SKATING ON STILTS

Why We Aren't Stopping Tomorrow's Terrorism

Stewart A. Baker

HOOVER INSTITUTION PRESS
Stanford University Stanford, California

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.

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)

Creative Commons Attribution-NoDerivs License