHS—all were on the wrong side of the new European-built wall.

My staff counted nearly a dozen limits that the agreement imposed on sharing of potentially valuable counterterrorism information with these agencies; they made practical interagency use of the data nearly impossible. In addition to this critical objection, there were three or four other practical problems with the deal that we feared could get Americans killed.

Some data was off-limits entirely, for example. European law treats certain kinds of information as "sensitive." This category includes information relating to union membership, race, ethnicity, sex life, and health status. Now, airlines do not ordinarily ask people whether they belong to trade unions, or what their sex life is like. We didn't see much need for a special rule to cover such data, but the European

negotiators had insisted on incorporating a provision from European law that set strict limits on the collection of sensitive information. Actually, they went further than European law, making a special and more restrictive rule that only applied to American authorities, prohibiting any DHS access to "sensitive" data. We didn't mind giving up access to the one routinely gathered bit of "sensitive" data—passengers' meal choices, where a *halal* or kosher meal preference might disclose a passenger's religion. But we were troubled by the absolute ban on collecting sensitive information. A passenger's health status is also considered sensitive information. What if DHS received intelligence that terrorists planned to smuggle explosives onto a plane using a wheelchair or a leg cast? Were we prohibited from finding out which travelers had boarded in casts or wheelchairs?

The agreement also restricted DHS's ability to spot problems early. DHS was prohibited from gathering information more than seventy-two hours prior to a flight; and once it began pulling information, it could do so only four times before the flight took off. This greatly limited DHS's ability to watch for the early stages of a large plot. And it made no sense. How did such an arbitrary rule help privacy?

Finally, the data could be used for only seven days. After that, the information could be stored for limited reviews, but it would all have to be destroyed within three and a half years. These restrictions also made no sense if we wanted to use the data to identify unknown terrorists. Al Qaeda and other terrorist groups had already been in operation for well over twenty years, and some of their plots had taken many years to develop. Since terrorists are less likely to use good tradecraft early in their careers, the destruction requirement could prevent DHS from using their early travel patterns and associates to connect the dots.

I had one more problem with the agreement. I'd spent years in private practice giving data-protection advice to companies, advising them on U.S. and European law, the Safe Harbor, and transfers of personal data across borders. I was already quite familiar with the 1995 directive.

And from everything I knew, the EU's claim that its airlines needed an "adequacy" agreement before they could give us data was claptrap. Diplomatically convenient claptrap, but claptrap all the same.

The airlines had at least five good defenses against liability. For example, the directive allows the processing of data "in the public interest or in the exercise of official authority."[10] This is the provision that allows companies to cooperate when the government asks for information, and there was no footnote in the directive saying that American government requests weren't "official."

The second defense was even better; the directive expressly allows transfers of data even to "inadequate" jurisdictions if "the transfer is necessary for the performance of a contract."[11] That was squarely on point, I thought. An airline ticket is a contract, and the airline could not perform the contract if it didn't comply with U.S. law, including our requirement to deliver reservation data.

A third strong defense was provided by the directive's language allowing transfers of data that are "necessary or legally required on important public interest grounds."[12] DHS's legal requirement was meant to keep terrorists off planes, and that surely qualified as an "important public interest."

That gave rise to the fourth good defense. We figured that keeping terrorists off planes would be good for the other travelers on those planes, and the directive also exempts transfers that are "necessary in order to protect the vital interests" of the person providing the data.[13]

Finally, a fifth defense was independent of all the others. The directive allows transfers of personal data to an "inadequate" jurisdiction when the data concerns someone who "has given his consent unambiguously to the proposed transfer."[14] So if push came to shove, the airlines could simply tell customers that their information was required by the U.S. government and get their consent. Most of them would give it willingly; those who did not could take their vacations elsewhere.

Those were a lot of defenses. And even if they all failed, the worst that could happen to an airline was that it might lose a case and face a fine. Since it could also be fined for not complying with U.S. law, the

airline would be faced with two inconsistent orders from two different governments.

That's not good, but it wasn't necessarily a reason for the United States to back down. The Europeans wouldn't want to put their airlines in that pickle either. Yet somehow DHS had been persuaded to rebuild the wall just to avoid the *possibility* that some day an airline would face such a choice.

It sounded like a bad deal to me.

So even with a bright sun streaming over the national mall and through the windows of the Arlington high-rise, tension began to build as soon we turned to the agreement. We were discussing a provision that was particularly offensive from an American perspective. European emotions had run so high on the privacy issue that European negotiators refused to rely on U.S. promises to implement the agreement. Instead, the agreement required the United States to stand for inspection once a year. A joint review would be conducted each year so that the European Union could satisfy itself that the United States really was doing what it had promised.

The first such review had just occurred in the fall of 2005. The European Commission sent a questionnaire that DHS had to answer. DHS's Privacy Office conducted an independent investigation and issued a 45-page report card on DHS's compliance with the undertakings.[15] DHS then opened its doors to a delegation of European officials insisting that they had to inspect the department's facilities; it spent a long day answering the delegation's pointed questions.

At last, the Europeans had issued their own lengthy report giving DHS that reluctant "B."[16] They complained about how long our compliance took, and they had several suggestions about ambiguities that DHS should clear up and improvements that DHS should adopt. They seemed to be settling in for years of audits, of auditors' reports demanding remedial actions, and of follow-up audits to make sure we carried out the demands. It looked as though the United States would never be off probation.

As Faull rehearsed these complaints, I had finally had enough.

"You know," I broke in, "you shouldn't push your luck. If I'd been here last year, DHS never would have signed that agreement."

The room went silent. This wasn't in the script.

But Faull did not back off. On he went, dwelling on our minor failings and demanding assurances that seemed to go beyond what the agreement required. The longer he talked, the deeper my conviction grew.

This was a bad deal. We needed to get out.

But why spend time on this issue now? I wondered. I don't like the deal, but it's done. It still has years to run. The Europeans should put it in the win column, I thought, and move on.

The Europeans, it turned out, couldn't let it go because they didn't see it as a win. Indeed, the European Commission's negotiator had been reassigned (some said fired) because the European side thought that the final deal was too easy on the United States. The whole arrangement was still under fire in Brussels. It had become tied up in Brussels's institutional politics. Traditionally, the EU has been run by the European Commission, Europe's executive branch. In fact, for years there was no legislative branch at all. The institution was not taken seriously until the late 1990s, when a revolt in Parliament forced the resignation of an entire commission.

Now the European Parliament was flexing its muscles, and the airline reservation conflict was tailor-made for legislative grandstanding. The European Parliament had played no part in the negotiations, so the parliament found it easy to say that the commission could have gotten a better deal. That view was shared by a committee of the European Union's data protection commissioners—the continent's top privacy bureaucrats. They too were sure that the commission could have extracted more concessions from the United States.

Hoping to make good on its complaints, the European Parliament had challenged the agreement in the European Court of Justice. It claimed that DHS's program did not meet the privacy standards set by the European Convention on Human Rights. It also made a

second, more technical, objection: The EU's agreement with the United States was beyond the commission's authority.[17]

The second argument grew from the EU's gradual, and often contested, assertion of ever-greater authority over member states. The European Union was, first and foremost, a customs and economic union. When it built on that "first pillar," it had broad authority to set the terms of private commercial activity across the continent. But if it wanted to set rules affecting diplomacy, national security, or law enforcement its authority rested on a different and weaker pillar; it could only act in these areas with the unanimous consent of the member states. The deal with the United States was about law enforcement, Parliament argued, not economics; the arrangement was built on the wrong pillar and so must be held unlawful.

If the best deals are the ones where everyone ends up unhappy, the negotiators of this one had done a superb job. DHS's leadership abhorred it; we couldn't wait for it to expire.

And most of Brussels held the same view.

Both sides thought they could do better if they tore up the agreement and started again from scratch. If the European Court of Justice ruled against the deal, we were going to get our wish.

We couldn't both be right, of course. One of us had miscalculated. Badly.

6 To the Brink

On May 30, 2006, we got what we had hoped for. And so did the European Parliament.

The European court struck down the agreement.[1] But only on the jurisdictional ground. The European Court of Justice was reluctant to decide just how much human rights law Europe could impose on the United States. Instead of finding U.S. law "inadequate," it ruled that the commission had fatally mixed up the commercial and the criminal enforcement pillars.[2]

The agreement was dead. But the court agreed to keep it on life support a little longer. Europe, after all, didn't want to kill the agreement right away. It wanted a renegotiation. Unless the court granted a grace period, there would be no time for DHS and the commission to put the arrangement on a new and proper basis. Accommodating the European negotiating interest, the court delayed the effective date of its decision for four months. The adequacy finding would expire on September 30.

On that date, if we did not have a new agreement, the "adequacy" determination would come to an end. Airlines flying to the United States would have no special protection from European data-protection law. But they would still have to comply with U.S. law requiring them to submit reservation data on all their passengers.

For the airlines, September 30 marked the beginning of Armageddon. Without a new agreement, they would face conflicting legal obligations. The European Union's data-protection law would require

them to withhold reservation data from the "inadequate" United States. At the same time, U.S. law would require them to hand it over.

If worse came to worst, the airlines that observed U.S. law could be prosecuted criminally and fined by European privacy bureaucrats. And those that refused to comply with U.S. law would be fined by DHS and could lose their landing privileges. Chaos would ensue. Some airlines might cancel flights. Those that flew would fly in fear.

Or so the Europeans thought. Me, not so much. I had confidence in the airlines' defenses to a privacy claim. And I was eager to put my theory to the test.

Oddly, then, the court's decision was welcomed on both sides of the Atlantic. The European Parliament was celebrating, as were European privacy bureaucrats. They had not won a human rights condemnation of the United States, but they were sure that a new negotiation would bring the United States to heel. This time they'd insist on a tougher line. This time they would get the privacy protections they wanted by threatening to throw all transatlantic travel into disarray.

DHS was just as pleased. We, too, thought the old arrangement was unacceptable. And, like the European Parliament and the privacy bureaucrats, we were confident that we could get a better deal the second time around.

Faull called as soon as the court's decision was formally announced.

—I don't think this is a surprise, he began, but I wanted you to hear it from me. The European Court of Justice has invalidated the PNR agreement.

It wasn't a surprise. I was delighted. But this was no time to say so.

—I remember quite well your remarks at the dialogue last year, Faull continued. I understand that you don't like the agreement. And of course we appreciate that the agreement was scheduled to be renewed next year.

What was going on here? I wondered. Jonathan Faull seemed surprisingly muted. He couldn't possibly agree that the deal should be tossed out.

—Under the court's decision, Faull added, we have only four months to find a substitute agreement and to avoid a crisis in transatlantic travel. That is not enough time to complete the careful review and negotiation that I know you'll want.

Ah, I thought, now I see where he's going. Very clever.

—There's an easy way to make this work, he went on. The problem is purely a matter of EU procedure. If the EU approves the agreement under our third pillar procedure, we can solve the problem. So I'd like to get your agreement to simply adopt the same agreement but put it on a different pillar. It will still expire in 2007, and I know you will want to renegotiate it. We will do that, in an orderly way, starting very soon. But we should fix this awkwardness without trying to negotiate with our backs against a four-month deadline. We don't want chaos on September 30.

I took a breath. Faull was being cautious, keeping emotion out of the call. I would do the same. But this proposal was utterly unacceptable. The European court had given us our best chance to remake the agreement, or kill it, and I had no interest in postponing the opportunity.

—Thanks, Jonathan, I said. I understand your thinking. It's like that scene from *Indiana Jones*, where Jones tries to quickly put a bag of sand in place of an idol. Do it fast enough, and perhaps no one will notice the change. But if I remember right, that scene ended with Jones running for his life and a giant boulder rolling after him.

—So I don't want to encourage you to think we'll take the Indiana Jones option. If we don't, though, I promise that we'll do all we can to avoid chaos four months from now.

—I understand, said Faull. Just so you know, I will be seeking a mandate from the European Council authorizing me to negotiate for renewal of the agreement as it now stands. And I hope you will obtain authority to do the same.

—Completely understood, I said, which is what you say in international negotiations when the other side says something you have no intention of agreeing to.

It was an odd conversation, I thought, after we hung up. Faull knew how strongly I felt about the evil the agreement was working;

and he must be under pressure to make progress on the privacy agenda of the European Parliament. Yet there had been no fireworks, no posturing. We had barely sparred.

Why not? The answer was in Faull's mention of his negotiating mandate. The fact was that neither of us had permission to stake out a position. The first task for each of us was to bring our own side into alignment. Only then could we engage each other.

Many negotiations in the private sector skip this step entirely. When negotiating the sale of a house, both the buyer and the seller know what price they want. At the negotiating table, buyer and seller exchange offers; they can decide quickly whether to accept or reject the other's offer. Even in the private sector, however, negotiations may be more complex. If the seller offers to re-shingle the roof rather than reduce the price, the couple buying a house may have to negotiate between themselves before deciding whether to insist on a price reduction or to settle for the new roof.

Government negotiations are closer to the second scenario, except that the buyer has to contend not just with a spouse, but with a mother-in-law, two uncles, and the guy next door who wandered in to borrow a hedge trimmer and has strong views on shingles. Arriving at a single U.S. position for international talks is in itself a major negotiation.

"I always knew when the United States had clear negotiating goals," one British diplomat told a State Department friend of mine in a moment of candor. "Then, they'd just send a negotiator. As soon as they sent an interagency team, I knew they couldn't agree on a final position. The team was there to make sure the lead negotiator didn't go beyond his authority."

Most of the time, he might have added, the United States sent a team.

So did the European Union. The EU has heavily laden processes for getting authority to negotiate anything, particularly with the United States. Any negotiations require a formal mandate from the

ambassadors representing twenty-seven nations, all of whom have their own special interests and relationships with the United States. In the best of times, the commission would have had difficulty bringing all twenty-seven to a single position.

But in this case, there were more than twenty-seven agendas to reconcile. The parliament was clamoring for a greater role—and a tougher line. So were the privacy bureaucrats. And because the next negotiations would be based on third pillar authorities, the Brussels institutions that stand atop the third pillar would expect primacy. Those institutions—the European Council and the European presidency (held by a different nation every six months)—have little role in commercial negotiations but would expect a large one now.

As he tried to find consensus, Faull's advantage, a powerful one in any government debate, was inertia. That was his best argument for the quick deal he'd proposed—simply taking the old agreement and putting it on a new jurisdictional pillar. Restoring the status quo would disappoint the parliament and the data-protection bureaucracy, which hoped to squeeze more concessions out of the United States. But they didn't understand the risk they were running, Faull must have thought. Reopening the agreement meant reopening everything, not just the issues the parliament wanted to raise. That, he knew, would play into DHS's hands.

My remarks the year before had made clear that a complete renegotiation was precisely what we wanted. Al Qaeda was looking for radicalized Western Europeans who needed no visas across the Atlantic to attack the United States; passenger name records and advance passenger information were the earliest line of defense that DHS had against these travelers. Why should DHS agree to destroy that data quickly, or to look at it in a tiny window that opened only seventy-two hours before the flight? Why should it put information out of bounds that might reveal plots involving leg casts or wheelchairs or false pregnancies? Why should we let privacy advocates or European negotiators determine in advance what information was useful to DHS and what was not?

I knew where DHS stood. The agreement would have to be rethought and renegotiated from the ground up. All that remained was to get the uncles and cousins and mothers-in-law that made up the interagency process to agree.

That would be my toughest challenge. The costs of the PNR agreement (in time, money and limitations) fell entirely on DHS. They didn't inconvenience any other agency. But the cost of reopening the deal would certainly be felt by other agencies. The State Department had an interest in smooth relations with Europe. It didn't need another dispute if it could avoid one.

DHS had allies, of a sort. Defense and the intelligence community wanted a more effective border defense system, and better information about travelers. They too believed in information sharing. But like the other agencies, they had little stake in particular DHS programs.

As I sketched the roster of supporters and adversaries that I'd face in the interagency debates, the Justice Department was the wild card. It should have been with us. After all, during the first passenger name record negotiations under Tom Ridge, the Justice Department had fought to keep DHS from making concessions on things like information sharing. Justice had been right, I thought, and our entire negotiating strategy would be aimed at taking back that concession. What's more, the Brussels approach was a threat to Justice too. The EU was using the privacy issue as a wedge to create new tensions in the law-enforcement relationship between the United States and Europe. Instead of relying on exchanges with the United States, Brussels wanted to build its own European institutions, such as Europol and Eurojust. So it was strengthening law enforcement exchanges within Europe at the same time that it was raising barriers to sharing of information across the Atlantic.

As I saw it, Justice and the FBI were in the same boat as DHS. The European approach—using the data-protection issue to slowly throttle investigative information exchanges with the United States—was irresponsible. It was going to get Americans—and Europeans—killed. Justice and the FBI should be as eager as DHS to confront

Brussels and back the EU away from this tactic. Wasn't that why Justice had tried to keep DHS from agreeing to the PNR arrangement in the first place?

Now that I was ready to admit that Justice had been right all along, I hoped the two agencies could make common cause to undo the worst aspects of the PNR arrangement.

It was not to be. Justice was still smarting from what it had lost when DHS was created. Until DHS came along, the uncontested representative of U.S. law enforcement abroad had always been the Department of Justice. The FBI was the biggest single federal law-enforcement agency. There might be more law enforcement officials elsewhere in the federal government, but they were specialized and dispersed. Now, though, DHS had pulled most of those law enforcers into one department. DHS's border and investigative duties matched well the responsibilities of interior ministers in other countries. They saw DHS as a natural partner. None of that was good for Justice. And Justice's pique at having to share the table with a second law-enforcement agency was making it hard for us to work together.

I thought that in the end Justice would be foolish not to stand with us. This wasn't just a renewal of the old deal. It would be the first explicit law-enforcement arrangement to set these kinds of data restrictions. For the first time, we'd be taking rules that were written for Safeway and Allstate and agreeing that they could apply to the FBI and Customs and Border Patrol. Once that happened, there'd be more and more demands from Europe to expand the principle—to make us run our criminal and antiterrorism investigations in accord with European standards and sensibilities.

My first job was to come up with a negotiating position—and a strategy—and then to sell it to the rest of the government. The negotiating position fell naturally from the many problems I'd found in my first review of the deal—the wall; the strict ten-day limit on using the data; an annual review that felt like an annual renegotiation; and an arbitrary and dangerous ban on ever using "sensitive data." Our

position, I thought, was simple: any new deal would have to cure all of these problems before it would be acceptable. To this list, I added another negotiating goal. I thought any new agreement would need a much tougher reciprocity clause.

At bottom a reciprocity clause means that the rules are the same for both sides of an agreement. I did not believe that European data protection law really demanded as much from law-enforcement agencies as the Europeans had claimed. There had never been a European investigation finding fault with Russian or Chinese or Syrian investigative agencies' use of information obtained from European companies. Was that because their law enforcement agencies had a better privacy record than U.S. agencies? Indeed, there had been practically no efforts to set data-protection standards for *European* law-enforcement agencies.

I suspected that the harsh rules in the 2004 arrangement had been made up by Europeans especially for Americans—that they wouldn't dream of applying the same rules to their own police agencies. But that suspicion undercut the whole rationale of the agreement, which was supposedly to force the United States to live up to high European standards for handling European data. If European privacy standards weren't as high as claimed, we should be able to reduce our own to match the European reality. A tough reciprocity requirement would provide long-term strategic flexibility for DHS; at any time, we could modify our undertakings if it turned out that Europe wasn't following the same rules.

This was an ambitious negotiating agenda, particularly since the Europeans were hoping to get new concessions—not to give them. To overcome their resistance, we needed a strategy. The strategy I came up with was simple but risky: Either the agreement would be completely overhauled or we would let it expire on September 30. I knew the pressure that the European Commission was under to get a better deal than in 2004. We could only combat that pressure if the United States was willing to let the agreement fail entirely.

The last time a deal on travel data had been negotiated, the risk of chaos in the skies over the Atlantic had been used to bludgeon DHS

into a quick settlement. This time around, buoyed by my own sense that the threat of chaos was overwrought, I was willing to let the September 30 deadline pass without an agreement.

If we went to the brink, I believed, the Europeans would cave. And if we went beyond, well, we'd find out who was right—the European prophets of doom or the DHS leaders who thought the threat was mostly manufactured.

To take that stance, the United States had to be willing to live with the consequences—expiration of the September 30 deadline without an agreement that protected the airlines. But were we?

I needed to persuade the rest of the government that the airlines didn't need an adequacy determination to avoid privacy sanctions in Europe.

I was sure they didn't. I knew that the 1995 directive offered many defenses for the airlines—data sharing is permitted for public safety or law enforcement, for protection of the interests of the passengers who provide the information, and for compliance with the laws that govern air travel. And, even without those defenses, airlines could fully insulate themselves from liability by obtaining the consent of their passengers for the data transfer to the United States.

The strategy didn't rely entirely on law. It was also grounded in *realpolitik*. The European Commission sets data-protection rules, but it does not enforce them. So if any airline were going to be fined for complying with U.S. law and providing travel data, the decision would have to be made by the country where it operated. Each country would have to decide whether to punish local airlines flying out of local airports. And any country that threatened to punish local carriers for following U.S. law would put those carriers at risk of DHS penalties—fines, delays and the loss of their rights to fly to the United States.

European solidarity went only so far, I thought. If French privacy bureaucrats made it impossible to fly to the United States from Charles de Gaulle airport, well, Schiphol, Heathrow, and Frankfurt would be only too happy to pick up the slack. When September 30 came around and no deal was done, who would want to be the first country to punish its airlines and its airports?

Europe, I figured, was bluffing.

If I was right, it would be no big deal to let the agreement expire. We should be happy to see the entire arrangement die, and the risk that it would hurt the airlines was small. So why not dramatize our confidence? We could take a tough line in the talks, insisting that the undertakings be completely overhauled and all their problems cured. At the same time, we should begin visibly and noisily planning for the end of the arrangement on September 30.

At the National Security Council (NSC), we ran into a buzz saw. The State Department had no interest in another confrontation with Europe—especially not at a time when U.S.-Europe relations were tender from the rancor over Iraq. DHS had signed this agreement two years earlier, State said, and if DHS was willing to live with it then DHS should be willing to live with it now. The Justice Department, which had counseled DHS not to negotiate a passenger names records agreement in 2004, now wanted to leave the agreement in place. DOJ insisted that DHS must renew it without change. It blamed DHS and the passenger names flap for increasing European restrictions on law enforcement data sharing. We should do nothing that might increase transatlantic tension over law enforcement.

Even more troubling, the National Security Council staff made no effort to disguise its determination to keep DHS from pursuing a hard-nosed strategy. The NSC was supposed to be an honest broker, shaping and narrowing disputes among cabinet departments so that only the most difficult and heartfelt conflicts got to the president for decision. But the NSC knew little about DHS, and what little it knew it didn't much like. The Homeland Security Council, created after 9/11, was viewed by many in NSC as an unnecessary subtraction from NSC's authority; and DHS in its infancy was thought incapable of handling hard diplomatic tasks.

NSC had many irons in the fire with Europe. Letting DHS blow up the existing agreement to get better terms sounded risky to the NSC staff. They doubted that DHS was up to the job. Better not let

the new guys rock the boat. This attitude showed up in every NSC memorandum, every summary of conclusions from NSC meetings, and even in the invitation list. DHS had to fight just to get NSC to invite Defense and the intelligence community when the NSC met to discuss travel reservation data.

DHS stood alone. But we were determined not to reinstate the old agreement. Secretary Chertoff and I simply would not accept a made-in-Europe version of the wall. The interagency participants and the NSC staff bitterly opposed the DHS strategy, but DHS had two advantages.

First, DHS was the agency whose interests were truly at stake. The others had strong passing interests in the dispute, but only DHS had direct operational responsibility for keeping terrorists out of the country. If DHS believed that a better PNR agreement was necessary to accomplish that end, it was very hard for other agencies to persuasively argue for a different view.

Second, the lines of communication from the bottom of DHS to the top were clear, short and quick. When new issues arose, Chertoff could be briefed and give decisions in hours. This was critical to the interagency debate, because many of the other participants might take weeks to get cabinet-level backup for their positions. Time and again, DHS officials were able to scotch opposition at the NSC by saying, "We've talked to our secretary. That's his view. If you disagree, you'd better bring your secretary to the table to close the deal."

But NSC and the rest of the interagency group had weapons of their own, most especially the power of delay. NSC could refuse to approve DHS's most ambitious and hard-nosed proposals. In a bureaucracy, the power to delay a proposal is often the power to kill it. The agencies that wanted DHS to quietly renew the PNR arrangement might not be able to force us to agree, but they could achieve the same end simply by delaying any decision that would allow us to negotiate an alternative.

So, in the weeks following the decision of the European Court of Justice, an eerie quiet settled over the Atlantic. Both sides were trying

to agree on how they would approach the negotiations. The commission was seeking a mandate simply to renew the old agreement. This took time, but the commission seemed confident that time was on its side. The closer we got to September 30, the commission seemed to think, the greater the pressure on DHS to accept a simple renewal.

At the same time, DHS was pressing for authority from the National Security Council to put forward an ambitious rewrite of the PNR arrangement. DHS also wanted authority to go directly to individual member states to begin planning for the expiration of the September 30 deadline. Reluctant to approve these tough tactics, the NSC was slow-rolling the DHS request. It had made the same calculation as the commission, and it seemed to want the same thing. The closer we got to the deadline, the more likely it would be that DHS would have to roll over the existing deal.

I could see the opposition strategies starting to unfold—both in Brussels and inside the interagency process. Both of our adversaries were playing a delaying game. They thought that the approach of the September 30 deadline would force DHS to make concessions. They thought that the deadline helped them, because they couldn't imagine letting the agreement actually expire. They were sure we'd have to get more flexible as September 30 neared.

But the strategy I'd devised for DHS saw the deadline as DHS's friend. I thought that the best thing that could happen to us was for September 30 to come and go. That would expose the Europeans' bluff.

And in the interagency process, DHS's unity would allow it to stand firm as September 30 approached. I was gambling that the September 30 deadline would turn out to be a bigger problem for the Europeans and the interagency players than for DHS. So the key for now was to keep them thinking that delay was their idea, not ours.

With everyone playing for time, June passed without action. Faull told everyone that he was seeking a mandate to renew the agreement without change. Before the EU enters into formal international

negotiations, the twenty-seven member states authorize those negotiations and set out the EU's objectives in a negotiating "mandate." This process means that the EU's negotiators are often kept on a very short leash—unable to make concessions or deals that materially vary from the mandate they have been given. The story was often told (I suspect it is apocryphal, though indicative of a larger truth) that an agricultural negotiator had to return to the European Council for a new mandate in order to remove a comma from a trade agreement.

Finally, in July, Brussels reached consensus, giving Faull the mandate he had sought. It was the *Indiana Jones* option—renewal of the old agreement on a new jurisdictional foundation. Faull called to let me know, and to tell me that, as a technical matter, it would be necessary for the United States and the EU to "denounce" the old agreement, since it had been overturned by the court. He wanted to make sure we weren't upset when that request was sent over.

I wasn't upset. I was overjoyed.

I agreed with enthusiasm to join Brussels in denouncing the old agreement. But I made no formal proposal for replacing it. That would have required interagency consensus, and consensus was slow in coming. Instead, I waited for the European Commission to put forward a draft. Once we saw the European draft, I would have to persuade a reluctant National Security Council to authorize DHS's proposal for a complete rewrite. That would be a hard slog, and I was in no hurry to start.

Brussels finally put forward its draft in mid-July. Had it really served up the *Indiana Jones* option, simply repeating the old agreement without change, my strategy might have been in trouble. There was plenty of interagency support for Faull's proposal that we simply renew the 2004 arrangement. But in the end, Brussels had not been able to achieve consensus on a straight renewal. Instead, perhaps driven by its privacy bureaucrats, it put on the table a draft that went well beyond the 2004 agreement. The new draft tried to turn all the U.S. undertakings into a formal and binding international agreement, rather than a loose *quid pro quo*. Worse, it allowed the privacy

bureaucrats of the member states authority to investigate DHS and to take enforcement action if they concluded that DHS was not living up to those obligations.

Brussels had overplayed its hand. No one in the interagency process was willing to argue that DHS should accept a worse deal than it got in 2004. The Brussels draft was not a basis for serious discussion. I had unanimous support for rejecting it out of hand. And in that moment, Brussels lost its best chance to force renewal of the 2004 deal.

It was now late July. Two months were gone from the four-month negotiating window that the European Court of Justice had allotted. And August vacation is nearly sacred in Europe. No serious negotiations could be expected then. Pointing out that combining August in Europe with the Labor Day holiday in the United States would leave only three weeks for substantive negotiations, DHS insisted that planning for a possible September 30 crisis should begin.

It was only prudent to do some quiet contingency planning, we told the interagency, and it agreed that we could approach individual member states and ask them what plans they had for avoiding a crisis on October 1.

This, too, fit our strategy. It allowed DHS to bypass Brussels and begin dealing with individual European countries. No matter how quiet the conversations, we knew they would get back to Brussels almost immediately. And that would make the Europeans realize that DHS might not be bluffing, that expiration of the deadline raised no undue fears in Washington. Best of all, we soon learned that several governments were indeed planning steps to avoid lawsuits or disruption of flights if the agreement expired on September 30.

This discovery bolstered DHS's interagency argument that chaos was unlikely on September 30, even if no agreement was reached. The airlines and the member states, I argued, were already working on ways to defuse the crisis and forestall chaos.

In August, the real world broke in. British authorities uncovered a plot to kill innocent transatlantic passengers on a nearly unprecedented

scale. British Muslims with ties to al Qaeda planned to smuggle liquid explosives disguised as sports drinks onto as many as ten transatlantic flights. The idea was to blow all of them up the same day. Thousands would have died.

Thanks to British surveillance, the authorities knew that preparations for an attack were well along. They bugged the plotters' apartments and listened, appalled, as some of the men videotaped their final testaments. Unsure exactly when the plan would go into effect, on August 10, 2006, the British moved in, arresting twenty-five people. At the same time, UK and U.S. authorities imposed restrictions on liquids in carry-on baggage.

The incident, which could have caused a death toll that rivaled 9/11, deepened DHS's determination to reshape the 2004 arrangement. If the liquids plot were a test, the 2004 procedures had failed it. We tried to use the plotters' reservation data to track their plans, but only one part of DHS—Customs and Border Protection—had access to that information, and it was hard to share the data with other agencies. Worse, when we turned to the plotters' reservation data to get advance warning of the attack, we ran into the provision that made it hard to get information about travel reservations more than seventy-two hours before the flight. At a time when we needed as much advance warning as possible about the plot, we were instead struggling with an arbitrary EU limit on how quickly we could get reservation data. That made no sense.

Even the liquids plot did not disturb the rhythm of the negotiations, or the vacation schedule in Brussels. Soon August, too, had slipped away, and still no negotiations had been held. September 30 loomed.

DHS and the European Commission still believed that time was on their side. Not so the interagency. The National Security Council was getting visibly anxious. The first negotiations were scheduled for early September, and the United States had to have a position.

DHS was unwilling to consider the *Indiana Jones* option—the same deal on a new footing. We wanted a complete revamping of the

2004 arrangement. Other agencies feared that such a demand would put an end to the talks. But DHS's firmness was beginning to bring the others around. They had no answer to our objection that the 2004 deal was too constraining, particularly after the August plot. They agreed that some renegotiation was needed but they took refuge in delay and procedural objections. Why not wait until the old deal expired by its terms, in 2007? There wasn't time, they said, for a wholesale renegotiation. Couldn't we keep the old deal for a few more months?

I wouldn't budge. I knew that rolling over the deal would give it greater power. It would be even harder to kill after it had been signed twice. And besides, the deadline would work in DHS's favor, I still believed. Why give that up?

DHS was constrained by interagency consensus in the formal negotiations, but it could not prevent Michael Chertoff from speaking his mind in public. In a late August *Washington Post* op-ed, Secretary Chertoff made the case for revision of the agreement in blunt terms, saying that European privacy concerns had limited the ability of counterterrorism officials to do their jobs.[3]

The op-ed made my job as negotiator easier. The NSC could hardly order me not to say in the negotiations what Chertoff had already said in the newspapers. It agreed that I could spend the first negotiating sessions explaining our objections to the 2004 deal and proposing that the deal be reworked. But I could not say that the deal would end on September 30.

There was no consensus in Washington for letting the deal die then. If I couldn't persuade the Europeans to rewrite the agreement by that date, most of the interagency members hoped they could force DHS to roll over the old deal, at least for a while and perhaps for another year.

At last even Labor Day had passed. Everyone was back at work, and we had to meet the Europeans. The interagency remained divided. Even so, I was determined not to compromise DHS's goals. As the lead negotiator, I was determined to make the best of my limited instructions.

With Faull sitting across the table, I blasted the 2004 arrangements. That agreement, I said, was "unacceptable to DHS," a formulation that left open the possibility that other agencies might find it acceptable. I insisted that it would have to be renegotiated, and I laid out the many objections that DHS had identified.

Faull was a formidable negotiator, but he had been given an impossible mandate. He was supposed to get us not only to restore the old agreement, but to accept the privacy bureaucrats' proposals, which would make the deal even harder on DHS. He must have known that he'd never get a deal on those terms. So he acknowledged that DHS's concerns were worth discussing, and he promised to do so. But not now.

We don't have time to negotiate a new agreement in three weeks, he declared, and I don't have a mandate to do anything other than renew this deal.

Hoping to break DHS's resistance at the start, Faull had gone straight to the issue that divided Washington. It was almost as if he were reading our interagency memos—or getting briefed by the U.S. agencies that opposed us.

If we are going to have productive talks, one thing must be understood, Faull told me. The only way to handle these talks is to proceed on the understanding that, while we are discussing the issues that DHS has raised, it must be common ground that we are going to roll over the 2004 agreement on September 30. That is the only basis on which I have a mandate to talk to you. If that's not understood, I might as well pack up and go home.

It was an ultimatum.

Whether we were going to take the *Indiana Jones* option was the crucial issue, and Faull wanted to force a concession right away. The EU's slow pace in scheduling talks now made sense; the Europeans thought that leaving only a few weeks for agreement would force us to postpone substantive negotiations and take the rollover.

Faull was smart enough simply to make his statement and move on. He wasn't asking for explicit assent from the United States, he was

putting the EU position on the table. But this would be his position from now on. If the talks went on after his ultimatum, it would be the basis for all further discussion.

For me, the ultimatum posed a tricky problem. I knew that DHS was united in rejecting the 2004 deal and in wanting an immediate revision. Indeed, DHS was willing to let the old agreement expire without renewal, since we thought that the risk of crisis was low. But there was no interagency consensus for the DHS position. The State Department, the Justice Department, and the NSC—all agreed with Faull; they too wanted us to take a rollover. I had no authority to insist that the deal expire without renewal.

But Faull had overreached without realizing it. By stating the understanding so explicitly, he created an opportunity that I would not have had on my own. I had no mandate to threaten the collapse of the deal on September 30, but I certainly could reject Faull's explicit ultimatum.

I waited. After more back and forth, Faull again declared that talks could only go forward on the assumption that the agreement would be renewed by September 30. Choosing my words carefully, I interrupted.

"I'm afraid that these talks can't go forward on the basis you've stated," I said. "I simply cannot promise you that we will renew this agreement at all."

In the dead silence that followed, I wondered whether I had gone too far.

No, I thought, that was a technically accurate statement of the interagency debate. As long as DHS held firm, no one could promise that the agreement would be renewed. Of course, no one could promise that it wouldn't. The issue was still being debated inside the U.S. government.

But in the negotiations with the Europeans, this formulation suddenly put the shoe on the other foot. By categorically rejecting Faull's assertion that the talks could only go forward with a rollover as the goal, we left Faull with the same harsh choice he had tried to force

on us. He either had to abandon his earlier ultimatum or walk away from the talks.

Faull called a break.

He had to consult with his delegation. Faull could not have been surprised at my position; he'd heard much the same informally before. But the other European representatives were shocked. Viewed from Brussels, the 2004 deal looked like a capitulation to the United States. Its privacy protections were far too weak, the Europeans thought; the deal had been criticized by the European Parliament, the press, and the privacy bureaucrats—by all right-thinking people, really.

The European negotiators had begun the session expecting to win a new and tougher deal. Now the United States seemed willing to let the deal die entirely—and in just three weeks. Worse, they now had to decide, over a coffee break, whether to fly home empty-handed or to start discussing ways to weaken an agreement their constituents had already spent years condemning as too weak.

The break stretched on and on. Finally Faull and his delegation returned. They would keep talking. Brussels had abandoned its ultimatum.

A new note of urgency suddenly filled the room. If we were truly going to rework the 2004 agreement in three weeks, we would have to begin immediately. Perhaps for the first time, the European negotiators understood just how much was at stake for them in these talks.

To soften us up, the Europeans realized, they had to restore our fear of the September 30 deadline. If the United States really was willing to let the deal die on September 30, then Europe had no leverage.

Faull began to stress the risks for both sides if there was no agreement on September 30. Just a threat of data-protection litigation could cause chaos if no agreement had been reached, he said. Airlines might withhold data from DHS. They might refuse to fly across the Atlantic at all. Hoping to add to this leverage, one or two of the European negotiators hinted that they might open a new front. They noted that Canada could not share PNR

data with the United States unless the United States was deemed "adequate" under EU law, a status that would expire on September 30. Did we want to lose access to Canadian data as well, the most anti-American members of the delegation asked.

The tactic was Europe's best hope, but it didn't change the dynamic of the talks. I explained that the airlines should be able to avoid liability and I expressed doubt that Canada would take actions counter to its own interest. I deeply resented the European effort to hold Canadian data-sharing hostage, but as a practical matter the data supplied by Canada was so hobbled by restrictions that it had only limited value. I was willing to roll the dice if those were the only stakes.

The tide of the talks had turned. From now on, the negotiations would be focused not on how the agreement could be made more favorable to European privacy campaigners but on how to address DHS's security concerns. The only question was how much ground Brussels would give up.

Faull declared that he found some of the U.S. concerns to be reasonable, but that he did not have any authority to renegotiate the 2004 deal. I can't possibly get a new mandate in the next few weeks, he explained. He added that he thought some of our concerns were based on too strict an interpretation of the 2004 arrangement.

—You're reading it so strictly that it is hurting your security more than necessary, he said.

It is not usually good negotiating tactics to emphasize your weakness and inability to cut a deal. But in choosing this formulation, Faull seemed also to be hinting at a solution. Could we leave the agreement from 2004 in place while reinterpreting it to avoid the consequences to which DHS objected? We could see that this fallback position had appeal from the European point of view. It would keep the commission within its mandate, if barely. And "interpreting" the 2004 agreement set natural limits on the concessions that Brussels could be asked to make. Interpretation might allow

the negotiations to stretch the terms of the agreement; it would not allow the negotiators to rewrite them.

Perhaps to Faull's surprise, I was also willing to explore the idea. That was because I believed the 2004 agreement could in fact be rewritten under the guise of interpretation. The arrangement included a clause that allowed DHS to adapt to changes in U.S. law. If amendments to U.S. law affected any of DHS's undertakings, then the amendments would trump DHS's promises, as long as DHS gave notice to Brussels. I thought that this clause might open the door to major changes, as long as I could tie the revisions to a change in U.S. law enacted after the 2004 agreement.

And there had been such a change. A bill implementing the recommendations of the 9/11 Commission had been signed into law in December of 2004, less than six months after the agreement. The legislation wasn't very specific. It didn't address travel reservation data; but it had the usual post-9/11 provisions requiring more information sharing. The act created a federal "information sharing environment" to facilitate the exchange of all terrorism information among federal, state, and local agencies. Because this measure was intended to respond to the 9/11 Commission's criticism of the "wall," we thought, it could be the basis for undoing the new wall constructed by the 2004 agreement for sharing of travel data.

In fact, read broadly, it could be the basis for repudiating large swaths of the 2004 agreement that affected information sharing. That, plus a generous view of what constituted "interpretation," meant that I could squeeze most of the changes that DHS wanted into Faull's formula, allowing him to stay at least technically within his current mandate. The 2004 agreement could be rolled over, in accordance with the commission's instructions, but with a sweeping set of changes based on the new U.S. law.

I was happy with the first negotiating session. It had forced the talks onto our terrain; I had been able to pooh-pooh the September 30 "deadline" without misrepresenting the state of interagency deliberations; and the way had been paved for a potential compromise—the

interpretive letter. I couldn't have planned on any of that, but our hard fights in the interagency process had left me prepared to pursue each of these opportunities when they arose.

But we had no victories yet. Time was short, and the Europeans had not agreed to any concessions. They couldn't. I had not actually asked for any. Indeed, we had no authority to put forward a proposal of our own. The interagency was still deadlocked. With only three weeks left, though, it was time to force the issue. Faull and I agreed to meet again in a week—at which time I would offer U.S. proposals for an interpretive letter and for what would be done on September 30 if agreement had not been reached.

Now came the hard part. We would have to fight off the other federal agencies that still wanted DHS simply to renew the 2004 agreement despite its troubling privacy restrictions. But DHS's interagency position was improving. First, DHS's judgment had been vindicated. We had successfully called Brussels's bluff. Its negotiators had stayed at the table after DHS refused to treat a rollover as the only possible outcome. The agencies that predicted a breakdown in the talks if DHS took a tough line had been proven wrong. And their efforts to minimize DHS's objections to the 2004 deal had been undercut when Faull acknowledged that our concerns had weight. Interagency debate was now moving to a battleground that favored DHS.

But compromise is the soul of interagency discussion. The process is designed to force agencies to make more and more compromises as disputes move up the ladder from assistant to deputy to secretary. If we walked into the interagency process and put our bottom line on the table, we'd soon find that we had in fact put it on the block, that serious security measures would be knocked down just to satisfy demands for compromise from State, Justice, and the NSC. To keep that from happening, we decided to ask again for what we really wanted—either the 2004 agreement should be rewritten from scratch or it should be scrapped. DHS put forward a rewritten draft of the agreement, reducing the whole thing to broad principles; the resulting

document emphasized that passengers could consent to U.S. security measures, and it dropped the strict regulation of DHS's data practices.

Interagency opposition to this proposal was heavy, and—oddly—it was led by the Justice Department. We thought that Justice would want privacy limits on law enforcement to be carefully circumscribed and reciprocal. As it turned out, Justice did feel that way about privacy limits on its own law-enforcement practices, but it saw no reason to apply the same principle where DHS's practices were concerned. As the interagency debate raged, Justice replayed earlier arguments: The EU would walk away if we put forward our proposal, and a failure of the talks would spoil the atmosphere for what Justice thought of as "real" law-enforcement data exchange—the trading of information in criminal investigations. To avoid even the possibility of a chill in that area, Justice wanted us to stop defending our own interests.

Our proposal had forced the interagency debate to focus on whether to put forward a complete rewrite of the 2004 agreement. For DHS, this was good news. We recognized that a sweeping reconsideration of the passenger names records arrangement would be hard to achieve. But our interagency opponents were concentrating all their fire on that part of our agenda. And that had the effect of making the rest of DHS's position less controversial.

There were two other pieces to DHS's interagency proposal. The first was an "interpretation" letter that would largely tear down the EU-imposed data-sharing wall and interpret away DHS's other problems with the agreement. It was a sweeping document that we believed could solve nearly all of our immediate concerns about the 2004 deal. Of course it went well beyond what most lawyers would call interpretation; parts of it were in truth a revocation of the original arrangement. But if the EU was willing to accept those provisions and to call them interpretations rather than amendments, why should we disagree? Calling them interpretations would give Europe a victory on paper while giving DHS a victory on substance. And if the alternative was giving up the 2004 agreement entirely, I thought, a paper victory

might look good to Brussels. It was aggressive, but I thought it might look good to the interagency when compared to DHS's other, more sweeping proposals.

Our final proposal was certainly harder for the interagency to swallow. I wanted to put complete abandonment of the 2004 agreement on the table. That was the best response to the European claim that there wasn't enough time to revise the entire agreement in just two weeks. There might not be time to rewrite it, but there was plenty of time to kill it. So we asked for authority to propose a joint statement that the parties could issue if we didn't reach agreement by September 30. I liked this proposal because it dressed up a hard-nosed negotiating position as simple prudence. There were only two weeks left, after all, so it only made sense to plan for the possibility that the talks would fail. But the very fact of planning for failure emphasized again how unconcerned we were about the September 30 deadline.

As drafted by DHS, the joint statement was uncompromising. DHS proposed to say that the two sides had not reached agreement but they were committed to keep talking and the EU would not take any action that would harm airlines or the flow of data during this period. Conspicuously, DHS did not commit to keep its undertakings in effect. We would make no promises about what we'd do come September 30. After much discussion, however, NSC brokered a compromise. DHS agreed to promise that it would give Europeans all of the privacy rights that Americans had under U.S. law—other than the right to sue the U.S. government (a right the executive branch could not confer in any event). We were happy to make this promise, first because we had already begun to apply U.S. law to all passenger name records and second because the formulation dramatized our view that U.S. privacy law was already at least as good as EU law and that the two should be treated as equivalent.

That was a small price to pay for approval of the rest of the document, which would dramatize how lightly we took September 30. Putting it forward would show for the first time that the U.S. government was united in that stance. Important as it was, approval of the

document came surprisingly easy. With the other agencies focusing all their fire on DHS's completely rewritten version of the 2004 agreement, I finally agreed to drop that proposal in favor of the "interpretive" letter and the joint statement.

But at the last minute the interpretation letter ran into a completely new set of Justice Department objections. Justice did not want to say that the 9/11 implementation law required the sharing of airline reservation data within the U.S. government. It argued that the new law was more or less meaningless, imposing no serious sharing obligations on U.S. agencies.

Since the interpretation letter was widely viewed as the best way to reach agreement and avoid a blow-up, Justice seemed to have switched sides. After insisting for months on compromise at any cost, now Justice was holding up the best hope for achieving a compromise.

Finally, after long discussions, we figured out what the problem was. The FBI apparently had many agreements with foreign agencies that required it to keep the data to itself and not share it with other U.S. agencies. Such clauses are disconcertingly common in international agreements—especially if the agreements are not reviewed by other agencies. The clauses are common because both sides are happy to adopt them. The foreign agency providing the data wants to know that its distribution will be limited; and the receiving agency (often the FBI) is happy to be given a legal monopoly on important data.

If the United States declared that the 9/11 implementation law required reconsideration of such restrictions, we realized, the FBI and Justice might have to reconsider their own restrictions on sharing data with other agencies. And Justice did not want to do that. These were the same prosecutors who had fought like tigers to tear down the wall that restricted their access to intelligence agencies' information; but now, with the shoe on the other foot, they were fighting almost as hard to keep other agencies from seeing the data they were getting from foreign partners.

I was disgusted. After suggesting that DHS should sacrifice its interests almost without limit just to keep the negotiations from

blowing up, now Justice was prepared to put the entire deal at risk, and in the worst possible cause—preserving the FBI's authority to keep terrorism data behind walls. The irony ran deep. DHS was fighting tooth and nail to win the right to share terrorism data with Justice, to break down the wall; and Justice was fighting just as hard to keep us from succeeding—for fear that it might then have to share more data with us.

It was the worst sort of bureaucratic politics, but Justice was determined. It played its trump card, saying, "We're the Justice Department. We're in charge of interpreting the laws of the United States, and we reject your interpretation of the 9/11 law." It looked as though the entire strategy would founder on the rock of Justice's self-interest.

But for once NSC took DHS's side. It badly wanted a compromise with Europe, and the interpretation letter was its best hope. NSC pressed for a solution. Finally, in a series of tense weekend phone calls, DHS proposed one. Instead of saying that the 2004 agreement's limits on information sharing were "inconsistent" with the statute, could we say that the limits, if read restrictively, would "impede" operation of the statute? The 2004 deal allowed us to modify our obligations if the obligations "impeded" compliance with U.S. law. I felt ashamed of this compromise, because it would give Justice and the FBI an excuse to keep their own barriers to information sharing in place. But it broke the deadlock over the letter. We had what we needed for the next negotiating session—a unified U.S. negotiating position on the substance of the deal, even if we still hadn't quite agreed on what would happen if we had no agreement on September 30.

That was looking more and more likely. The interagency squabbling had eaten up a lot of time. Now there was just a week left before September 30.

But the collapse of interagency resistance left the EU with no options. It was quite clear now that the United States was determined to rewrite the 2004 deal. And, it looked willing as well to let the old deal expire without regret.

With just days to go before September 30, the Europeans dropped their effort to postpone negotiations until the next year. But old assumptions die hard. The EU negotiators still seemed to believe that it was the United States that needed a deal or a rollover by September 30, and they seemed surprisingly unhurried as the days ticked away.

This was fine with me. My biggest worry all along was that the NSC would intervene at the last moment to force DHS to keep the 2004 deal in place if we missed the deadline. But the closer we got to the deadline without NSC forcing the issue, the less likely that became. I was sure that inertia and delay were on DHS's side. If we did nothing, and NSC did nothing, the deadline would pass. If I was right, that event would prove that the deadline was no big deal, and DHS's leverage would increase. If I was wrong, well, all hell would break loose.

I was starting to get a feel for just how bad it could be. Industry had been following the talks through intermediaries, but it had assumed, along with the EU and much of the interagency, that a rollover was inevitable and that DHS would have to cave in eventually. So the airlines had not pressed the two sides to reach substantive agreement. But when the U.S. proposed a joint statement to be issued if no agreement was reached, everyone suddenly realized that failure really was an option. The "adequacy" determination that the industry was relying on might simply evaporate on October 1 with nothing to take its place. The airlines would be flying naked. They didn't want that. They began pressuring DHS to accept a deal, any deal. But they were too late. Our course was set. The slow-moving interagency process had labored and brought forth the two documents. They could not be changed now; they would have to be the basis of further negotiations.

Talks proceeded all through the last week, as Saturday, September 30 loomed. The interpretive letter was proving to be the key to a deal. As I hoped, it allowed EU negotiators to stay technically within their mandate to renew the 2004 agreement while giving DHS time to argue for all the substantive changes it wanted. But many of the substantive changes were hard for Brussels to swallow. Finally on

Friday we put our best offer on the table. Only then did the EU realize that we weren't bluffing. They had evidently hoped against hope that with less than a day to go, we'd be forced to compromise further.

This wasn't in Europe's script. It could not accept DHS's last offer without further consultations in Brussels.

So, they asked, would we agree to leave the 2004 deal in place while negotiations continued? I was firmly opposed, of course. I wanted everyone to see that the threat of chaos and liability all around was mostly hype. But the issue was going to be decided well above me. That was good news. Chertoff was firm in wanting to break free from the European data-protection shackles, and he understood the value of ending the threat of transatlantic chaos. What's more, with the interagency issues elevated well above the usual players, the entire process was growing smoother. At the Deputy and Secretary level, both State and Justice were more supportive of DHS. At that level, the interagency reached agreement on a final step to demonstrate U.S. resolve.

Chertoff contacted his counterpart in Brussels, Franco Frattini. Commissioner Frattini was a charmer. As far as I know, he never really wore his topcoat over his shoulders like a cape, yet somehow that's the impression he left. Always smiling and full of energy, he had the dash of a young Marcello Mastroianni. He had made his career not in Brussels but in Italy, as a right-of-center politician and interior minister. He represented the European Commission's views with enthusiasm, but when push came to shove, he was on the side of law enforcement. His practical experience as a law enforcement minister allowed him to reach across the Atlantic and find common cause with Chertoff whenever tensions rose.

Encouraged by his conversations with Frattini, Secretary Chertoff decided to dramatize how close the parties were. He initialed the last DHS offer and sent it to Frattini. And he issued a public statement revealing that the ball was in the EU's court. The commission had only to initial the same document by the end of the day to avoid any further delay.

If it did not, though, the 2004 undertakings were dead. DHS made clear that it would unilaterally implement the changes it had proposed in the interpretive letter as promptly as possible. And we also declared that on October 1, "planes will continue to fly uninterrupted and our national security will not be impeded. Importantly, the proposal ensures the appropriate security information will be exchanged and counterterrorism information collected by the department will be shared, as necessary with other federal counterterrorism agencies."[4]

The wall was going to end, agreement or no agreement.

The crunch had truly arrived. All Saturday, airline representatives burned up the phone lines, trying to reach the negotiators. One association called me to insist that the United States had to get a deal; some airlines were already making plans to put their planes on the ground at midnight, the association claimed. Only a deal, or perhaps an agreement to roll the arrangement over for a time, would forestall chaos.

But we were determined not to bend. The threat of chaos was the weapon that Brussels had used in 2004 to extract dangerous concessions on security from the United States. No more. The statement we issued on Saturday quite deliberately made no mention of continuing to abide by the undertakings. DHS was willing to acknowledge informally that changing its procedures would take a bit of time, but the undertakings would be at an end—dead—at midnight.

Once the EU's negotiators had left for the airport, there was nothing to do but wait. The other negotiators and I were on tenterhooks all Saturday night and Sunday morning. Had we miscalculated? Would the European airlines stop flying or stop providing data? Would DHS have to begin imposing fines to force the airlines to cooperate? Would the EU lean on Canada to end its cooperation on passenger name records with the United States?

If the gamble failed, and the threat of chaos turned out not to be a bluff, my strategy would be discredited, and DHS's control of the talks would be at risk. Those who believed that DHS was not competent to manage a high-stakes negotiation successfully would roll out

their I-told-you-so's. And resistance to the EU's information restrictions would begin to crumble.

By Sunday afternoon, though, it was over.

Not one airline had canceled a single flight. Not one had withheld passenger name records. The UK had even issued an order requiring its airlines to continue supplying them to the United States. And on Monday, Canada quietly let the United States know that it would continue to share data despite the end of the EU adequacy determination.

In Brussels, too, Sunday was a strategic turning point. But not a good one from the EU's point of view. The airlines had been pressing DHS to reach a deal right through Saturday. But when that didn't work, they shifted their tactics. Now they were pressing the EU to take the deal that Chertoff had sent to Frattini on Saturday. The airlines didn't care who gave ground, or what compromises had to be made. Every day without a deal was a day of risk, the airlines believed. And since the United States had made clear that it wasn't moving, the airlines now wanted movement from the European Union.

Even as its leverage was collapsing, though, the EU could not take the deal that was on the table. By Wednesday, sources in Brussels were complaining that Chertoff had scuppered the deal by introducing new last-minute demands, and EU negotiators sent back a marked-up draft of the U.S. proposal that made dozens of changes. Indeed, the draft tried to pull back concessions the EU negotiators had already signaled they would accept.

I was puzzled. This kind of negotiating tactic was almost willfully self-defeating. It was like the first EU text, which Brussels had claimed would simply roll over the 2004 agreement but which in fact made it worse. That aggressive proposal had united the U.S. government behind DHS for the first time.

Now the EU's Wednesday draft had the same effect. With the planes still flying and the data still flowing, DHS's interagency stock had risen, and the EU's Wednesday draft was so unacceptable that

DHS's tough line came to seem like the only appropriate response. There was no more talk in the interagency of showing good faith by agreeing to leave the wall in place voluntarily.

Why did the EU take this tack, I wondered, not once but several times? Faull was too good a negotiator not to realize the harm done by such maximalist positions. The source of the problem, I thought, had to be the EU's own internal politics.

Negotiating with the United States was in the European Commission's blood. For some of the EU's founders, the whole point of uniting Europe was to act as a counterweight to the United States. In trade talks with the United States, Brussels had made real headway by taking a tough line. Parts of the commission viewed their job as finding ways to confront the United States. Unless Faull had extraordinary authority, these elements would always press for the toughest possible line. And it was simple group dynamics that negotiating positions would harden if there was not a single clear decision maker. Proponents of aggressive measures could always say, "Well, why not try it? They can always say no." But the result of that approach was to produce drafts that lacked credibility in Washington and undermined the assumption that Brussels and Washington shared the same antiterrorism goals. And it ratified our view that only the toughest tactics would yield an acceptable outcome when dealing with Brussels.

Once again unified by the EU's overplaying of its hand, the interagency now backed DHS in its determination simply to stare down the maximalists on the European side. DHS was given broad authority to reject practically all of the European positions. As the airlines continued to pressure Brussels, a videoconference negotiating session was set for the end of the day on Thursday, with the hope that a deal could be reached and recommended to a permanent representatives' meeting on Friday.

The timing was bad from the start for the EU. The U.S. negotiators were beginning the talks at 11 a.m. Washington time. For the commission, that meant starting at 5 p.m. in Brussels. And as the United States rejected change after change proposed by Brussels, the

time difference grew more important. Impasse after impasse forced delays and consultations on the European side. The phones would be muted but the video showed the European team's body language. It was not pretty. Bitter arguments were clearly breaking out whenever the talks paused. But in the end, each argument was followed by a European retreat.

It became clear that the commission itself had a deadline. It had to have an agreed document to recommend the next morning to the permanent representatives. We were in the catbird seat. If they wanted a document by the following morning, they would either have to persuade us to accept their change, at best a lengthy process, or recede. Moving systematically through dozens of proposed changes took many hours, so that the last issues were not finally addressed until eight or nine at night in Washington—two or three in the morning in Europe. At last we had not just the calendar on our side, but the clock as well.

That did not mean that DHS had everything its own way. This was still a negotiation among equals, and there were some issues where DHS did not press for unequivocal victory. It's never a good idea to press a tactical advantage so hard that the other side feels trounced. That only sets up a grudge match for the next set of talks.

DHS gave ground on information sharing, mainly to defuse a few of the most explosive fantasies being peddled about U.S. practices. To reassure the EU that other agencies would not have free rein to rifle travel records at will, DHS agreed not to grant "unconditional" and "direct" electronic access to other agencies. This formulation would, of course, allow other agencies to log into the database, as long as their access was conditioned by the requirement that they obey the rules that governed access. Perhaps most important, DHS agreed to share data only on a case-by-case basis. We could live with this because "cases" were defined very broadly. They did not have to be classic criminal investigations but could include all the common-sense circumstances in which DHS needed another agency's expertise or assistance to address an actual concern.

And DHS retreated at least for a time on the question of how long it could retain passenger name records. The three-and-a-half-year limit on record retention was a sore point for DHS; we believed that travel data was likely to have value for many years. But Faull stressed that there was no need to address the issue now. The retention period could be revisited in the next negotiation; no data would have to be destroyed before then. Much as DHS wanted to expand the retention period, Faull's point made sense. We agreed that the issue could be postponed.

These compromises sealed the deal as dawn broke outside the windows in Europe. With no time for sleep, Faull carried the marked-up documents to the member states' permanent ambassadors and got their approval that day.

The last round of negotiations was tough for the Europeans, but not as tough as their next task. They had to explain the deal to the parliament members and the privacy bureaucrats who had pressed to reopen the negotiations.

"European data protection authorities are choking on their baguettes after seeing the detail of the data-sharing agreement the EU signed with the U.S. on Friday," a reporter for *The Register* in Britain summed up colorfully. "European data protection authorities said they were 'amazed' when they saw the letter yesterday because it watered down the new agreement so that it was even weaker than the last."[5]

It was true. The European privacy bureaucrats—and the European Parliament— had gambled and lost.

"Unfortunately, the outcome of the court hearing was such that we basically sidelined ourselves," said Sophie in't Veld, a parliament member who opposed the U.S. deal, in an appearance before the UK House of Lords.[6]

But it was worse than that. The European Parliament had not been on the sidelines. By going to court and getting the first deal knocked out, it was the parliament that made it possible for DHS to remove the most onerous privacy terms from the arrangement.

What's more, letting the September 30 deadline expire had done permanent damage to Europe's position in future talks. The fear of chaos that was the EU's most valuable bargaining chip had been devalued by two weeks of calm between the expiration of the first agreement and adoption of the second.

Recognizing the facts of life, parliamentary and data-protection agency complaints about the second agreement and the interpretive letter sputtered on for a time and then died away.

The lesson was not lost on either side. Each now knew that the bark of the data-protection ideologues was worse than their bite. It seemed likely that the next negotiations would end much as the last negotiations did—with the EU in gradual retreat.

Within a few months, of course, we were back at the negotiating table. As Faull had pointed out, the 2004 agreement had to be replaced in 2007. The drama surrounding September 30, 2006, was followed almost immediately by another round of negotiations, this time about whether to renew the agreement. DHS again took a tough line, suggesting that the agreement simply be allowed to expire in July 2007.

"It has outlived its usefulness," I insisted. But the interpretive letter had taken much of the fire from our opposition. It gave DHS the flexibility it needed in most cases. If the concessions Europe had made in the letter could be incorporated into the next agreement, and the three-and-a-half-year retention period could be greatly extended, there was no practical reason to kill the arrangement entirely.

So, in a long anticlimax, that's how the second round of negotiations in 2007 played out. Because DHS was willing to live without an agreement, the EU had to make further concessions just to hang on to an agreement of some sort. The principal issue was how long data could be kept. The old agreement had insisted that data would be kept only three-and-a-half years and that the data collected under the agreement would be destroyed on that schedule no matter what. Both provisions had to go, in DHS's view.

This time around, the negotiations quickly moved to a higher level. By now, the European Council's presidency had rotated to Germany. That was good news for us. In April 2007, Secretary Chertoff made a quick, one-day, trip to Berlin to meet with the head of the German Ministry of the Interior. The German interior minister, Wolfgang Schaeuble, was as forthright an ally as we had found in Europe. (He has since become finance minister in Germany's center-right coalition government.) The victim of an attempted assassination himself, Schaeuble was confined to a wheelchair. A practical man with a sharp mind, he had a cheery affinity for Chertoff.

They met in September 2006, when Schaeuble first came to see Chertoff in the United States. Germany had recently concluded the "Pruem Agreement," allowing European countries to share information about criminal records. We'd briefed Chertoff on the agreement. Schaeuble was impressed with Chertoff's grasp of the agreement, and before the conversation was over, he half-jokingly invited the United States to join the agreement. He must have been surprised when Chertoff, who'd been briefed on the possibility, immediately took him up on the offer. Within two years, though, the deal had been done, and a friendship had been cemented.

With Schaeuble and Frattini leading Europe's team, we hammered out a deal with far less drama than in the first talks.

The two sides agreed that data would be kept for fifteen years instead of three and a half. But to cushion the public reaction, we agreed that the data would spend only seven years in an active database and the next eight in an inactive database. All of the data was put on this schedule, including anything gathered under the old agreement with its three-and-a-half-year schedule. Faull had been right to urge that we postpone that question.

On the crucial question of information sharing, Chertoff again stood firm. He was not going to rebuild information-sharing walls after the failures of 9/11. In the end, the Europeans agreed that DHS could use and share data based on any case that it was investigating or examining. This allowed DHS to identify routes of concern and to share

travel data if the routes were the objects of DHS scrutiny. So long as the concern and the examination arose in good faith, data could be shared easily, assuming good security protections were in place.

As the talks proceeded, the text grew simpler. Many of the detailed and prescriptive security and procedural rules from the 2004 agreement were simply dropped. We began to think that we would have an uneventful second negotiation.

Unfortunately, not everyone in Brussels was reading from the same script. In 2007, the Cricket World Cup was held for the first time in the Caribbean. The Caribbean Community (CARICOM) nations worried that terrorism might mar the games, which attract visitors from India, Pakistan, and other South Asian countries. They asked the United States for help in screening travelers to the Caribbean. The United States helped CARICOM set up a system to collect and process advance passenger information. Data sent to the Caribbean nations was collected by the CARICOM nations and shared with DHS, which alerted the countries to risky travelers bound for their airports. A number of dangerous travelers were identified and refused entry or arrested as the games drew near.

The screening was a success for the United States and the CARICOM nations. But as the deadline for a third agreement on passenger name records drew near, a European representative decided to put the CARICOM arrangement in play. We learned about it when we got an agitated report from one of the top officials in a Caribbean nation that the EU was "essentially blackmailing CARICOM." The EU told CARICOM's trade negotiators in Brussels that it would withdraw all development funding for the region, if the United States did not follow "international standards." If the EU followed through on this threat, the official declared, the economy of the region would essentially be destroyed.

At the next negotiating session with the EU, I lost my temper. This was beyond the pale—an attempt to bully weaker nations into denying us information about dangerous travelers on our doorstep. After a

brief attempt to justify the action, the EU beat a quick retreat, blaming the incident on unauthorized action by a British member of the European Commission staff. The threat to CARICOM was withdrawn. The EU's effort to find additional leverage in the talks, if that is what it was, had provoked so much outrage in Washington that it backfired.

But we weren't satisfied. Counting the Canadian gambit from the earlier talks, this was the second time that the EU had tried to organize an international information boycott of DHS. In reaction, we insisted that the new agreement make clear that such efforts would not be repeated. As long as the agreement was in effect, we insisted that the EU not interfere with third-country transfers of passenger name records to the United States. Jonathan Faull reluctantly agreed.

For the same reason, we pressed successfully to strengthen the reciprocity provision. We wanted an assurance that Europe could not insist on one rule for the United States while allowing its own terrorism authorities to follow less demanding rules at home. If the EU did not apply to its own members the rules in the new agreement, then the rules would not apply to the United States either.

With these changes, the agreement was signed in July 2007. We were finally through. After three negotiations in four years, neither side was interested in a rematch. The Americans were satisfied with the changes, and the Europeans had no appetite for further negotiations on a subject where their leverage had turned out to be so limited.

In fact, the Europeans were about to execute a remarkable pivot, from confrontation to imitation. After three years of complaining about the U.S. travel data system, the commission suddenly proposed that Europe adopt one of its own. More remarkably, the system resembled the U.S. system in almost every detail—except that it provided fewer protections for personal data.

The U.S. negotiators reviewed the proposal for European PNR systems with amazement. "Thank God we insisted on a reciprocity clause," said one. "By the time they're done making the rules for themselves, they'll relieve us of half the obligations in the new agreement."

What had happened? It would be tempting to chalk the about-face to a kind of institutionalized blind spot that makes American systems look inadequate to the EU just because they're American, while European systems look adequate just because they're European. The truth is a little more complicated.

The ironic effect of the conflict over PNR was that it forced us to justify our system. And we did. While the debate was ongoing, France and Denmark enacted laws authorizing the collection of PNR. The UK and the Netherlands launched pilot PNR projects. A committee of the UK House of Lords, deeply skeptical at first, declared in the end, "We are persuaded that PNR data, when used in conjunction with data from other sources, can significantly assist in the identification of terrorists, whether before a planned attack or after such an attack."[7]

Persistence and a full-throated defense of our program had won the day. Even so, DHS had been lucky. There was still a large body of opinion in Europe that wanted to thwart—or at least hobble—most of the U.S. data programs initiated in the wake of 9/11. To understand what could have happened if DHS had been less determined, it is only necessary to look at the U.S. and European handling of the SWIFT affair.

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is one of the great rivers of financial data that flow around the world each day. It carries international bank transfer messages for thousands of banks in two hundred countries.

Some of those transfers have helped fund terrorism. Terrorist groups must raise money to pay for their outrages. Then they must move the funds to their operational units. To do so, the terrorists must either physically carry cash or use modern financial institutions. A host of electronic networks and links among banks make the international transfer of funds easy. Al Qaeda often took advantage of these networks to move its funds. The alternative, sending cash by courier, runs the risk of interdiction, since carrying large, undeclared amounts in cash is illegal in many countries.

After 9/11, the United States Department of Treasury decided to ramp up its efforts to prevent terrorist groups from using modern financial networks. Banks were already under an obligation to "know their customer" and to report suspicious transactions. But often, Treasury was aware of information about suspicious persons or activities that it could not share widely with the banks. It therefore had to gain access to a large amount of data and then sift that data, using its own classified search terms and algorithms.

Treasury was doing the financial equivalent of what DHS did on the border. Far and away the vast majority of financial transactions—like the vast majority of travelers—held no interest for the government. They were simply part of the vast ebb and flow of money from institution to institution for legitimate purposes. Hidden in that river of transactions were a tiny few that bore the hallmarks of terrorism—a known al Qaeda financier, a suspected middleman, an institution that made a business of supporting suspect groups. Using modern information technology, it was relatively easy to pluck those transactions from the stream for more detailed review. But just as DHS did not rely on the airlines to decide which passengers should be scrutinized, Treasury could not rely entirely on the banks. The names and other facts that triggered scrutiny were sensitive; Treasury could not simply hand the list to SWIFT and ask it to conduct a search.

Treasury had full legal authority to simply order SWIFT to hand over its data. SWIFT kept a full set of records for its transactions in two locations, Belgium and the United States, and records kept on U.S. soil are routinely subpoenaed in criminal investigations. But even after 9/11, SWIFT was extraordinarily reluctant to disclose the transactions it carried. SWIFT could have resisted in court, forcing Treasury through public litigation that would have greatly diminished the value of access to the data. If terrorists and their financiers knew that interbank transfers were being monitored, they would switch to other methods.

To avoid litigation, Treasury and SWIFT negotiated an agreement that seemed to give each party what it wanted. SWIFT would

carry its transaction records to Treasury, where they would be run through a "black box" that applied Treasury's patterns, names, and other algorithms. Neither side would have access to the other's sensitive data. At the end of the process, Treasury would be given only transaction data that had triggered one of its tripwires.

It worked. Treasury later credited the program with allowing it to track and capture the mastermind behind the Bali bombings that killed two hundred people. The program was also said to have allowed Treasury to identify and convict a Brooklyn man who had laundered $200,000 for al Qaeda.

Alas, the program was soon to lose much of its value. In June 2006, the *New York Times* evidently decided that the program must be scandalous; over the vehement objections of the Treasury, it published a lengthy expose′ about it.[8] The public editor of the *New York Times* would later conclude that the paper had been wrong to compromise the secret program, declaring "I haven't found any evidence in the intervening months that the surveillance program was illegal."[9] But by then it was too late. The *New York Times* had managed to create a storm over the program in Europe.

Because SWIFT was a Belgian company, Treasury's access to its records was quickly wrapped into the same storyline as PNR. Americans, the European media claimed, were overreaching to extract private European data from compliant companies without proper safeguards. Investigations were begun in more than a dozen countries. The Belgian data-protection authority seized the initiative. By September, it had issued a report declaring without citing much evidence that SWIFT was in violation of Belgian data-protection law.[10] By November, the entire working party of European privacy bureaucrats had joined in support of the Belgium ruling.[11]

This was, to say the least, an aggressive reading of European law. The data that had been subpoenaed was located in the United States. And SWIFT had done everything it could to minimize intrusions into the privacy of transactions that did not trigger suspicion.

What exactly had SWIFT done wrong?

In essence, the Belgian data-protection authority concluded, the United States Treasury had not lived up to European standards of conduct, and SWIFT had failed to force the Americans to adhere to those standards: "From the beginning, SWIFT should have been aware that the fundamental principles of European law were to be observed, apart from the enforcement of the American law, such as the principle of proportionality, the limited retention period, the principle of transparency, the requirement for independent control and an adequate protection level."[12]

No company had ever been found in violation of European law because it failed to bring a sovereign government to heel, but for European privacy advocates, that was just the beginning. SWIFT soon faced actual civil investigations in Germany and Canada, as well as Belgium, plus complaints in more than thirty countries. On top of all that, SWIFT executives were being criminally investigated and threatened with jail time. All for the crime of obeying U.S. law, in the United States, to assist in pursuit of an enemy that had killed more Americans on U.S. soil than anyone in a hundred years.

The legal theory being used against the company was dubious at best: Even the notion that the U.S. program somehow violated European law was doubtful. DHS's Privacy Office would later publish its findings that European programs to collect and analyze hotel registration were far more intrusive and less carefully constructed than Treasury's program; but they had never been questioned by the privacy bureaucrats who claimed to be so outraged by the U.S. program.

All that hardly mattered in the frenzy of objection to an American program that everyone knew, even without evidence, must be an abuse of power. For SWIFT, having legal defenses that ought to prevail was cold comfort; it could not afford even victory if the price was this public beating. SWIFT is a cooperative owned by banks in many nations; and most of the owners were none too pleased to learn about SWIFT's cooperation in breaching the secrecy of their transactions. They no doubt made this displeasure felt through their representatives on the SWIFT board. SWIFT began looking for an exit.

Desperate, Treasury opened talks with the European Commission, and within six months, in mid-2007, the two sides struck a deal that we found familiar. Treasury offered the Europeans unilateral representations, setting out the protections it was prepared to implement. And the commission relied on those representations to declare Treasury's protections "adequate," setting at rest the preposterous claim that SWIFT was somehow liable for violations of data protection law. Treasury's undertakings followed the PNR model, too; the department agreed that it would search only for terrorism data, that it would delete data that was not relevant to this search, and that most data would be deleted in five years. In another mark of European distrust, the Treasury's compliance with its promises would be audited by an "eminent European person"—who would have to be given a U.S. security clearance so as to be able to investigate even classified activities.

Separately, SWIFT agreed to apply European law to data stored in its U.S. offices, and the U.S. government agreed to enforce European law under a "safe harbor" agreement with the EU. In case there were a few terrorist financiers who had missed the *New York Times* article and the European flap, SWIFT also agreed to provide notice of the program.

By the end of the Bush administration, a kind of peace had been restored. SWIFT was protected from liability, and the furor had died down. Subpoenas were being served and honored. The Belgian data-protection authority issued a report admitting that, after a more detailed examination, what SWIFT was doing was consistent with European law. The "eminent European person" also concluded that Treasury was keeping its word.

But it was the peace of a patient on life support. The secrecy of the program had been breached fatally. SWIFT's American CEO, who had defended the program as necessary to combat terrorism, retired in 2007. He was replaced by a Spaniard. Shortly thereafter, SWIFT announced that it would restructure its data systems to store data on European transactions only in Switzerland.

European privacy bureaucrats crowed that they had crippled the American program, at least as far as European terror finance was concerned: "the creation of a new operation centre in Switzerland . . . means personal data in intra-European transactions will no longer be processed in the US."[13] The Belgian data-protection authority also cited the new Swiss center favorably when it announced in early 2008 that SWIFT actually hadn't broken Belgian law. Coincidence? Nope. SWIFT admitted that pressure from the privacy bureaucrats was one of the reasons it adopted the new architecture: "Distributed architecture will improve resilience, add capacity, control long-term average message costs, *and alleviate European data protection concerns*."[14] In short, it's pretty clear that SWIFT was forced to withhold European terrorist financing information from Treasury by European government officials.

The lessons here are disturbing, to say the least. It now appears, in the wake of the UBS tax evasion scandals, that renowned Swiss bank secrecy laws will be modified to allow the pursuit of tax cheats. Yet a substantial number of European officials seem to think that those same secrecy laws should remain inviolate when the subject of scrutiny is terrorist financing. There's no justification for this distinction.

Having made a mess of an effective U.S. terrorism program without substantially serving privacy, some in Brussels tried to minimize the damage. The European Commission negotiated an agreement to give the United States access to intra-European bank transfer data even after the Swiss operations center is set up—but only if Treasury continued to live up to European standards.

Remarkably, even this was too much for the privacy campaigners of Europe. In the first exercise of new authorities granted to it by the Lisbon Treaty, the European Parliament rejected the agreement, essentially creating a European safe haven for terrorist finance.

What lessons can we draw from these stories? Certainly the implications for U.S.-EU relations are not good. DHS's passenger screening system was deployed at the direction of a Democratic Congress and in

reliance upon a series of Supreme Court rulings; in effect, both parties and all three branches of the federal government participated in the decision. The EU could have acknowledged that, while American law policy did not comport with its own preferences, the United States nevertheless was entitled as a sovereign to choose differently. It could have let the United States follow its own path in fighting terrorism.

It did not.

Instead, Brussels claimed the right to sit in judgment on American data privacy practices. Worse, it assumed that its natural role was to thwart any new American initiative, either permanently or at least until it had been persuaded to imitate the program in Europe.

Perhaps most troubling for anyone who believes in multilateralism and international law, the tactics adopted by the European Union cannot easily be defended. The European Union never explained why its domestic commercial data-protection directive should override the spirit and text of the longstanding multilateral Chicago Convention, which clearly says that airlines must give the countries where they land personal data about the travelers they carry. Ignoring this convention and putting the airlines at risk of penalties for obeying U.S. law was a breach of settled principles of international law and comity. Nor did Europe ever justify its assumption that no criminal data-protection law could be adequate unless it was nearly identical to European law. In fact, the European Union never defined "adequacy" in the law-enforcement context, leaving the concept a moveable feast that can be modified on the basis of political, rather than legal, judgments. Finally, and most troubling for large multinational enterprises, the European Union seemed almost enthusiastic about threatening private companies with sanctions as a way of attacking U.S. government practices.

Putting private actors in a position of having to violate the laws of one sovereign in order to heed the laws of another is dubious practice under international law. But far from being reluctant to do so, the European Union seems to have concluded after the PNR episode that the tactic should be applied to new fields. It encouraged a criminal

data protection investigation of SWIFT, saying in essence that, before complying with U.S. law, SWIFT had to ensure that the U.S. government met European standards. Since no private company, particularly after receiving a subpoena, has the leverage to demand such assurances from investigators, such an analysis dooms the company to simply deciding which law to violate.

Why would Europe sacrifice its traditional commitment to multilateralism and international law for the purpose of thwarting terrorism investigations in other countries? There are many possible explanations, but in fact the fights over SWIFT and PNR seem more and more to be of a piece with fifty years of Brussels policy making. The first instinct in Brussels, it seems, is always to oppose U.S. initiatives, perhaps directly, perhaps obliquely, and then to call for negotiations. There's an institutional reason for such a stance. Forcing the United States into negotiations demonstrates Brussels's relevance; at the same time it pulls authority away from the member states and toward the commission and its negotiators.

This dynamic is not just an artifact of Europe's dislike for President George W. Bush. President Obama got a taste of the same thing within months of taking office. After years of clamoring for the United States to close Guantánamo, how did Brussels react when President Obama proposed to do just that, and got a few European countries to agree to take a handful of the prisoners?

With a kind of genteel horror the EU asked, "How could the United States do such a thing without first getting permission from Brussels?" The European Commission insisted on interposing itself between the United States and the European countries that were willing to take a few prisoners. It then took months of negotiations to get Brussels to agree that, yes, the member states really could help out the new administration by accepting detainees. Only then could the United States and the member states negotiate actual transfers of prisoners.

The Brussels instinct to say "*non*" to American initiatives, at least until they have been milked for a contribution to European solidarity, is a force for global conservatism. If Europe's first inclination is always to slow the Americans down, question their motives, and make them pay for any changes in policy, there will be no quick responses to the challenge of accelerating technologies. This international conservatism is among the most powerful forces favoring a kind of exponential status quo.

It was a force we'd have to face again as we implemented the next step in our strategy for responding to the challenge of commercial jet technology.

7 Al Qaeda's Frequent Traveler Program

In the days before Christmas 2001, the attacks of September 11 were still an open wound. But international flights were slowly returning to normal. Americans were going home from Europe for the holidays; Europeans were taking their holidays in Florida's warmth.

Now was the time for a second strike, al Qaeda's leaders thought. Americans must know that military success in Afghanistan was irrelevant—it could not protect them at home. The first attack inside the United States had succeeded beyond expectations. Another would be devastating.

But the U.S. response had been tougher and more effective than al Qaeda expected. Its agents and sympathizers inside the United States had mostly been rounded up or expelled, often on immigration charges.

To launch a new attack, al Qaeda would have to send terrorists into the United States. But that path was perilous. American border officials were on high alert; customs and immigration controls had been tightened.

Visa applicants from Muslim countries faced tough new scrutiny. U.S. visa processing had returned in many ways to the 1950s. All applicants had to complete a form filled with personal questions. All applicants were interviewed by consular officials at a U.S. embassy or consulate. And in a new measure, all were fingerprinted to confirm their identities. Before allowing visa travelers in, the United States

learned a lot about them—their family status, prior travel to the United States, present employment, the purpose and length of their planned trip to the United States, where they planned to stay, and who was paying for their trip.

The original focus of the questions may have been whether the travelers would overstay their visas and take illegal jobs in the United States, but the process was quickly revised to search for terrorist ties. If any doubts were raised on that score, the applicants simply didn't get a visa. And without a visa, the airlines wouldn't even let citizens of those countries get on a flight bound for the United States.

That was al Qaeda's problem as it looked for a way to launch a second strike on the United States. It had no trained terrorists left inside the country and it couldn't send a new team in, at least not from Saudi Arabia or Yemen or Egypt.

It sounded like a riddle. How do you attack the United States without entering the United States?

But al Qaeda had the answer. It had a plan.

And a man to carry it out.

Boarding Flight 63 from Paris to Miami, Richard Reid did not exactly blend in. He was huge—six-feet-four and over 200 pounds—and the son of an English mother and a Jamaican father. In other circumstances, he might have made the other passengers a bit uneasy. He was, after all, a hardened street criminal who'd spent time in England's notorious Feltham Prison. But in the jittery months after 9/11 what mattered most was that he bore no resemblance to the Arab hijackers.

In fact, though, Reid had converted to a radical brand of Islam in Feltham. Al Qaeda was eager to use a Western convert on a suicide mission. He would get less scrutiny, and a successful suicide mission by a British subject would show the West that it was rotting from within.

But the real beauty of sending Reid on the mission was his passport. All the visa controls imposed by the State Department were irrelevant to Reid. As a British subject, he was part of the Visa Waiver Program. Citizens of developed countries were permitted to travel to

the United States without a visa and to stay for up to ninety days. Launched in the 1980s as a flood of commercial jet travelers overwhelmed U.S. border controls, the VWP was widely praised by business groups and travelers. It allowed easy, spur-of-the-moment trips to the United States, and it allowed Americans to make similar trips to Europe, Australia, Japan, and other popular destinations.

After 9/11, it was also the answer to al Qaeda's prayers. VWP travelers could get on planes without any screening by U.S. authorities. They could fly from Europe into American airspace without any scrutiny until the plane landed. And if the plane never landed—if they blew it up while it was near or over the United States, U.S. authorities would be helpless. All its border controls would be for naught.

That was al Qaeda's plan. It could evade all of America's new visa and border measures and still bring death to American skies.

Reid took a row to himself. He refused food and drink, even though it was a ten-hour flight. But he didn't draw much suspicion until hours into the flight. Then one of the attendants smelled smoke. Walking the aisles, she saw Reid hunched over in his seat.

"I thought, he's smoking," she told *Time* magazine. "It got me mad. I was talking to him, saying, 'Excuse me,' but he just ignored me. I leaned in and said, 'What are you doing?' "[1]

Then she saw.

"He's got the shoe off, between his legs. All I see is the wiring and the match. The match was lit," she says.[2]

I'm going to die, she thought.

She might have been right. According to the FBI, that one shoe held enough plastic explosive to blow a hole in the side of the plane.

She called for help. Another attendant grabbed Reid from behind, and he sunk his teeth into her hand.

"I couldn't get my hand out of his mouth" the second attendant told *Time*. "I thought he was going to rip my hand apart it hurt so bad."[3]

Passengers rallied to the attendants' aid. They helped pour water over Reid and his match. (It was a flight from Paris, so they used Evian.) Crew members used everything on hand to truss up

the massive terrorist—plastic cuffs, headphone cords, and a seatbelt extension. A doctor on the flight injected Valium.

Reid still tried to break free; he bared his teeth at the crew when they spoke to him.

But passengers and crew had done their job well. When the plane finally landed, he was so thoroughly hogtied that the FBI had to cut Reid out of the improvised restraints. After a trial and conviction for terrorism, he was sentenced to life in prison.

Al Qaeda had been thwarted once by an alert air crew. Five years later, no one boarded a plane without sending one's shoes through the x-ray machine. But the real hole in American defenses hadn't been patched. The VWP was still going strong.

So al Qaeda—which doesn't easily let go once it gets an idea in its collective head—decided to try the same thing again, but on a bigger scale.

Al Qaeda planned several simultaneous suicide attacks on trans-atlantic flights from Great Britain to the United States. It couldn't use shoes this time, so the terrorists would smuggle common household chemicals onto the planes, then mix them together into an explosive concoction.

Later tests by the Transportation Security Administration found that the liquids were more than enough to blow holes in each of the planes, bringing them all down over the Atlantic Ocean or the United States.

And how were the plotters going to evade U.S. security controls? The same way Richard Reid did. They planned to use British passports to get on the planes, and then destroy the plane and its passengers before American authorities ever laid eyes on them. At least eight British citizens of Pakistani descent were part of the conspiracy. Every one was eligible for visa waiver treatment. Visa waiver had become al Qaeda's favorite travel program.

Once again, overlapping security measures managed to compensate for the lack of controls on visa-waiver travelers. This time it was

good law enforcement and intelligence. The British discovered the plot while it was still in the planning stages. They monitored the plotters before swooping in to arrest them.

We had dodged a bullet again. But we couldn't count on luck to keep us safe forever.

So why didn't we just get rid of the visa waiver program? That was the question that some in Congress kept asking. Senator Dianne Feinstein and Senator Jon Kyl were particularly dubious about the VWP, and they regularly complained about the program's flaws.

But the reasons for adopting the program hadn't gone away. All in all, travel to the United States helps the economy and may even reduce anti-Americanism. Tourism and business travel are crucial in a country like ours that runs trade and payments deficits each year. Each year more than four million travelers come here from the UK and more than three million from Japan. In all, nearly twenty million visitors arrive in the United States under the VWP. Whole business models had been built on the ever-increasing pace of international travel. Were we willing to bankrupt those companies?

And what would we do at the embassies that were suddenly asked to process visas for millions of European and other travelers? Lines would run around the block. State Department officials would have to be drafted for consular duty in these countries, and the pressure to process the applications quickly would make rigorous scrutiny almost impossible.

What's more, international pressure to undo the change would mount quickly. At the time, twenty-seven countries were part of the U.S. visa waiver program, including all the most important American allies in the Cold War—nations like the United Kingdom, France, Japan, Germany, Australia, Italy, and New Zealand. Every one of these governments listened to their businesses and their travelers. They, too, expected the exponential rise in jet travel to go on forever. And they would not tolerate an American policy that interrupted that trend. They would insist that the program be reinstated. If it was not, they would retaliate, withdrawing visa-free treatment from U.S. travelers and forcing Americans to stand in lines around the block for visas to enter their countries.

If all that came to pass, Senator Dianne Feinstein's high-tech constituents would not thank her. Right now, they can catch a flight to Europe or Japan on less than a day's notice, and so can the customers or investors that visit them. Travel barriers that ran both ways would crimp their international ties.

No one wanted less travel. No one wanted a return to the 1950s. The forces of exponential conservatism still wanted jet travel to double and double again every decade. These were the forces that had created the VWP. And they were building again, making the case for expansion of the program.

We couldn't just stand in their path and shout, "Halt."

But the world had changed while the VWP had not. If it was meant to be an exclusive club for American allies, then it was out of date. It was like a museum exhibit of American allies from the Cold War era. When the United States decided to attack Saddam Hussein, the old alliance was ripped apart. Countries like France and Germany more or less switched sides, working with traditional U.S. adversaries such as Russia and China to thwart the U.S. plan. In contrast, the United States received backing from Eastern Europe. Poland, the Baltic states, Hungary, the Czech Republic, Slovakia, Ukraine, Romania, and Bulgaria all sent troops to fight in Iraq alongside the Americans. Asked why his little country had sent a force to Iraq, the Latvian ambassador's reply was poignant: "Because you asked."

We didn't have allies like that in Western Europe. But as far as VWP was concerned, Eastern Europe was still behind the rope line waiting to be let in. Indeed, some of the hardest conversations we regularly had with Jonathan Faull and others at the European Commission were about the VWP. Faull routinely pressed for inclusion of the new EU members from Eastern Europe in the program and, to be frank, his case was convincing.

Actually, it was more convincing for Eastern Europe than for Western Europe. Sure, travelers from these relatively rich countries were a lot less likely to become illegal immigrant laborers than

travelers from poor countries. But after 9/11, the biggest danger posed by foreign visitors wasn't that they'd take dishwashing jobs away from New Yorkers.

If you're worried about Islamic terrorists traveling without visas, the last countries that should belong to the visa waiver program are those with large and disaffected Islamic populations. That's true of most of Western Europe. In contrast, Eastern Europe still hadn't needed to import much labor from abroad. If we were making generalizations about "safe" countries, in short, we'd have let Eastern Europe into the visa waiver program before France, the United Kingdom, Germany, or the Netherlands.

The new alignment hadn't gone unnoticed elsewhere. Ethnic politics reinforced a sense of obligation to our most committed allies as Polish, Lithuanian, and Latvian communities across the country campaigned to bring their homelands (and their relatives) into the program.

Shortly after the Iraq War ended, Senator Rick Santorum, a deep-dyed conservative Republican from Pennsylvania, introduced a bill to give VWP status to Poland. His Democratic cosponsor, Senator Barbara Mikulski of Maryland, pointedly asked why France had VWP status while Poland did not. That was troubling. If even security-minded legislators like Senator Santorum wanted to expand the VWP, our security concerns about the program weren't getting through.

Then, in 2006, Senator Santorum got his bill attached to the massive immigration reform bill being shepherded through the Senate. It was a classic legislative move. The senator knew the Bush administration would have to swallow the change in order to keep its priority legislation on track. DHS might squawk, but it would be ignored.

The test didn't come that year, it turned out. Immigration reform failed, and Senator Santorum was not reelected.

But as far as I was concerned, trouble was surely coming. Senators Kyl and Feinstein might rail against the VWP, but as memories of 9/11 faded it was likely to be expanded, not cut back. If we didn't do something, the security hole would get bigger soon.

Luckily, we'd already begun thinking about alternatives. In 2005, at the urging of the State Department, we'd agreed to lay out a "road map" to VWP status for a new group of countries, mostly in Eastern Europe. But that effort was doomed from the start. We didn't want to expand the program as it stood and the way the law was written, we probably couldn't have done it even if we'd wanted to.

But we had to do something. In November of 2005, a storm broke in Europe over an allegation that the CIA was moving detainees from one secret prison to another in parts of Eastern Europe. European institutions, backed by Western European politicians, excoriated the Easterners for aiding this controversial tactic. It was clear that the split over the war had not been forgiven in Brussels. Countries like Poland would be made to pay and pay again for deviating from the Franco-German line on Iraq.

I stopped by Secretary Chertoff's office. We had several things to talk about. When we were done with our main business, I dropped in another idea. "You know, our best friends in Europe are getting the worst deal under VWP," I said. "I'd like to spend some time thinking of ways to get them in—and improve security at the same time." He was walking around his desk at the time. He stopped in midstride and turned with a glint in his eye. He pointed a thin finger at me and with a smile that was almost mischievous said simply, "Let's do that." That was all the policy guidance I needed.

The deputy secretary at the time was named Michael Jackson. A tall gray-haired workaholic from Texas, Jackson was also a gifted government official. He had worked his way up from the bottom of the bureaucracy to become deputy secretary at two different departments—Transportation and Homeland Security. His easy Texas twang and aging athlete's spare tire hid a canny political mind.

He, too, could see the trap about to spring. He called me and my deputy, Paul Rosenzweig, into his office not long after my conversation with the secretary. "The road map," he said, "is a road to nowhere. I feel like we're just stringing these folks along." He asked the policy office to develop a series of options for completely rethinking the VWP

program. The secretary's three-word guidance was going to become a full-fledged DHS initiative.

But this was not a problem we could fix under the law as it stood. Written to keep illegal dishwashers out of the United States, the law set a host of requirements for VWP status that had nothing to do with security. If consular officials in a country turned down more than 3 percent of the visa applications that they received, the result was fatal for the country's VWP candidacy. The theory was this: consular officials usually turn down applicants because they fear the applicants really intend to immigrate to the United States illegally. So countries with a high visa refusal rate are countries that may send us too many illegal immigrants.

That may be true. You could argue about what the exact cutoff should be, and you could object that countries were being graded on consular officers' perceptions and not actual conduct. But those arguments weren't our concern. The big problem was that the law focused mainly on immigration risk. It failed to do anything about security risk.

Congress had sprinkled a bit of security over the program after 9/11, saying that no country could stay in the VWP unless it adopted secure electronic passports with biometric identifiers. But resistance even to this modest requirement was fierce. The deadline had to be extended by a year, to 2005, and then again to 2006. Even with two extensions, some countries were not able to deploy the new passports on schedule.

It had worked in the end. More than two dozen countries had raised their passport security standards in order to stay in the VWP club. Why not do that on a much larger scale, we asked? If countries would revamp their passports to stay in the club, surely they'd improve security even more to get in the club in the first place. We could re-engineer the VWP to screen for terrorists as well as dishwashers. We could ask VWP candidates to offer reasonable security measures as part of the VWP negotiation. Those measures would set a new security bar for participation in the program. Once the bar was set, the rest of the club members could be held to the same standard.

Outside the department, the world was divided between those who hated the VWP and wanted it closed down immediately and those who wanted it expanded as soon as possible. We had to assemble a coalition of the middle. The expansionists, we figured, couldn't get past the VWP haters without accepting our security measures. And the VWP haters might get no security measures at all if they didn't accept our view that the measures should be tied to expansion. We were a small part of the debate, not strong enough to prevail on our own. But by carefully shifting our weight from one side to the other, we could provide the crucial swing vote that shaped the final outcome. That was my hope, at any rate. But if either the VWP haters or the expansionists gained a decisive advantage in Congress or the administration, the leverage we were using to set new security standards would be gone; we'd fall off one side of the tightrope or the other. We would need luck, determination, and leadership.

Working quickly, my office pulled together the elements of a traveler security program. At the top of the list was information. We could not continue to let travelers hop on planes in Europe without giving DHS enough information to decide whether they ought to be allowed into the country. We had to know who was coming. Our only sources of traveler information right now were provided by the airlines, and the European Commission was still trying to cut off that data flow. Well, they couldn't have it both ways. If they wanted to be part of the VWP, they would need to agree to better data sharing. We finally settled on three measures that would give us the kind of information we could get from a visa program—without the hassles and endless queues created by the visa system.

First, we'd set up a website to collect information directly from the traveler. That would let us control the kind of information we were gathering, rather than depending on what the airline reservation clerk decided to write down. It would also allow us to identify a suspect traveler in time to tell him that he couldn't come to the United States—thus keeping him off the plane and making it harder for al Qaeda to carry out transatlantic plane bombings.

As a bonus, it would even make the traveler's life easier, since the website could be a substitute for the aggravating forms he'd otherwise have to fill out with a borrowed pencil on the arm of his seat while the plane was landing. We even had a name for the system (one we borrowed from our Australian friends, who already had a similar program up and running). It would be the ETA, or Electronic Travel Authorization.

Implementing the ETA wouldn't actually require anything from our VWP partners, other than restraint and understanding. But knowing who was coming was just part of the job. We also needed to know who *shouldn't* come. And for that, we needed information from the traveler's home country. We needed to know which of their citizens they considered a terrorism risk. And we needed a way to find out whether someone coming to the United States had committed crimes at home.

These items seemed almost embarrassingly obvious. But the State Department had been trying for years to get other countries to share lists of terrorists with us, and their successes could be counted on the fingers of a single hand. When drivers are stopped by highway patrolmen in this country, their criminal records can be quickly obtained from other states—and from Canada. But when a traveler was stopped at the border, not a single VWP country had agreed to tell the United States whether he had a criminal record.

Imagine: Even if a border agent is suspicious of a man who says the young boy traveling with him is his nephew, he would never know the man was a convicted sexual predator at home. DHS had no idea whether the traveler it was inspecting had been convicted at home of smuggling drugs or of committing terrorist attacks. That had to be fixed.

Finally, as always, screening for risky travelers would fail if terrorists could switch identities at will. So we would need a second generation of protections against passport fraud—both better security for the passports and better reporting of lost and stolen passports. To deal with the threat to transatlantic flights, we added provisions to strengthen airport security, air marshal cooperation, and other safeguards we cared a little less about. We knew enough about negotiation not to ask only for the things we had to have.

In exchange for these security measures, we proposed to relax the strict 3 percent refusal criterion in the law—essentially taking a bit of risk on the immigration front to get a lot of new protection on the terrorism front. Without that relaxation, none of the Eastern Europeans would qualify for VWP. In 2005, Poland had a visa refusal rate above 25 percent, while Latvia's was nearly 22 percent. The rates were coming down fast in many countries, but getting below 10 percent would be an accomplishment; 3 percent was, for most of our allies, but a distant dream.

We knew what we wanted. But we didn't know whether we could get it. Like any tightrope act, this proposal would be at risk right to the end. If it hadn't been fully executed by the end of the administration, it could be delayed or the security measures could be watered down.

That shouldn't be so hard, we thought. After all, the president had been sworn in for a second term just that year. The administration had more than three years to run.

But in those years we had a lot to do. First, we needed to make sure the Eastern Europeans were as eager as we thought—and as willing to take security seriously as we hoped. Then we had to get our security measures through the same National Security Council and interagency process that was fighting us on PNR. Then we had to get Congress to adopt the same balanced proposal we were advancing in the interagency. And once Congress acted, if it did, we'd have to negotiate something like two dozen international agreements at the same time we were launching an unprecedented Web-based travel authorization application capable of handling millions of transactions a year.

Suddenly, three years didn't look like much time at all.

Petr Kolar, the Czech Republic's ambassador to the United States, is a bookish man with the mild and friendly air of a college professor. Kolar had barely finished school when the Communists fell. His timing was good. Untainted by service in the old regime, he moved easily from academia to stints in the Czech foreign ministry. He became a

confidant of the Czech prime minister, who sent him to Washington. That turned out to be a wise move.

The Czechs are a proud people who spent most of the twentieth century under one autocratic boot or another. Austro-Hungarian emperors, Nazi *gauleiters*, and Soviet apparatchiks all took turns ruling the Czechs.

None found the job particularly comfortable.

Even today, the Czechs are prone to insisting at inconvenient times that their allies actually live up to their high-minded diplomatic pronouncements. That's understandable; twice in the twentieth century the West gave strenuous verbal support to Czech democrats and then stood idly by while first the Nazis and then the Soviets crushed them.

For Kolar, the Czech Republic's absence from the visa waiver program was a last vestige of the Iron Curtain. It had to go. He pulled together the rest of Eastern Europe in the hope that they could achieve the goal more quickly as a group.

Kolar developed a close relationship with Paul Rosenzweig, my deputy. Kolar kept prodding for action, but he seemed to understand that the world had changed on 9/11, and that security concerns about the program could not be dismissed. Rosenzweig trusted him. So, once we had our wish list of security measures, Rosenzweig urged that we ask Kolar for a confidential assessment: Would the Eastern Europeans be able to accept these measures as the price for VWP?

They met one afternoon at the Starbucks on New Mexico Avenue, near the department's headquarters. With him, Rosenzweig brought our wish list of security requirements.

Kolar took the draft list away with him. A few days later he called Rosenzweig to tell him that by and large the security requests were feasible; no promises, but they could form the basis for substantive discussion. We knew that we were in shouting distance of a successful negotiation.

But we knew that our hardest international talks didn't take place overseas. Once again, the toughest negotiations would be inside the government.

We knew there would be no difficulty persuading the National Security Council or the other cabinet departments that the visa waiver program should be expanded. President Bush felt a deep connection to the newly independent Eastern European states that had backed his campaign against Saddam Hussein when older allies turned against him. The National Security Council would be on board.

The State Department, too, wanted to stop requiring visas in these states, both because they saw how it hurt our reputation and for a more practical reason. All those visa-processing consular officers took up valuable embassy office space and distracted ambassadorial attention from more interesting diplomatic issues. The Department of Defense would also be glad to do something for their brothers in arms.

Justice, too, would favor easing VWP standards. The department was used to supervising the immigration agencies, which had been part of its domain until 2003, and it was usually willing to sacrifice immigration interests to improve prosecutorial and law enforcement relations. Indeed, there were press reports that Justice and State had already slipped up to Capitol Hill to offer clandestine support to the Santorum bill—cutting DHS out of the process because they knew we'd never support a VWP expansion that did not improve security.

Everyone, in short, would be pleased to expand the VWP. That was the problem. At the level of bureaucratic interest, all the other players would be willing just to surrender to the exponential logic of international travel. But our job was to guarantee that the border failures of 9/11 wouldn't be repeated. We were alone in wanting to tie expansion to the new security measures.

That would be the battleground.

We had two advantages in the battle. The first was a short chain of command and superb top cover. Chertoff and Jackson were the smartest leadership duo in the cabinet. We briefed them, and they at once saw the logic of the principal security measures. We knew they'd back us up all the way.

The second was the rest of the team. Rosenzweig was committed to winning the fight against terrorism. Stout, balding, and ebullient,

he wore the bow ties favored by men who are proud of their quirks and independence. He was loyal, smart, and one of our fastest writers, a crucial skill in interagency fights where words are weapons.

He was too high-ranking to kick off the interagency scrum. For that I chose a young and talented lawyer who had already served at the Justice Department as well as in private practice. Nathan Sales was a thin, intense lawyer whose cowboy boots were a clue to his spirit. He was a fighter with a sharp mind. If he couldn't fight terrorists, I figured, he would gladly settle for fighting the National Security Council staff.

Sales drafted our proposal. Chertoff and Jackson blessed it. We took it to the interagency.

Unlike our PNR proposal, this initiative met with cautious interest rather than determined resistance. DHS had for so long simply said "no" to VWP expansion that the other players were delighted to hear us say, "Yes, but …" And, like good negotiators, they first wanted to pocket our "yes;" there'd be time enough later to water down our "but."

And that's how it went. As we negotiated over the precise nature of the legislation, time and again the National Security Council staff or the Justice Department would suggest that maybe we didn't need to include all the security measures. That could be left to Congress, they suggested. Or perhaps the security measures could just be "factors" for the administration to keep in mind while expanding the program. Anything but a clear, straightforward statement that the security measures were as crucial as the expansion. We had to fight for the security half of the package at every turn.

This was the highest of high-wire acts. Like a man on a tightrope, we had to keep the proposal balanced as we moved forward. Over and over again, from Sales to Chertoff, the DHS representatives insisted that we could not support expansion of the VWP without closing its security holes. I'd like to think that we were persuasive, but we also owed a lot to Senators Feinstein and Kyl. In the current climate, we said, this bipartisan pair would kill any proposal for expanding VWP unless we could show a net gain for security. Many senators, particularly the Homeland Security committee leaders, Senator Susan M.

Collins and Senator Joseph Lieberman, were skeptical about expansion but open to persuasion. Only if DHS could make a heartfelt security case for expansion would we be able to persuade the Homeland Security committee's leadership. And we wouldn't be persuasive if the interagency compromised away the security features of the plan.

Dan Fried, a wily lifer in the Foreign Service who had risen to become assistant secretary of state for Europe, was the first to realize that the game had changed. State had tried pushing a reluctant DHS into adopting individual "road maps" to VWP status for candidate countries; when that failed it had tried getting the same result from Congress without telling DHS. Nothing had worked.

Fried had served on the NSC and spent years in Poland, eventually rising to become U.S. ambassador there. He knew the region, he knew the issue, and he knew the Hill was deeply split between hardliners and expansionists. DHS's proposal to link expansion and security measures offered the first new idea after years of deadlock. Still, it was a hard idea to swallow—not least because of where it came from.

From the moment of its creation, DHS had been State's adversary. At the outset, State barely prevented Congress from transferring its consular service to the new department lock, stock, and barrel. And we were constantly complicating State's diplomacy, either demanding more of foreign nations on the security front or sending their most prominent citizens to hard-nosed secondary inspections at the border. Worse, DHS was still building its international capability, from nothing. The department's reputation for international follow-through was not good. Even if we were sincere, Fried wondered, could we deliver?

In the end, Fried decided to take a chance on the DHS proposal. Perhaps he figured that State could always step in if we stumbled. In any event, he agreed to the essence of the idea—legislation that would both set new security standards and relax the 3 percent refusal standard that stood in Eastern Europe's way.

Once State was on board, the way was clear, though both Justice and NSC kept trying to water down the security measures.

The president seized on a November 2006 trip to Estonia to announce that he was sending Congress a new approach to VWP expansion.

We were now launched on a very public high-wire act. The other end of the wire was far away. We needed legislation, followed by dozens of agreements, not to mention a new computer system. And we'd burned a year of the president's second term—a third of the time we had—just getting the interagency on board.

Actually, it was worse than that. During that year, the American people had gone to the polls. After four years when Republicans controlled both houses of Congress as well as the presidency, they'd had enough, electing Democratic majorities to both the Senate and the House. Now, campaigning for the Democratic presidential nomination also shifted into high gear. The outgoing President Bush had a whiff of lame duck about him. Anything on his legislative agenda was likely to get a cold shoulder and a slow walk.

This was going to be a squeaker.

VWP reform would require legislation. We knew that. But members of the executive branch are always wary of Congress. Football coach Woody Hayes, it is said, used to defend his conservative ground game with the aphorism, "There are three things that can happen when you throw a pass, and two of them are bad."

That's how we felt about going to Congress. If we asked for legislation, a lot of things could happen, and most of them were bad. We could lose, of course, but almost worse would be to get a win that upset the balance between security and expansion.

We had no choice, however, and no time. Early in January 2007, Rosenzweig and Sales went to the Hill to brief the Senate staff. We had legislative language and a rough consensus from the interagency on what should be in the bill. The early reaction was as good as we could hope. Senators Feinstein and Kyl were opposed, as expected, but the crucial Homeland Security leaders—Senators Lieberman and Collins—were open to the idea.

Then we got lucky. The new leadership of Congress announced that it was going to adopt legislation implementing the recommendations of the 9/11 Commission.

This was an odd thing to be doing in 2007. The commission had delivered its report in the middle of 2004. It had pressed for rapid and bipartisan implementation of its recommendations, and that's what it got. By December of that year, Congress had passed and the President had signed a law to implement the commission's recommendations. But the new House leadership wanted to dramatize its view that the first law was inadequate. A second bill implementing the 9/11 Commission recommendations was duly introduced with the coveted title of "House Resolution No. 1," signaling that it was a top priority in the new Congress.

Even better, the bill would go through the Homeland Security committees that we had already briefed on VWP reform. Maybe, we thought, we could hitch a ride on this powerful locomotive.

Our proposal was attracting bipartisan support. In the House, Rahm Emanuel had long favored expansion of the program. His district had a huge Polish-American population. As part of the new leadership he could provide crucial help. In the Senate, the cause was championed by Senator George Voinovich, a member of the Homeland Security committee.

There was just one problem with adding VWP reform to a bill implementing the 9/11 Commission's recommendations. The commission hadn't actually made any recommendations about the VWP. It hadn't even asked for the information sharing and other security measures we were adding to the program. But, we reasoned, it did express strong views about terrorist travel. So it wasn't too much of a stretch to suggest that maybe VWP reform ought to be part of the new legislation. Representative Emanuel, Senator Voinovich, and the Homeland Security committee's leaders agreed. Perhaps they thought it would give substance to a bill that was otherwise largely symbolic. Or perhaps they wanted to make sure that President Bush had a reason to sign the bill rather than vetoing it. Whatever the reason, all of a

sudden we found ourselves holding a ticket on the first legislative train out of the station.

Until then, we had been wary of the groups that were campaigning on the Hill for VWP expansion. We feared that they would cheerfully push for expansion without security. But once the administration's position took legislative form, it was their best hope. If anything showed the wisdom of our fight to include security measures as part of the President's package, this did. To be our allies, the expansionists had to offer at least some support for the security provisions. And they did. Energized and convinced at last that the United States was serious, Kolar and the other Eastern Europeans began mustering support from sympathetic ethnic constituencies. They made common cause with other VWP applicants (most notably the South Koreans) to expand their base, a tactical move that helped us win the support of Hawaii's tourist-conscious delegation.

It wasn't quite enough. Not everyone thought our security measures were sufficient. Senator Lieberman liked the ETA, but he didn't want VWP expanded until ETA applied to every VWP traveler. Senator Feinstein wasn't giving up either. She could see that the reforms would improve VWP security, but she wasn't satisfied that it did enough to prevent illegal immigration. That was a hot button issue in 2007. If she took to the floor to attack reform as a new avenue for illegal immigration, she might knock out the provision.

It was time to make a deal. To ease Senator Feinstein's concerns, we agreed to new conditions on expansion. No new countries would come in, we agreed, until the secretary certified that all the security measures were in operation—including the ETA. That would further reduce the time we had to get everything done, but it was good for security. If we left the hardest part of implementation to the new administration, they'd be lobbied endlessly to stall or drop the ETA. Unfortunately, when Congress drafted the provision, it inadvertently used language requiring that all our security measures had to be in place by October of 2008. Congress had cut three months from our already tight schedule.

We had a tougher time with Senator Feinstein and the immigration provisions. We didn't think that illegal immigration from Eastern Europe was that big a risk. Most Eastern Europeans could already work legally in places like the United Kingdom; how many would turn down legal work in Britain to live an underground life in the United States? But the committee was wary of the immigration issue, and of giving the executive too much discretion. Rather than dropping the 3 percent visa refusal requirement in exchange for security improvements, the committee decided that the 3 percent requirement could be waived—but only up to a maximum of 10 percent.

This was a tough blow. It meant that one of our strongest allies would be left out of the first round of expansion. Poland had gotten the reform movement rolling, and it was one of our best allies. But the refusal rate for Poles was still too high; they could not get under 10 percent before the end of President Bush's term.

The legislative train was moving; we had to take the deal if we wanted to stay on board. The tight timetable had claimed its first casualty.

And Senator Feinstein wasn't done. She had long believed that the United States should fingerprint everyone who leaves the country. If we tracked everyone who came in and everyone who left using their prints, she thought, then by process of subtraction, we'd also have the prints of people who came in but didn't leave when they were supposed to. Armed with that information, she thought, we could track them down and deport them. She insisted that we implement fingerprint exit monitoring, at least in airports, before we were allowed to expand VWP.

This was a deal killer. We weren't opposed to exit measures on principle, but identifying people on their way *out* of the country didn't have much to do with security. It was a bookkeeping measure. And it was based on a misunderstanding. First, we already had a paper-based system for recording departures. It could be better, of course, but it identified better than 90 percent of all departures. What's more, even if DHS had a dazzlingly accurate list of everyone who overstayed their visas, it didn't have anything like the resources to track down and

deport all of them. We had to set priorities. Terrorist risks and criminals were our top priorities, and we were already tracking them down using the paper system. On top of everything, the Feinstein system would be staggeringly slow and expensive to implement. We could never do it in the time remaining.

We said no. The senator insisted.

We were stuck.

Then, at the last moment, I got a call from the Homeland Security committee. Could we live with alternative language? The new language, drafted by a creative travel industry lobbyist, said that we would have to implement an exit system in airports by the middle of 2009; if we didn't, we couldn't expand the program. As I parsed it, that meant we could expand VWP until mid-2009, but the curtain would come down on additional expansion if we didn't implement air exit. That wasn't good, especially for countries like Poland that missed the first cut; and it would create a real headache for the next president, whose Homeland Security secretary would have to work overtime to get the air exit program in place by mid-2009. But in the near term, it would allow us to bring in most of Eastern Europe and set a new security standard.

Well, hell, I thought. We only had eighteen months left to get this job done. This was no time to be worrying about the next president's problems.

I took the offer.

So did the senator.

There would be no floor fight.

Despite Woody Hayes's dictum, we had put the ball in the air, and it had come down all right, battered but still recognizable. VWP reform became law in August 2007. It had gone from proposal to enactment in just eight months—a miraculously rapid legislative voyage. But we had no time to celebrate. We had only seventeen months left, and in that time we had to draft multiple standard security agreements, shunt the text through the interagency process, then bring home eight separate but simultaneous negotiations over the texts. It was a tall order.

But that wasn't all.

We also had to get the electronic approval system up and running before any country could be admitted. Designing, developing, field testing, deploying and operating a new computer program in seventeen months is well-nigh impossible. Especially for the government, which has to follow strict procurement procedures and must issue proposed and final regulations before it can actually put a program like this into effect.

Governments have a history of failure where big new computer systems are concerned. We all knew that. The managers may stay on schedule for months, then one day announce the discovery of flaws that will take months and millions to cure. Customs and Border Protection was the responsible agency, and it was better than most of the other DHS agencies at implementing programs, but that was no guarantee. I once compared the agency to a trophy wife—the implementation might be as good as you hoped, but the cost was likely to be far more than you could ever have imagined.

This time, we couldn't have any surprises. I put Kathy Kraninger in charge of overseeing the program. Kraninger is a blond wisp of a woman. She looks like the first strong breeze might waft her away. But she had brought order to the DHS credentialing programs with a combination of expertise, steely charm, and persistence that agency executives could not resist. She made an odd contrast to the burly men who dominated CBP, but she worked well with Paul Morris, the experienced program manager who oversaw the team of programmers and technicians who would build the ETA.

Morris and Kraninger had begun planning the system in the late spring of 2007, as our legislative hopes began to rise. Now with the passage of the 9/11 bill, they kicked the team into gear.

Soon, the programmers had a schedule showing that the system would be up and running by October 2008, but few of us were comforted. There were dozens of contingencies built into that schedule. If any problems arose, any at all, we were going to disappoint a lot of people very publicly: our allies and friends overseas, Secretary Chertoff, our colleagues at State and the NSC, and, most of all, the president.

Managing big government IT projects is hard, in part because the usual rules for fast government action don't apply. Usually, being able to get quick decisions from the top is an advantage, and top-level monitoring of progress is a good way to smooth the project's path. Not so with computer projects, where most of the problems come from contingencies that don't yield to the kind of help high officials can offer. Once launched, the program can't usually be speeded up by throwing more resources at it—putting nine women on the job, as they say, won't produce a baby in a month. All the top officials can do is count the contingencies and wake up in the middle of the night worrying about whether the technical managers can overcome them.

Actually, it's worse than that, because one of the keys to making progress on government computer programs is: Don't change the instructions you gave the programmers at the start. Unfortunately, the top decision makers in government are used to, well, making decisions. The more they learn about the project the more they want to decide its details. They don't like to hear that their good idea was overruled by design decisions reached four months earlier when a batch of low-ranking techs set the specs.

So when the National Security deputy adviser told me he wanted regular briefings on the progress the ETA was making, my job was a little tricky. I needed to reassure him without inviting the kind of help that turned into change orders.

I kept the briefings short.

I'd show up in his office, show him the timeline, and say, "We're still on track."

And we were. I just hoped he wouldn't ask how many contingencies were still open.

Then he wouldn't sleep any better than Kraninger or me.

While the programmers toiled in pressure-cooker anonymity, we were trying to deliver the international agreements on which we'd based our entire strategy. With somewhere between eight and ten candidate

countries and several agreements to be reached with each, just keeping track of the paper and the schedules would be a challenge.

My most experienced assistant secretary, Rich Barth, took point on the task. When I first met Barth in the early 1990s, both of us had other jobs. I was at the National Security Agency and he was a staffer at the NSC. I'd stayed in touch with him when he went off to be a senior executive at Motorola. Instead of the usual legal or liberal arts background, Barth brought a chemist's discipline to his work: problems were there to be solved, not admired. We'd lured him to DHS to manage the policy development process. For the delicate task of delivering all the deals in cooperation with the international office, Barth recruited Marc Frey, a young staffer who bore an uncanny resemblance to Clark Kent, minus the glasses.

Their task was complicated by the interagency process. As usual, negotiations with State and Justice were more difficult than with our foreign counterparts. To avoid squabbles over text, we first put forward a high-level memorandum of understanding on all of the security measures we wanted; it would be followed by a detailed set of agreements that would take longer to clear the interagency process.

To minimize conflicts and speed negotiations, we wanted all of the agreements to be as similar as possible. So Barth's team set out to nail down a standard-setting partner. Once again the Czechs were willing to lead the way. But the calendar was slipping away. Not until February 2008 did we get both the interagency and the Czechs to agree on a memorandum of understanding that could be a model agreement for the other countries.

We had eight months left.

And a lot still to do. After we signed the memorandum of understanding with the Czechs, we'd have to agree on the same principles with eight or nine more countries, and then negotiate the detailed agreements with all of them before October. With enough determination on both sides, though, we still reckoned that we could get it done.

We reckoned without Brussels.

As DHS's plan for a secure VWP unfolded, the European Commission had spent the winter quietly simmering. This was not the way it wanted events to unfold. The commission had told the Eastern European states to stand back and let it take the lead. It would use the combined might of European solidarity to force the United States to expand VWP—without any new security measures. That was its raison d'être, after all, and its business model. The first play in the Brussels playbook was, "Confront the United States with a United Europe; extract concessions that no one European country can obtain on its own."

Despite years of trying, that approach had gone nowhere. DHS had quietly turned aside the commission's demand for talks, saying that U.S. law required a separate evaluation of each country.

Worse, from the Brussels point of view, the Eastern Europeans seemed to be doing better on their own than the commission had been able to do on their behalf. Instead of invoking privacy to slow the U.S. initiative, they had readily agreed that sharing information about travelers would improve security on both sides of the Atlantic.

Now, with the signing of the Czech memorandum, visa-free travel was at last on the horizon. And it was met with something close to full-blown rage in Brussels.

For daring to take the initiative on VWP, the Czechs were pilloried. The commission's leaks to the press portrayed them as bad Europeans who were splitting the EU and delivering their citizens' personal data to the Americans. The commission publicly threatened to take the Czechs to court to punish them for their deviation, and the European Union summoned them to a meeting with the entire council for a tongue-lashing and a possible European repudiation of the memorandum of understanding.

The Czechs gave as good as they got. Asked to justify the decision to follow its national interests rather than the commission's wishes, Czech Interior Minister Ivan Langer could not have been more blunt.

"I am a free man, and not a slave of the commission," Langer told the press after one bruising confrontation in Brussels.[4] At DHS,

someone suggested having Langer's words printed up on T-shirts for the next U.S.-EU negotiating session on passenger name records.

Despite the leaks criticizing the Czechs for compromising European privacy, it was clear that the dispute ran deeper than that. Brussels and the new members had already lost patience with each other when DHS showed up with its proposal. A European Commission official once complained to me over wine that, "The Eastern Europeans are different. They're not like the other new member states. They just don't seem grateful that we let them in."

That wasn't inaccurate. After years under the Soviet boot, the Eastern Europeans treasured their sovereignty. In Western Europe, nationalism had been tainted by World War II. The surrender of sovereignty to Brussels could be cast as the key to avoiding a repeat of that conflict. In the East, nationalism was a secret flame that flickered behind the iron curtain until it could at last revive when the walls fell. Surrendering sovereignty to another distant capital had no great appeal for these newly freed nations.

From our perspective the European Commission's gambit was a disaster. We could not negotiate productively with the European Commission on these topics. European countries had widely varying practices where passports and airport security and information sharing were concerned. We couldn't ignore those differences, or U.S. law.

But there was more. The EU's unremitting campaign of privacy objections to U.S. policy on travel data had left a scar. DHS had no confidence that the commission would agree to cooperative arrangements or exchanges of information, even when U.S. lives were at stake. Quite the contrary. The leaks coming out of Brussels seemed to promise yet another effort to keep the United States from knowing more about the travelers who showed up at its borders.

DHS had learned its lesson from the PNR talks. We had productive, collegial relationships with the European interior ministers, who had the same interest in fighting terrorism as DHS. The commission did not. It had sown its combative approach to PNR, now it would reap ours to VWP.

Still, we were running out of time, and the whirlwind in Brussels was threatening to pull apart the entire strategy. The commission was trying to blow up the whole deal, or take over the talks, claiming that the Czechs had no authority to enter into the agreements we were seeking. It was getting backing from the countries at the core of the Union—France, Germany, Italy, and Benelux. The Czechs in turn were getting support from the East, even from countries that wouldn't be eligible this time around.

It was ugly. When the Czechs were summoned to Brussels the stakes were high. The commission wanted to take over the talks; and even if that gambit ultimately failed, the rancor could stall negotiations long enough to kill all hope of a deal.

Then Brussels overplayed its hand.

Determined to use the privacy weapon to punish the Czechs, it began suggesting that they had no authority to sign an agreement on sharing criminal information with the United States. Only Brussels could allow an agreement on that topic, commission staff argued.

This was a strike at the heart of our security strategy. To focus our enforcement on the riskiest travelers, we needed better access to foreign criminal records. Turning that agreement over to the commission would kill progress on a critical security issue. But the agreement was not something we made up for the Czechs. It was a carbon copy of the agreement that Secretary Chertoff had worked out with Wolfgang Schaeuble, Germany's interior minister. The deal had cemented their friendship with substance, and it was dear to both men's hearts. When we told our German counterparts that Brussels was playing the privacy card and questioning their landmark deal, they were visibly displeased.

That was the turning point. Not long after, the EU met in Brussels to decide whether to discipline the Czechs or let them go their own way. According to second hand reports, at the showdown meeting the German representative broke ranks with the commission. Without German support, the European Union could not muster a consensus to bring Eastern Europe to heel.

We offered an olive branch as well, agreeing to talk to the European Union on two topics—a small issue where it clearly had jurisdiction and, in a triumph of hope over experience, the sharing of EU enforcement data. The European Union did have some data on visa and refugee applications; finding ways to share information to reduce fraud would be good for both of us, we thought.

By the middle of March, when it was clear that the EU's power play had failed, it accepted our offer and then more or less dropped from sight. Despite several efforts on DHS's part, no progress was made on the issues ceded to the EU. Since none of them were central to our security concerns, the lack of progress was disappointing but would not stall reform. The only concrete result of the consultations was that we agreed to change the name of the system from ETA (which evoked the initials of a Basque terror group) to Electronic System of Travel Authorization, or ESTA.

We were back on track.

Except that now we only had seven months left.

And while we had been focused on the memorandum of understanding and the drama in Brussels, the interagency process was grinding toward gridlock over the detailed agreements.

With Brussels back on the sidelines, the candidate countries had quickly signed on to the memoranda of understanding. Now we needed to complete the detailed agreements that would define more particularly what information would be shared, in what manner and by whom. DHS wanted those protocols complete before the expansion took place. Only by negotiating detailed protocols could we avoid lingering disagreements and get enforceable commitments.

But now the Justice Department was balking. DHS had come up with the proposal for criminal data sharing because we needed the data for evaluating travelers. Justice was glad to share data with other countries. But it wanted to keep DHS from doing the same.

Its argument was a convoluted take on the principle of reciprocity—the notion that we shouldn't ask other countries to do things for us

that we wouldn't do for them. Justice claimed that under U.S. law, border inspections aren't always treated as law enforcement operations for purposes of disclosing criminal convictions. So Justice wouldn't always be able to give criminal conviction data to foreign border inspectors. For the sake of reciprocity, Justice argued, DHS border inspectors should be forbidden from getting criminal information from the authorities in other countries. This was laughable. Our allies weren't insisting on importing U.S. law into every aspect of the deal. All they wanted was a rough reciprocity that would give them information they actually needed.

I wondered again if some of Justice's fault finding and obstruction had a deeper cause. Until DHS came along, foreign interior ministers had only one counterpart in the United States—the Justice Department. But in some ways, DHS's role was closer to that of an interior minister than Justice's. As DHS expanded its contacts abroad, even when it used its contacts to help Justice, the Justice Department's international staff couldn't help but feel crowded. Perhaps its insistence that DHS was doing everything wrong was a natural reaction to the fear of losing turf. Certainly, cutting DHS out of criminal data exchanges would put Justice back at the center of the international law enforcement; we suspected that was a more potent motivator than some abstract notion of reciprocity.

Whatever the reason, Justice continued to insist that the criminal data-sharing agreement couldn't be executed as we'd written it. We tried arguing that Justice was wrong about U.S. law. It made no sense to read the law as denying criminal records to border officials, even for early screening decisions. But Justice insisted that its position was driven not just by law but also by concern for privacy and civil liberties. Prosecutors could use the data freely, of course; the FBI could use the data, too; hell, highway cops in every corner of the country could see the data every time they stopped someone with a broken taillight. But letting DHS use the data to screen travelers as they crossed the border—well, that raised serious privacy concerns. This was evidently a wall the prosecutors could live with.

The summer was nearly over. Rich Barth pressed me to yield. Justice must have thought that the ticking clock would bring us around—or that the buzzer would sound and we'd lose the deal entirely. The countries we were negotiating with had to see text right away. We were weeks from the deadline. Negotiations couldn't begin until we told our partners what we wanted. And we couldn't do that without an interagency agreement.

I was willing to take this one to the mat, though. Trying to isolate Justice, I called Dan Fried at the State Department. "Isn't this the deal you proposed three years ago?" he said to me. "You've done what you promised. There's no reason to change the rules now." We were still deadlocked, but Justice was the lone holdout.

Finally, the NSC took fright. It had always been more interested in VWP expansion than in the security improvements. Time was up. If the deadlock continued, NSC feared, expansion would be at risk.

The NSC staff set a deadline for DHS; if we didn't reach agreement with Justice right away, they would come down on Justice's side. In fact, they threatened to push VWP expansion through without the criminal information sharing protocols.

Close as we were to the finish, the tightrope walk was not over. We still might get visa expansion without adequate security.

But DHS still had one last advantage—short lines of communication. I walked down to Chertoff's office and briefed him on the NSC's threat. He understood the stakes. He refused to buckle. Under the new VWP law, he said, new nations could not be admitted to the program unless he personally certified that visa expansion would not jeopardize American security interests.

"There are a couple of people who can instruct me to make that certification," he told me, "but none of them are staffers at the National Security Council. And none of them are likely to think that the criminal data agreement should be dropped."

Told of the secretary's position, NSC blinked. They instead pushed Justice into a compromise. It was August by then, almost too late. But we had a free hand at last.

It was up to Barth and his team to deliver.

August slipped into September. The heat was on. We needed everything signed and sealed by mid-October. We broke our staff into teams so we could negotiate with several countries at the same time. One by one, our counterparts began signaling that we were close to a deal. But there were problems everywhere. Every country has different criminal procedures; different privacy rules; different requirements for approving international agreements. Some of the obstacles were substantive, some were procedural, but any of them could prevent us from signing the countries up by October.

In the end, two countries missed the deadline. Tiny Malta had trouble keeping up the pace—and had not been a negotiating priority. And Greece had booted its chances months earlier. It had failed to take the security provisions seriously, perhaps hoping that European solidarity would make a security agreement unnecessary.

The rest made it. Barely. On October 17, 2008, in a Rose Garden ceremony, President Bush announced the expansion of the Visa Waiver Program. He announced that effective November 17, citizens of Estonia, Latvia, Lithuania, the Czech Republic, Slovakia, Hungary, and South Korea would be allowed to travel to the United States without a visa. Malta was added a few weeks later. The Greek ambassador attended, glowering amid the smiles. It was the one sour note on a sweet day.

All we needed was a computer system.

One month later, on November 17, we turned on ESTA in test mode. Czech Deputy Prime Minister Alexandr Vondra and Interior Minister Ivan "Not-a-Slave-of-the-Commission" Langer flew on the first flight from Prague to New York. Barth and Kolar were proudly there to greet them as they got off the plane. A few days later, at a celebration marking Latvian Independence Day, the Latvian ambassador proudly announced that the violinist who was performing had arrived, visa-free under the new program, from Riga.

It looked as though we had made it to the end of the tightrope. Except for ESTA. In test mode, it could process a few dozen new

VWP travelers from Eastern Europe each day. Come January 2009, when the system went live it would have to apply to everyone traveling under the VWP program—twenty million of them a year.

And so, from November to January we waited with bated breath. Every day Kraninger would bring in the statistics on ESTA's performance. Every day we saw improvement. And glitches—problems in translation, problems in operation, and problems in decision making.

Day by day, CBP fixed the glitches and expanded the system. We started taking advanced ESTA applications from the other VWP countries that would be covered by the system in January. Meanwhile we ran stress tests on the system to assess its stability. All seemed to be ready.

Finally on January 12, we turned the switch and ESTA went live for everyone coming to the United States without a visa—more than 400,000 arrivals each week.

It worked. For the first time since the 1980s, American border officials knew who was coming to the United States in time to say "no" or to flag some travelers for closer scrutiny.

We were done.

Four working days later, President Bush was out of office, and so was I.

We could not have cut it finer.

8 Privacy Victims in the Air

If you've got to fly during the holidays, Christmas Day is as good as it gets. For a brief moment, the crowds drop off. Airports are almost peaceful. And if you start the day early in Europe, you can be in the United States in time for Christmas dinner.

Nearly three hundred passengers were taking advantage of that brief respite on December 25, 2009. Northwest flight 253 from Amsterdam to Detroit had been uneventful. No one thought anything about the young Nigerian complaining of a stomach bug; he had spent twenty minutes in the toilet and then covered himself with a blanket when he returned to his window seat in the middle of the plane.

The flight was well into its descent when Umar Abdulmutallab burst into smoke and flames. As the flames climbed the wall of the plane, and a brave Dutch passenger struggled with the man at the center of the fire, the passengers must have felt an unsettling sense of déjà vu. For the 2009 attack bore an eerie resemblance to another Christmas season attack eight years earlier.

It was another transatlantic flight, another al Qaeda terrorist from outside the Middle East, and another near miss. Once again, the solo terrorist had trouble triggering the explosive—in his underwear this time instead of his shoe. Once again, he didn't get a second chance, as passengers and crew subdued him and extinguished the flames.

Counting the "liquids plot" of August 2006, this was al Qaeda's third post-9/11 attempt to bring down transatlantic jets. The fixation on destroying transatlantic flights is reminiscent of an earlier fixation

on the World Trade Center. It's safe to assume that they'll keep trying until they succeed.

We'd known that for years. We'd revamped our entire Visa Waiver Program just to make it harder for European al Qaeda members to launch transatlantic attacks. Yet we hadn't managed to keep an al Qaeda operative and explosives off flight 253.

Why not?

As I write, detailed reviews of the incident are under way. But the basic facts are not in dispute, and they raise serious questions about our air security strategy.

Abdulmutallab began his journey in Ghana, flying first to Lagos and then to Amsterdam before transferring to flight 253. He had 80 grams (about three ounces) of plastic explosive sewn into his underwear and carried a syringe full of acid to use as a detonator. He passed through airport screening three times, attracting no special attention at any of the airports.

Abdulmutallab had only carry-on luggage for a purported two-week trip, and he'd paid cash for his round-trip ticket. None of that was deeply suspicious by itself. Cash purchases aren't as rare in Africa as they are in Europe or North America. And for anyone who's waited—and waited—for luggage at the end of a long flight, a traveler who can carry on the luggage he needs for a two-week stay is cause more for envy than for suspicion.

But there was plenty of reason to be suspicious of Abdulmutallab, and the information was already in the hands of the U.S. and UK governments.

Umar Abdulmutallab began his journey to Islamic terrorism where so many did. In Europe. While attending University College London, Abdulmutallab established communications with several dangerous Islamic radicals who were under surveillance by MI5, the UK domestic intelligence service. But MI5 evidently lacked the evidence and manpower to follow up. In the absence of a reason to believe that Abdulmutallab was an immediate threat, MI5 never put him

under surveillance. Worse yet, MI5 decided that privacy and politics required the agency to withhold information about Abdulmutallab from American agencies. As one British official told London's *Sunday Times*, "You can imagine the public fuss if they passed the Americans everything they had on all those who simply hold radical views."[1]

Indeed you can. This attitude permeated European thinking. It was the reason we had revised the VWP program to insist on greater information sharing about suspected terrorists from our counterparts in Europe. Unfortunately, even the British, with whom we had a relatively close counterterrorism relationship, had not agreed to a broad sharing of information about Islamic radicals—even foreign radicals—operating within their borders. In 2008, lacking any information from the British that might have spurred a deeper inquiry on terrorism grounds, the United States Embassy in London issued a two-year visa to the young man, whose wealthy father guaranteed that he would pose little immigration risk.

But it wasn't just our European allies who let us down. Our own government made plenty of errors as well. Abdulmutallab went on to study in Dubai and then Yemen, where he made the transition from radicalism to terrorism. He cut ties to his father, saying that he had found the true Islam and that, "You should just forget about me, I'm never coming back."[2] Alarmed, the father contacted the United States Embassy in Nigeria just five weeks before the attack, warning officials of his son's extreme views and presence in Yemen. In the end, he was interviewed by both consular officials and CIA officers, who prepared reports on the conversation but did not revoke Abdulmutallab's visa—perhaps because of an error in spelling his name.

They did enter Abdulmutallab's name into a lookout system in case he sought a visa in the future. Information on the Nigerian was also added to a 550,000-name classified database on terrorism suspects. But the information was not deemed sufficient to add Abdulmutallab to the formal Terrorist Screening Data Base, with its 400,000 names—let alone to the much smaller and more selective lists used to screen air passengers, the 4,000-name no-fly list or

the 16,000-name list of "selectees" who are always screened with care before being allowed on a plane. One reason for this decision was a failure to connect Abdulmutallab to a separate stream of intelligence suggesting that al Qaeda's Yemeni arm was planning attacks, perhaps involving a Nigerian operative.

Despite all these failures, our border security system seems to have worked. The Transportation Security Agency (TSA), which screens air passengers, had no clue that Abdulmutallab was a risky traveler, and so it did nothing special as he boarded flight 253. In contrast, Customs and Border Protection (CBP), the agency responsible for screening travelers at the border, had access to both the 400,000-name Terrorist Screening Data Base and the State Department's consular databases. It also very likely had information about Abdulmutallab's lack of baggage and his cash ticket purchase, both of which should have been included in his travel reservation data. According to press reports, this information had already led CBP to flag Abdulmutallab for secondary screening when the flight landed in Detroit. There, border agents could have inspected his passport and asked about his travel to Yemen and his father's concerns. It seems likely that, as a result of that screening, Abdulmutallab would have been turned away at the border. The information-centered screening process that we had built at the border, in short, seems to have worked as we hoped.

But a system that only works after a transatlantic flight has landed doesn't do much good if al Qaeda is trying to blow up the plane before it lands. Protecting the flight, as opposed to the border, is supposed to be TSA's job. If CBP can construct a workable screening system that uses all of the government's data, why didn't TSA have such a system eight years after 9/11?

The short answer is that TSA tried to build such a system and was rebuffed by a well-organized privacy campaign. In fact, during the years since 9/11, privacy lobbyists managed to stall a host of new air security measures. In particular, they forced TSA to postpone and largely neuter the kind of data-based screening system that has worked so well at the border.

They had help from history. Keeping weapons off planes was our central strategy for years—since the days of the Cuban hijackings in the 1960s. But it was obvious for years that that strategy was played out. Weapons kept getting smaller and their hiding places kept getting more imaginative and harder, or more embarrassing, to find. (The 80 grams of explosive that Abdulmutallab was carrying weighed a bit more than a hot dog, and a bit less than bra inserts that can change a B cup to a C.)

The focus on weapons had to change (about which more later), but at present searching for weapons is the system we have, and it needs improvement badly. As everyone now knows, we actually do have better ways to find small weapons hidden in embarrassing places. The millimeter-wave and backscatter machines that look beneath clothing are far preferable to a "pat-down" that probes everywhere that three ounces of explosives could be hidden. And, creepy as the scanners are, the privacy issues can be handled by making sure the images can't be stored or copied and the image screeners are nowhere near the people being screened.

TSA had been using these machines as an alternative to pat-downs in "secondary" screening for about a year. But most travelers don't trigger secondary scrutiny. Abdulmutallab didn't. If keeping weapons off the plane is our main line of defense—and it is—we need to screen everyone for the weapons Abdulmutallab was carrying.

So why don't we? After the attack, everyone was clamoring for the scanners, and the privacy groups seemed quite responsible on the subject. As Marc Rotenberg, head of the Electronic Privacy Information Center (EPIC), told the *New York Times*, his group "had not objected to the use of the devices, as long as they were designed not to store and record images."[3]

For an organization committed to staving off 1984, EPIC seems remarkably adept at dropping things down the memory hole. Just three months before claiming that it didn't want to prohibit whole body imaging, EPIC and nearly two dozen other privacy groups sent a letter to Congress saying that whole body imaging ought to be, well, prohibited.[4]

In fact, the groups said, DHS's Chief Privacy Officer had violated the law when she *failed* to prohibit TSA's new policy on whole body imaging. If the law had been followed, the groups said, "the new policy would not have been implemented in the first place."[5] Such screening, they declared, "is exactly the type of action that the Chief Privacy Officer should be preventing in satisfaction of her statutory obligations."[6]

For the privacy groups, it was just another day at the office. The coalition that signed the letter was by now a well-oiled machine. It had stalled many new security measures since 9/11. And as far as whole-body imaging was concerned, the privacy machine was on the brink of another success.

In June, a bipartisan majority of the House of Representatives had voted to prohibit TSA from using the machines for primary screening. With a three-to-one margin of victory, it was nearly inevitable that the restriction would have found its way into an appropriations bill or some other must-pass piece of legislation. If not for the inconvenient timing of the Christmas attack, another new security technology would have been taken off the table.

This wasn't a victory just for the left-leaning groups that have traditionally scoffed at a war on terrorism. The privacy coalition that nearly killed imaging also included the American Association of Small Property Owners and the Gun Owners of America, and they persuaded large numbers of conservatives to vote against the security interests of air travelers. The alliance reflects a kind of political circularity, in which the far left and the far right discover that they have more in common with each other than with the center.

But in a deeply divided Congress, where each side counts on its most vociferous supporters to turn out the vote, one way to achieve bipartisan action is to propose legislation that appeals to the fringe of each party. The ban on whole-body imaging was just such a proposal. Republicans and Democrats alike could claim a victory for their base. Republicans and Democrats alike were protected against partisan second-guessing in the event of an attack because the measure had support in both parties.

It is a magic combination that has worked for the privacy coalition for years, despite the fact that most Americans are far more concerned about effective security than privacy.

In fact, nothing illustrates the clout of the left-right privacy machine than a second failing demonstrated on Christmas Day, 2009. That is TSA's inability to use screening information that is routinely used by all the other security agencies in government.

The United States has pretty good information on four hundred thousand terrorism suspects, but fewer than twenty thousand of them are on the lists that TSA uses to screen air travelers. That means that 95 percent of the identified terrorist suspects can get on a plane bound for the United States without receiving any more scrutiny than a grandmother from Dubuque.

CBP knows about these four hundred thousand suspects. The FBI and CIA know about them. So does the State Department. But not TSA. For TSA, if you aren't on the no-fly or selectee lists, you're just regular folks.

Why? Because that's the way the privacy campaigners want it. It's the intended result of their remarkably successful effort first to stall and then to roll back the security reforms undertaken after 9/11.

There's a well-establish civil libertarian mythology about the nation's response to 9/11. In the myth, a frightened U.S. government throws civil liberties out the window within weeks of the attacks, launching a seven-year attack on our privacy that a new administration is only now slowly (too slowly, say the advocates) beginning to moderate.

In real life, privacy groups mobilized within weeks of 9/11, and they won victory after victory, right from the start. First, within a month of the attacks, they forced the Justice Department to negotiate the USA PATRIOT Act line by line with Chairman Leahy of the Judiciary committee—a process often ignored when the act is presented as a *fait accompli* imposed on a panicky Congress by the executive branch.

Then within eighteen months of the attacks, the privacy campaigners killed the TIPS program, designed to encourage citizens

to report suspicious behavior, as well as Admiral Poindexter's Total Information Awareness program.

After that, they went looking for bigger game. What they found was TSA, a gift that would keep on giving for half a decade.

DHS was brand-new in 2003. One of its priorities was to do exactly what the talking heads have been demanding in the wake of the Christmas Day attack. It wanted to transform TSA's screening system from one that looked mainly for weapons to one that looked for terrorists as well. The tool for doing that would be a second generation of the Computer Assisted Passenger Prescreening System, or CAPPS II. CAPPS II would process passengers' travel reservations to identify possible terror suspects much earlier and screen them more carefully—both before they got to the checkpoint and while they were there.

Until 2003, because it lacked access to travel reservation data, TSA had relied on the airlines to do the screening. It sent over a list of names, and the airlines checked to see if anyone with that name had made a reservation. If the person was on the no-fly list, the airline refused to give him a boarding pass. If he was on a selectee list, his boarding pass was marked so that screeners could single him out for additional screening.

That system was deeply unsatisfactory for many reasons, particularly as information sharing took hold, and a consolidated list of terrorism suspects was assembled from the many separate databases that existed before 9/11. Once these names had been assembled, the list was long and sensitive. No one wanted to trust unknown airline personnel with the crown jewels of U.S. counterterrorism intelligence, so giving them the entire list was out of the question.

Plus, the airlines weren't that good at figuring out when they had a name that matched. They'd flag Abdulmutallab for screening if that was the name they received from the government. But not Abdul Mutallab. Or Abdulmuttallab. If even the U.S. government can't manage to match a misspelled Abdulmutallab to the real thing, it's asking too much to expect the airlines to do better. So, to make sure

that planes were not brought down by a typo, the government tried to supply all the likely variants and misspellings and aliases for every suspect's name.

But that created a new problem. Millions of Americans have names that resemble those on the list. Of course they have different addresses and birth dates, so a halfway decent computer system would not flag those people for scrutiny. The problem was that the many in the perennially bankrupt airline industry didn't have a halfway decent computer system, and they weren't eager to spend money upgrading their systems just to do the government's screening job for it.

So in 2003, DHS proposed to take over the processing of the list. The idea was straightforward. TSA would collect reservation data from the airlines and run its terror suspect lists against the reservations. The reservation data would help resolve ambiguities where two people had similar names. It would also provide new security capabilities, allowing TSA to identify connections between suspects that were on its list and previously unknown passengers who shared addresses or phone numbers with the suspects and who might be conspiring with them.

In short, it would create the one tool that could have stopped the attacks of 9/11. It would give security officials quick and easy access to domestic travel reservations. If they'd had that in August of 2001, officials could have first located the two known al Qaeda operatives and then spotted most of the others through links in their reservation information.

With that background, the new system must have seemed like a no-brainer to the leadership of DHS. But, fresh from their victories over TIPS and TIA, the privacy coalition had other ideas.

"This system threatens to create a permanent blacklisted underclass of Americans who cannot travel freely," an ACLU counsel told the Associated Press in February 2003.[7] Another 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," a swipe at Admiral Poindexter.[8]

By June 2003, the organization had filed suit to block the program. By August, a left-right privacy coalition was lobbying against it. And by September, just two years after 9/11, the privacy groups had won. Congressional appropriators stopped the program dead in its tracks, prohibiting implementation of any such program until the General Accountability Office (GAO) certified that ten strict conditions had been met.

DHS spent the next five years trying to meet those requirements. Finally, in late 2008, DHS announced that it was launching Secure Flight, a pale imitation of the original program that gave TSA access to no traveler information other than name, gender, and birth date.

Even then, GAO demonstrated that it had learned the facts of life in Washington—you can't go wrong overestimating the clout of the privacy lobby. Knowing that it would never be criticized for refusing to certify compliance, GAO declared that TSA had met only nine out of ten requirements and let the appropriators deem that sufficient to begin Secure Flight. To its credit, the Obama administration did not treat that as an excuse to delay the program; it continued to roll out Secure Flight in 2009.

But if you've wondered why, eight years after 9/11, we're still looking for weapons and not for terrorists, now you know. Privacy advocates turned the use of even ordinary data like travel reservations into the policy equivalent of a toxic waste site. No one wanted to go anywhere near it, and those who did rarely survived the experience.

Remarkably, that wasn't all. The episode turned out to be far worse for security and far better for the privacy campaigners than even they could have hoped. Because as long as Secure Flight was stalled, we were all stuck with the old system of sending lists to airlines and living with whatever their creaking computer systems dished up. Most of the airlines couldn't tell Senator Stevens's wife, Catherine, from the singer formerly known as Cat Stevens, a reported apologist for the fatwa against Salman Rushdie.

As the lists grew and Secure Flight languished, you might have thought that the privacy groups and the airlines would start to take

some heat. After all, their opposition was the reason that so many people were being hassled for no good reason. But they didn't feel any heat at all. Quite the reverse. In an unexpected bonus, the blame fell entirely on the agency that had tried to fix the problem years earlier.

That must have been deeply satisfying. The privacy machine had created a vicious cycle. As long as Secure Flight was stalled, administering even a small no-fly and selectee list was painfully difficult—and a massive inconvenience for travelers whose names resembled those on the no-fly and selectee lists. Even better, TSA took all the blame, thus discrediting both the idea of screening for possible terrorists and an agency that no traveler was much disposed to love in any event. Every time TSA's reputation took a hit for mismatched names, it became easier for Congress and the privacy groups to argue that the agency couldn't be entrusted to administer a new program.

Better still, from the privacy groups' perspective, the millions of privacy victims created by the mismatched names became an excuse for rolling back other security measures, including the terrorist watch-list. In 2008, when TSA began to get close to meeting the Congressional requirements for Secure Flight, Barry Steinhardt of the ACLU held a news conference to announce that the watch-list had reached one million names (he was wrong, but the coverage was good anyway). "The list is out of control," he said. "There cannot possibly be one million terrorists threatening and poised to attack us. If there were, our cities would be in ruins."[9]

And with a chutzpah rarely equaled in American policy circles, Steinhardt mourned "the tens of millions of Americans [who would now be] caught up in a Kafkaesque web of suspicion."[10]

He should know.

He had spun the web those Americans had been trapped in.

That brings us back to Christmas Day, 2009, and the question of why Abdulmutallab wasn't on a no-fly or selectee list, or for that matter why 95 percent of the terrorist suspects known to the U.S. government are treated like upstanding citizens when they get to the TSA checkpoint.

Imagine for a minute that you were a security official watching the ACLU press conference in 2008. You see that the organization got the number of names on the list wrong, trashed TSA for a problem they'd created themselves, and received fawning coverage for it. Do you really want to stick your head over the parapet and suggest a substantial expansion of lists that the ACLU says are already "out of control" and are victimizing tens of millions of Americans? Nope, in those circumstances, there wasn't much chance that standards for getting on the lists would be eased, or that TSA would soon get operational access to the other 95 percent of the database.

In the end when all is said and done, the investigations of the incident will find errors in how the agencies handled the lists and the screening. But when they do, for once we should skip the football analogies.

The errors weren't "fumbles" or "dropped balls." Instead, the most apt analogy comes from tennis.

Because if ever there were a "forced error" in policy making, this is it.

And as in tennis, full credit should go to the privacy advocates that forced it.