# SKATING ON STILTS

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

Stewart A. Baker

HOOVER INSTITUTION PRESS
Stanford University Stanford, California

# 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.

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

*www.hoover.org*

**Hoover Institution Press Publication No. 591**

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



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

Manufactured in the United States of America

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

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

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