Bruce Schneier, Beyond Fear: Thinking Sensibly About Security in an Uncertain World (NY: Copernicus, 2003)

Almost all terrorist attacks are minor affairs, affecting only a few people. Airplane bombings are the traditional exception, causing millions of dollars' worth of damage; the attacks of 9/11 were also an anomaly. Most terrorist attacks don't cause much damage directly. The real damage is from the secondary effects: people being too scared to fly or take public transportation. And while it's easy to imagine a disaster scenario or movie plot involving a nuclear bomb in terrorist hands, the reality is much more mundane. These kinds of attacks are very difficult to pull off, and very unlikely.

There is a real risk of terrorism, but the situation is not nearly as dire as most people thought in the months directly after 9/11. International terrorists are trying to attack the U.S. and Western Europe (and their interests around the world), but they're rare and they've become rarer since governments started counterattacking and arresting terrorists before they strike. It's impossible to quantify the risk in any meaningful sense, but we can look back at the previous decades and see the trends. International terrorism happens, but it's much less common than conventional crime.

None of this discussion is meant to belittle or deny the risks—it's just to put them in perspective. In 2001, 3,029 people died in the U.S. from terrorism (the 9/11 attacks). During that same year, 156,005 people died from lung cancer, 71,252 from diabetes, 41,967 from motor vehicle accidents, and 3,433 from malnutrition. Consider what we're willing to spend per year to cure diabetes or increase automobile safety, and compare that with the $34 billion we're spending to combat terrorism. The response to the terrorism threat has not been commensurate with the risk.

The problem lies in the fact that the threat—the potential damage—is enormous. Security is all about trade-offs, but when the stakes are considered infinitely high, the whole equation gets thrown out of kilter. In the frightened aftermath of 9/11, people said things like: "The budget for homeland security should be infinite. The trade-offs we need to make *should* be extreme. There's no room for failure." It was easy to succumb to hysteria and scare-mongering and to overre-

Deadliest Terrorist Strikes in the U.S.

Date	Attack and Location	Fatalities
11 Sep 2001	Crashing of hijacked planes into World Trade Center, New York, NY, Pentagon in Alexandria, VA, and site in PA	3,029
19 Apr 1995	Truck bombing of Federal Building, Oklahoma City, OK	169
16 Sep 1920	Bombing near bank in New York, NY	34
1 Oct 1910	Bombing at newspaper building in Los Angeles, CA	21
29 Dec 1975	Bombing at airport in New York, NY	11
23 Jul 1916	Bombing at parade in San Francisco, CA	10
4 May 1886	Bombing at Haymarket Square rally in Chicago, IL	7
26 Feb 1993	Truck bombing of World Trade Center, New York, NY	6

Significant Terrorist Acts Using Unconventional Weapons

Date	Attack and Location	Casualties
20 Mar 1995	Sarin nerve gas attack in Tokyo subway, Japan	12 killed, 5,511 injured
27 Jun 1994	Nerve gas attack in Matsumoto, Japan	7 killed, 270 injured
Sep–Oct 2001	Anthrax-laced letters to multiple locations in the U.S.	5 killed, 17 injured
19 Apr 1946	Cyanide poisoning in prison near Nuremberg, Germany	2,283 injured
15 Sep 1984	Salmonella poisoning in restaurants in The Dalles, OR, USA	751 injured
19 Apr 1995	Tear gas attack in Yokohama, Japan	400 injured

Source: "Worst Terrorist Strikes U.S. and Worldwide," compiled by Wm. Robert Johnston, used by his permission.

Deadliest Terrorist Strikes Worldwide

Date	Attack and Location	Fatalities
11 Sep 2001	Crashing of hijacked planes into World Trade Center, New York, NY, Pentagon in Alexandria, VA, and site in PA	3,029
23 Jun 1985	Midair bombing of Air India flight off Ireland, and attempted bombing of second flight	331
8 Aug 1998	Truck bombings of U.S. embassies in Kenya and Tanzania	303
23 Oct 1983	Truck bombings of U.S. Marine and French barracks, Lebanon	301
21 Dec 1988	Midair bombing of Pan Am flight over Scotland	270
12 Mar 1993	15 bombings in Bombay, India	257
12 Oct 2002	Car bombing outside nightclub in Kuta, Indonesia	202
19 Sep 1989	Midair bombing of French UTA flight in Chad	171
26 Oct 2002	Hostage taking and attempted rescue in theater in Moscow, Russia (includes 41 terrorists killed)	170
19 Apr 1995	Truck bombing of Federal Building, Oklahoma City, OK	169
16 Apr 1925	Bombing of cathedral in Sophia, Bulgaria	160
14 May 1985	Armed attack on crowds in Anuradhapura, Sri Lanka *	150
3 Aug 1990	Armed attack at two mosques in Kathankudy, Sri Lanka *	140
2 Oct 1990	Crash of hijacked PRC airliner in Guangzhou, China	132
23 Nov 1996	Crash of hijacked Ethiopian Air flight off Comoros	127
18 Apr 1987	Roadway ambush in Sri Lanka *	127
13 Sep 1999	Bombing of apartment building in Moscow, Russia	124
13 Aug 1990	Armed attack at mosque in Eravur, Sri Lanka *	122
29 Nov 1987	Midair bombing of Korean Air flight near Burma	115
23 Sep 1983	Midair bombing of Gulf Air flight over the UAE	112
22 Sep 1993	Crash of airliner struck by missile in nation of Georgia *	106
21 Apr 1987	Bombing of bus depot in Columbo, Sri Lanka *	106
4 Dec 1977	Crash of hijacked Malaysian airliner, Malaysia	100
25 May 1973	Midair bombing of Aeroflot airliner, Siberia	100
13 Dec 1921	Bombing of Bolgard palace in Bessarabia (modern Moldova)	100

Note: Items marked with an asterisk are not usually considered to be terrorist attacks.

Source: "Worst Terrorist Strikes U.S. and Worldwide," compiled by Wm. Robert Johnston, used by his permission.

act to the terrorist threat. In fact, one of the primary goals of terrorism is to create irrational terror far in excess of the actual risks. But this kind of talk is meaningless. When a country allocates an infinite budget to homeland security, the terrorists really have won.

Sensible security does not result from fear. Just because anomalies happen doesn't mean security has failed. The risk of a terrorist attack before 9/11 wasn't appreciably smaller than the risk of a terrorist attack after 9/11. Before 9/11, European countries mostly had an accurate assessment of their risks. In the U.S., the risks were largely underestimated; many people thought it couldn't happen there. But after 9/11, the risks in the U.S. suddenly became grossly overestimated. This situation has lessened somewhat, but the public perception of risk is still wildly out of proportion to the actual threat. The reality is that the risks are low; and even if some terrorist manages to set off a dirty nuke in the middle of a crowded city, the risks of an individual being affected by terrorism still won't change appreciably.

This is a precarious position to take politically, which is why I believe most politicians have steered clear of it. It's safe for a political leader to make dire predictions about the future and recommend an extreme course of action. If another terrorist attack happens, then she can say that the event proved her right. And if nothing happens, she can claim that her security program was a success. (And that it keeps away the vicious purple dragons, too.) A politician is on shaky ground when he says, "Don't worry; it's not that bad." He looks ineffectual compared to his colleagues who are trying to *do something* to make us safer (even if the "something" doesn't really make us safer); worse, he looks as if he doesn't care about his constituents. And if another attack happens, he looks even worse. The public's difficulty in assessing risks plays into this. Many people have been frightened into believing that terrorism is a far greater risk than it is. All sorts of incidents are immediately assumed to be terrorism, even though investigations prove other causes. And when the next terrorist attack occurs on U.S. soil, people, politicians, and the press will all exaggerate the risks of terrorism even more.

Here's the bottom line when you realistically and unemotionally assess the risk to your personal security of a terrorist attack: If you're don't live in a major coastal metropolitan city or next to a nuclear power plant or chemical factory, you're more likely to die of a bee sting than a terrorist attack. Even if you do live in a big city or next door to a power plant, the odds of being a terrorist victim are still vanishingly

small. Any precautions you take should be directed toward and in proportion to those risks.

Step 3: How well does the security solution mitigate those risks? There are exceptions, but most of the countermeasures put in place after 9/11 don't do a very good job of mitigating the risk of a terrorist attack. Many of the problems are inherent in the characteristics of the assets and the risks to those assets.

- Defending targets is hard. It's one thing to defend a military target—or even a military office building like the Pentagon—and quite another to defend the sorts of civilian targets that can be attacked. In military parlance, most of the assets we need to defend are known as soft targets: undefended nonmilitary sites. These targets are meant to be accessed all the time by all sorts of people; they have poorly defined perimeters, and they're generally situated in populated areas. These characteristics make them particularly hard to defend.
- Preventive countermeasures are largely ineffective because of the huge number of possible targets. Defenses that simply shift the attacks from one target to another are wasteful, although—as I said before—it is important to defend particular high-profile targets nonetheless.
- Detection and response is more effective than prevention. The notion of secure preventive barriers around many of these targets is simply nonsensical. There's simply no way to keep terrorists off buses, weapons off airplanes, or bombs out of crowded intersections. Far more effective is to detect terrorist attacks in the planning stages and to respond before damage can occur. Of course, doing this is very difficult, as well; most terrorist attacks happen too quickly for defenders to respond before the damage is done. Detection and response are more useful for mitigating the effects of an attack than they are for preventing it from happening.
- Benefit denial is a critical countermeasure. Morale is the most significant terrorist target. By refusing to be scared, by refusing to overreact, and by refusing to publicize terrorist attacks endlessly in the media, we limit the effectiveness of terrorist attacks. Through the long spate of IRA bombings in England and Northern Ireland in the 1970s and 1980s, the press understood that the terrorists *wanted* the British government to overreact, and praised their restraint. The U.S. press demonstrated no such understanding in

the months after 9/11 and made it easier for the U.S. government to overreact.

- Proactive countermeasures, such as advance detection and counterattack, are more effective than reaction. In general, reactive countermeasures are only a small part of the answer; we will never be able to stop terrorism solely by defending the targets. The only way to deal effectively with terrorists is to detect terrorist plots before they're implemented, then counterattack and go after the terrorists themselves: rolling up terrorist networks, disrupting funding streams and communications, and so on.
- Long-term countermeasures, such as deterrence and education, are the only real solution, and even they are imperfect. The best way to reduce terrorism is to solve the underlying socioeconomic and geopolitical problems that cause it to arise in the first place. This isn't absolute, but nothing in security is ever absolute. It is also extremely difficult, and some of the problems seem, and may be, impossible to solve. Deterrence has a place, as well, although it is unclear how effective it is against suicide terrorists.

To summarize: Prevention is impossible. Mitigation is important. Intelligence and counterattack are critical. And none of this is as effective as addressing the root causes of terrorism.

Authentication systems suffer when they are rarely used and when people aren't trained to use them. For example, if someone approaches you and says he's from the FBI, or Scotland Yard, or the Ministry of Defense, how do you verify that he is who he says he is? Do you know what one of their ID cards looks like? Could you identify a forgery? I know I couldn't. And there's a power imbalance; many people are reluctant to question a police officer because he might take offense and retaliate. Some years ago, a CIA agent approached me and wanted to ask me some questions. (No, I didn't help him. Yes, the CIA is going to be unhappy when agents read this paragraph.) I told him that before I would even believe that he was from the CIA, I wanted to see him at the CIA headquarters at Langley walking out of the turnstiles. I figured that if he could do that, he was legit.

Imagine you're on an airplane, and Man A starts attacking a flight attendant. Man B jumps out of his seat, announces that he's a sky marshal, and that he's taking control of the flight and the attacker. (Presumably, the rest of the plane has subdued Man A by now.) Man C then stands up and says: "Don't believe Man B. He's not a sky marshal. He's one of Man A's cohorts. I'm really the sky marshal."

What do you do? You could ask Man B for his sky marshal identification card, but how do you know what an authentic one looks like? If sky marshals travel completely incognito, perhaps neither the pilots nor the flight attendants know what a sky marshal identification card looks

like. It doesn't matter if the identification card is hard to forge if the person authenticating the credential doesn't have any idea what a real card looks like. Uniformed sky marshals would be much more secure against this kind of failure because the uniforms would be seen frequently. On the other hand, putting a sky marshal in uniform is like putting a huge bull's-eye on his chest. This is a classic security trade-off.

Perhaps the best solution is to require sky marshals to show their identification cards to the pilots and flight attendants whenever they board an airplane. Then, assuming the cards are hard to forge, this failure would not happen. If there were an identification dispute, the flight attendants could point to the authentic sky marshal. And since the flight attendants already have the trust of the passengers, they would have credibility. If the flight attendants are all incapacitated ... but I'm not going to go there. No system is ever foolproof.

Many authentication systems are even more informal. When someone knocks on your door wearing an electric company uniform, you assume she's there to read the meter. Similarly with deliverymen, service workers, and parking lot attendants. When I return my rental car, I don't think twice about giving the keys to someone wearing the correct color uniform. And how often do people inspect a police officer's badge? The potential for intimidation makes this security system even less effective.

Uniforms are easy to fake. In the wee hours of the morning on 18 March 1990, two men entered the Isabella Stuart Gardner Museum in Boston disguised as policemen. They duped the guards, tied them up, and proceeded to steal a dozen paintings by Rembrandt, Vermeer, Manet, and Degas, valued at $300 million. (Thirteen years later, the crime is still unsolved and the art is still missing.) During the Battle of the Bulge in World War II, groups of German commandos operated behind American lines. Dressed as American troops, they tried to deliver false orders to units in an effort to disrupt American plans. Hannibal used the same trick—to greater success—dressing up soldiers who were fluent in Latin in the uniforms of Roman officials and using them to open city gates.

Spies actually take advantage of this authentication problem when recruiting agents. They sometimes recruit a spy by pretending to be working for some third country. For example, a Russian agent working in the U.S. might not be able to convince an American to spy for Russia, but he can pretend to be working for France and might be able

to convince the person to spy for that country. This is called "false flag recruitment." How's the recruit going to authenticate the nationality of the person he's spying for?

Authenticating foreign currency has a similar failure. About fifteen years ago, I was in Burma and a street-corner currency changer tried to change old, worthless Burmese money for my American dollars. The only reason I wasn't taken is that earlier my bus driver had warned me of the scam. Otherwise, how would I know what real Burmese *kyat* looked like? Some Las Vegas taxi drivers give casino chips from defunct casinos as change to unsuspecting passengers. Familiarity is resilient; novelty breeds brittle security.

In 1975, Stephen Holcomb walked into a Traverse City, Michigan, bank with a German 100,000-mark note, printed in 1923. The foreign exchange teller dutifully cashed the note, and Holcomb walked out with $39,700 cash for an otherwise worthless piece of paper. And in 2002, someone used a fake $200 bill with a picture of George W. Bush on the front to buy a $2 item at a Dairy Queen in Kentucky. The clerk accepted the bill and even gave him his $198 in change.

In Chicago in 1997, someone spent French franc traveler's checks as if they were dollars. The store clerks dutifully inspected the traveler's checks to make sure they were authentic, but didn't think to check the type of currency. Since the French franc was worth about 17 cents back then, the attacker made a tidy profit. Another scam centered around substituting French francs for Swiss francs. Still another involved writing a check with the correct numerical dollar amount and a smaller amount in longhand. The person receiving the check probably just looks at the number, but the bank pays what the words say. All but the Dairy Queen story are examples of I'm Sorry attacks; even Holcomb might have gotten away with saying that he didn't know German history.

If someone doesn't know what characteristic of the object to authenticate, that's the weak link in the system: Nothing else matters. I have a friend who has, on almost every one of the many flights he has taken since 9/11, presented his homemade "Martian League" photo ID at airport security checkpoints—an ID that explicitly states that he is a "diplomatic official of an alien government." In the few instances when someone notices that he is not showing an official ID, they simply ask for a valid driver's license and allow him to board without a second glance. When he noticed that the gate agents were scrutinizing expiration dates on IDs, he simply made another version

of his Martian League card that included one.

Example: Face Scanning in Airports

The trade-offs for automatic face-scanning systems in airports are more complicated than their rates of active and passive failures. Let's go through the five steps.

Step 1: What assets are you trying to protect? We're trying to protect air travelers, and people in general, from terrorists.

Step 2: What are the risks to those assets? The risk is that a known terrorist will board an airplane. Even if he is boarding the plane without any ill intentions, he might have future terrorist plans, and we would like to identify, stop, and interrogate him.

Step 3: How well does the security solution mitigate those risks? Not well. There are about 600 million airplane passengers in the U.S. per year. Any system that has any hope of catching real terrorists will falsely accuse hundreds of thousands of innocent people per year. The system won't be trusted by the security screeners, and they'll most likely end up ignoring it.

Step 4: What other risks does the security solution cause? We have to secure the database of faces. If the database becomes public, then terrorists will know whether they're in the database and what their picture in it looks like, so they can modify their looks. Also, we need trusted people to manage the database. Anyone who is authorized to modify the database could add people in order to harass them or could remove people. We need to secure the process that designs, develops, and installs the system. We need to secure the operational system so that it can't be disabled while in use.

Step 5: What trade-offs does the security solution require? Money, first of all. This is a very expensive system to install, and an even more expensive one to administer and maintain. People need to be hired to respond to all those false alarms. Then there is the inconvenience and the invasions of privacy for all of those innocents flagged by the system, and the cost of lawsuits from those harassed or detained. What happens if someone is wrongfully included in the database? What rights of appeal does he have? It's up to society to decide if all of that is too great a price to pay to fly in this dangerous age.

A system like this is clearly not worth it. It costs too much, is much too intrusive, and provides minimal security in return. In fact, if a system forces guards to respond to false alarms constantly, it probably reduces security by occupying them with useless tasks and distracting their attention. All field trials for these kinds of systems have been failures, and the only major proponents of face-recognition systems are the companies that produce them. Their agenda is to convince everyone that the technology works, and to sell it.

Example: Biometric Access Control

The failure of automatic face scanning at airports doesn't mean that all biometrics are useless. Let's consider biometric access control—an example of biometrics being used as an authentication tool.

Step 1: What assets are you trying to protect? Whatever assets are behind the barrier being protected by this system.

Step 2: What are the risks to those assets? The risks are that unauthorized persons will get access to those assets.

Step 3: How well does the security solution mitigate those risks? Pretty well. A person identifies himself to an access-control system (generally with an access code), and we want the system to authenticate that he's really who he says he is. Some attacks can fool the systems—one Japanese researcher recently showed how to fool most commercial fingerprint readers with a fake gelatin finger, for example—but biometric technology is up to this task. Biometrics are convenient: no access codes to forget or keys to lose. The system needs to have good failure procedures for when someone legitimate is not recognized—perhaps she has a cut marring her fingerprint—but with that in place, it's a good solution.

Step 4: What other risks does the security solution cause? The system must be trusted. There must be a secure process to register people's biometrics when they are allowed access, to update their biometrics when their access fails for some reason, and to delete their biometrics when they're no longer allowed access. Other potential problems are that the biometric could be stolen or an attacker could create a false biometric to gain access to the system. Remember: Biometrics are unique identifiers but not secrets. Making this system as local as possible—not sending the biometric over the Internet, for example—will minimize this risk.

Step 5: What trade-offs does the security solution require? Money. Biometric authentication systems are considerably more expensive than "something he has" solutions. On the other hand, this solution is more secure than giving everyone a key (or even a code to a combination lock). And it's much cheaper than posting guards at all the doors.

In many situations, this trade-off is worth it. Biometrics would be an effective addition to airport security, for example. I can imagine airline and airport personnel such as pilots, flight attendants, ground crew, and maintenance workers using biometric readers to access restricted areas of the airport. They would swipe a card through a slot or enter a unique code into a terminal (identification), and then the biometric reader would authenticate them. That's two forms of authentication: the card or memorized code and the physical biometric.

The difference between a system like this and a system that tries to automatically spot terrorists in airports is the difference between identification and authentication. Face scanning in airports fails as an identification mechanism not because bio-

metrics don't work, but because of the huge number of false positives. Biometrics are an effective authentication tool but not, at this point, an effective identification tool.

Example: ID Checks in Airports and Office Buildings

About a year after 9/11, I visited a New York company. Its offices were in a large Midtown Manhattan building, and it had instituted some new security measures. Before I was allowed into the elevator area, the guard asked to see my ID and had me sign in. While I waited, I watched building employees wave their badges past a sensor. Each time it beeped securely, and they walked on.

Since 9/11, ID checks seem to be everywhere: in office buildings, at hotels, at conferences. Examining the countermeasure with the five-step process will shed some light on its efficacy.

Step 1: What assets are you trying to protect? The building and the people in it, by preventing anonymous people from getting into the building.

Step 2: What are the risks to those assets? Many and varied. Basically, we are worried that people might do mischief.

Step 3: How well does the security solution mitigate those risks? Given how easy it is to get a fake ID—hint: get a fake from another state or country; the guard is less likely to know what a real one looks like—and how inattentive the average guard is, not very well. I believe that you can get past the average guard with a fake corporate ID printed on a home computer and laminated at a nearby Kinko's, with a fake name and fictitious company. Even if you assume the guards are more on the ball, most high school students can tell you where to get a fake ID good enough to fool a bartender. And what happens if a person does not have ID? Does the guard keep him out? Does someone inside the building vouch for him?

Step 4: What other security risks does the security solution cause? The security problem I would be primarily concerned about is the false sense of security this countermeasure brings. If the guards are supposedly stopping the villains in the lobby, then everyone in the building must be trustworthy, right? Even the guards may be more likely to ignore their own intuition and what's going on around them, because they're too busy checking IDs. Bad security can be worse than no security, because people expect it to be effective, and consequently they tend to let down their guard.

Step 5: What trade-offs does the solution require? Outfitting everyone working in the building with an ID card can't be cheap, and some office has to take on the job of issuing IDs to new employees, confiscating IDs from departing employees, and replacing lost cards—all activities fraught with their own potential security problems. Then there's the fact that electronic readers must be acquired and maintained. There's the inconvenience to visitors. And there's the continuing erosion of personal freedom.

By this analysis, the countermeasure is not worth it. Individual offices have always authenticated people to the extent they needed to, using receptionists, locks

on office doors, alarm systems, and so on. An additional centralized ID-checking system is security theater at its finest.

ID checks at airports are no more effective, but I can explain why they exist: It's the agenda of the airlines. The real point of photo ID requirements is to prevent people from reselling nonrefundable tickets. Such tickets used to be advertised regularly in newspaper classifieds. An ad might read: "Round trip, Boston to Chicago, 11/22–11/30, female, $50." Since the airlines didn't check IDs and could observe gender, any female could buy the ticket and fly the route. Now that won't work. Under the guise of a step to help prevent terrorism, the airlines solved a business problem of their own and passed the blame for the solution on to FAA security requirements.

Ironically, in the two years since 9/11, we've got the security level mostly right but the costs wildly wrong. The security we're getting against terrorism is largely ineffective, although it's probably commensurate with the minimal level of risk that actually exists. But it comes at an enormous expense, both monetarily and in loss of privacy.

To understand why people were willing to give up their privacy to attain a feeling of security, regardless of how effective that security actually was, you need to recall the general mind-set in the months after 9/11. In the aftermath of the mind-numbing shock and horror, people needed to do something immediate, and invasive countermeasures seemed the easiest solution. Many Americans declared themselves willing to give up privacy and other civil liberties in the name of security. They declared it so loudly that this trade-off now seems to be a *fait accompli*. Pundit after pundit has talked about the balance between privacy and security, discussing whether various increases of security are worth the privacy and civil liberty losses. This discussion seems odd to me, because linking the two is just plain wrong.

Security and privacy, or security and liberty, are not two sides of a teeter-totter. This association is both simplistic and misleading. Security is always a trade-off, yes, but privacy and liberty are not always the things traded off. It's easy and fast, but not very cost-effective, to increase security by taking away privacy. However, the best ways to increase security are not necessarily at the expense of privacy or liberty. Use airline security as an example: Arming pilots, reinforcing cockpit doors, and teaching flight attendants karate are all examples of security measures that have no effect on individual privacy or liberties. Other effective countermeasures might be better authentication of airport maintenance workers, panic buttons and automatic controls that force planes to land automatically at the closest airport, and armed air marshals traveling on flights.

And privacy- or liberty-reducing countermeasures often require the most onerous trade-offs. At this writing, the U.S. has arrested about a thousand people and is holding them incommunicado, without allowing them trials or hearings or, in many cases, access to an attorney. It's likely that among these people are a few would-be terrorists, and keeping them in jail has probably been pretty effective at preventing further terrorist attacks. But the cost—arresting a thousand innocent people—has been enormous.

Lack of planning is why we saw so much liberty-depriving security directly after 9/11. Most of the assets that had to be defended were not designed or built with security in mind. Our leaders had an extreme reaction driven by a grave perceived risk, and they wanted a lot more security—quickly. People in power were asked "What do you need to fight a war on terror?" There was no time to think through security and choose countermeasures based on their effectiveness and

trade-offs. Nearly all the proposals were things that the FBI, the CIA, and various factions within the administration had been wanting for a long time. "Give us more money" and "Give us more power" were natural answers that required very little detailed analysis.

That analysis needed to come from outside the FBI, and outside the administration, but no one was willing to do it so soon after 9/11. The most politically expedient option was to slap highly invasive and expensive countermeasures on top of existing systems. At the same time, people wanted to be reassured, responding more to the feeling of security than to the reality; and because they were driven by fear, they accepted countermeasures that required extreme trade-offs. People felt that they must be getting *something* because they were giving up so much.

That was two years ago, though, and it's about time we replaced these invasive systems with good security that mitigates the real threats while minimizing the necessary trade-offs. It's about time we made sensible security trade-offs.

• • • •

Which brings us to the Department of Homeland Security. According to its own writings, the "mission of the Department of Homeland Security is to: (1) prevent terrorist attacks within the U.S.; (2) reduce America's vulnerability to terrorism; and (3) minimize the damage and recover from attacks that do occur." The most heartening thing about this mission statement is the third item: the open admission that absolute success is impossible and that there are limits on the department's preventive abilities.

Unfortunately, the Department of Homeland Security is far more likely to increase the country's vulnerability to terrorism. Centralizing security responsibilities will create a commonality of approach and a uniformity of thinking; security will become more brittle. Unless the new department distributes security responsibility even as it centralizes coordination, it won't improve the nation's security.