Testimony of Jim Harper

Director of Information Policy Studies

The Cato Institute

at the Hearing Entitled

"The Promise of Registered Traveler"

Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity

Committee on Homeland Security

U.S. House of Representatives

June 9, 2005

Executive Summary

Registered Traveler seeks to overcome the delay at airports, a tax on travelers time, by increasing the amount of personal information and privacy that travelers "pay" – information that is used to investigate and pre-clear them for travel.

There are merits to the Orlando pilot, which will use a privately issued identification card. Private card issuers make privacy promises that are legally enforceable, which no government program has done, or can do. The "Clear" card to be used in Orlando particularly promises to dispose of data about travelers' movements, which is a notable anti-surveillance feature. Uniform identification systems are harmful to interests like privacy, autonomy, and liberty, so the emergence of a private identification system like this is welcome.

The TSA should avoid inadvertently picking winners and losers. It should open private card issuance to competition, which will tend to drive down prices and increase the appeal of the system to consumers. Also, if Registered Traveler is expanded, the TSA should select airports based on neutral standards.

There are problems with Registered Traveler. It is unseemly to have government agents associated with segregating "preferred" travelers from others. The Registered Traveler program essentially denies fairness, due process, and privacy protections to volunteers. And the "voluntariness" of the program could disappear at any time. Because it is a government program, no promise about it being optional can be assured.

The problems with Registered Travel are premised on the error in having government provide security services to the air transportation industry. There are emotional and political justifications for it, but there is no principled, security-based, or economic rationale for providing a massive security subsidy to airlines.

The government checkpoints that Americans must pass through in order to travel are an affront to American freedom and civil liberties. They require travelers to submit to government search and seizure based on no suspicion and to show papers in order to exercise the important liberty interest of traveling within their own country.

Identification-based security is intuitive but deeply flawed as a protection against terrorism. Private responsibility for airline safety would better secure us against the threat of terrorism, using all the tools that our free society has at its disposal.

Chairman Lungren, Ranking Member Sanchez, and Members of the Subcommittee –

Thank you for examining the Registered Traveler program through today's hearing. I appreciate the opportunity to share my views with you.

I am Director of Information Policy Studies at The Cato Institute. The Cato Institute promotes fundamental American principles of limited government, individual liberty, free markets, and peace. The Jeffersonian philosophy that animates Cato is often called "libertarianism" or "market liberalism." It combines an appreciation for entrepreneurship, the market process, and lower taxes with strict respect for civil liberties, and skepticism about the benefits of both the welfare state and foreign military adventurism.

At Cato, I study, write, and speak about the difficult challenges of adapting law and policy to the unique problems of the Information Age. My areas of study include privacy, data security, identification, surveillance, and cybersecurity, as well as intellectual property, telecommunications, and Internet governance.

I am also the Editor of *Privacilla.org,* a Web-based think-tank devoted exclusively to privacy. On the Privacilla site, there are hundreds of pages of material about privacy, including book reviews and discussions of privacy fundamentals, privacy from government, and topics such as online privacy, financial privacy, and medical privacy.

Recently, I was appointed by the Secretary of the Department of Homeland Security to serve as a member of the Department's Data Privacy and Integrity Advisory Committee. This group is constituted to advise the Secretary and the DHS Chief Privacy Officer on programmatic, policy, operational, administrative, and technological issues within DHS that affect individual privacy, as well as data integrity, data interoperability and other privacy-related issues.

The Privacy Advisory Committee will have its second meeting in Boston next week. We are only beginning our work and deliberations so nothing in my testimony, oral or written, reflects the views of the Privacy Advisory Committee or any other member of the Committee. I am confident, however, that the Privacy Advisory Committee appreciates the attention being paid us by Members of Congress. Mr. Thompson, the Ranking Member of the full Homeland Security Committee and an *ex-officio* Member of this Subcommittee, was good enough to come speak to our first meeting in early April, as did Mr. Cannon of Utah, who serves on the Judiciary and Government Reform Committees.

I am currently writing a book on identification called IDENTITY CRISIS: HOW IDENTIFICATION IS OVERUSED AND MISUNDERSTOOD. It is slated for publication early next year and will address many of the issues in current airline security programs on at least a theoretical level.

In my testimony below, I have first done what I can to highlight the good elements of the Registered Traveler program. I have many reservations about Registered Traveler, which I address second. My deep misgivings about the entire system that Registered Traveler tries to fix come last, but please consider these equally as carefully. Their position at the end of my testimony should not suggest that they are my least important contribution. Indeed, they are probably the most important.

Though I am highly concerned with, and critical of, our current approach to airline security, I acknowledge without reservation that the people working on these policies at the Department of Homeland Security and the Transportation Security Administration do so in good faith, with the best interests of our country, its people, and our tradition of freedom in their hearts.

Registered Traveler Summarized

Like the beneficent motives of the people at DHS and TSA, there is no doubt about the good intentions behind the Registered Traveler program. Some relief from the uncertainty and delay for travelers at airports is certainly in order. Anything that will restore our air transportation system to better functioning is a welcome effort.

Registered Traveler amounts to the following "deal" for air travelers: If you submit information to the government and pass a background investigation (also paying a fee in some cases), you will be given slightly less inspection, on average, at airport checkpoints. Registered Travelers will generally have their own lines at checkpoints and will not be subject to random secondary screening and other security measures in place for the general population.

Stated in different terms, the program works like this: Airport checkpoints now amount to a tax on travelers in two ways: in travelers' time and in their privacy/anonymity. Users of Registered Traveler will pay a privacy/anonymity fee by handing information over to the government (the fee, paid in lost privacy, is higher than the tax, because more

personal information is used), and a cash fee in some cases. In return, less of their time will be taxed away through waiting in lines at airports.[1]

People often trade privacy for convenience which is why some estimates of American travelers' participation are relatively high. Though there are many reasons for concern, there are interesting potential benefits from a version of Registered Traveler slated to begin soon in Orlando, Florida.

The Innovative Orlando Version: Privately Issued Identification

The Orlando version of Registered Traveler includes what I think is a fascinating and welcome innovation: the use of a privately issued identification card. The Greater Orlando Airport Authority has entered into an agreement with a private identification card issuer called Verified Identity Pass, Inc. This company will market, issue, and operate Orlando's Registered Traveler card under the brand name "Clear."

Clear will collect information from applicants for Registered Traveler, including fingerprints and iris images. These are highly accurate biometric identifiers that machines can read fairly well today. It will forward applicants' personal information to the TSA so that the TSA can investigate the applicants. (As discussed below, conditioning travel on government investigation is not okay, but my focus in this section is what is good in Registered Traveler.) Once the applicant has been approved by the TSA, the Clear card can be used to access airport concourses.

At the airport, the Clear member will place the card in a reader and allow his or her finger or iris to be scanned. The scan will be compared to the biometric information embedded in the card using an algorithm designed for matching these biometrics. Meanwhile, a unique identifier on the card will be compared to a database of members' identifiers. If the card information matches the person carrying it, and if the card identifier is on the list of approved cards, the Clear member will continue through the expedited Registered Traveler line.

---

[1] The plans of Verified Identity Pass, Inc., at the Orlando, Florida, airport are discussed in detail below. According to the Washington Post, the company expects to have 3.3 million customers for its "Clear" Registered Traveler identification card within six years at annual memberships fees of $100. This estimate holds that far in excess of 330 million dollars worth of consumer time each year is wasted by the wait times and uncertainty of wait times at airports.

Privately Issued Identification Cards are Good

Reading the privacy policy on the Verified Identity Pass Web site illustrates why privately issued identification is superior. It is for a reason that might be surprising: because the Verified Identity Pass privacy policy is a *contract*. It gives Clear members enforceable legal rights and it gives potential applicants information that they can rely on when deciding whether to use it. A private identification issuer like the Clear program submits itself to enforceable contractual terms and commits itself to future actions consistent with its contract.

Neither of these things is true of government privacy policies or the Privacy Act notices published routinely in the *Federal Register*. Privacy Act notices can be changed merely by a new publication. Congress and federal agencies can change the privacy commitments they have made, denying recourse to citizens, because these government entities are law*makers* not law subjects.

A program like the Orlando Registered Traveler, operated as it is by a private identification card issuer, can be much more protective of privacy than a government operated program, about which future privacy consequences cannot be predicted. And, as I discuss below, the Clear program is more protective of travel information than the government programs we have seen.

For years, the American Association of Motor Vehicle Administrators has been trying to build the role of Departments of Motor Vehicles in American life and commerce. They are among a small few who seem to recognize that identification is an important and useful economic and social tool. AAMVA and the DMV bureaucrats they represent are seeking to use the power of government to perpetuate the happenstance – the mere historical accident – that the most common and recognized identification services are provided by governments. It does not have to be this way, and it should not be this way.

Uniform Identification Systems Are Bad

In my forthcoming book, I summarize and build on the work of many scholars and advocates who have shown that uniform identification systems have significant negative consequences for important interests that Americans cherish, both as citizens and as consumers.

Uniform identification systems enable surveillance by both public and private entities. They are a tool that undermines the privacy and obscurity people enjoy every day. That

is, governments use uniform identification to watch and record the movements and actions of citizens, often contrary to their interests. Likewise, companies and marketers watch and study consumers. This is usually done for the purpose of improving customer service, product design, marketing, and so on, but many people object to it. They are free to do so and would be better able to prevent such monitoring if there were more choice among different identification systems.

Exacerbating the problem, the existence of uniform identification systems makes it easier for more institutions to demand identification than otherwise would. Most consumers accede to requests for identification when they check into hotels, enter buildings, and so on because it is easier to do so than to ask why or to refuse. For this reason, identification is becoming overused. It is often not actually necessary or useful for a transaction, but it gets added for marginal-to-nonexistent security reasons, or to create the impression of security. This kind of identification allows further surveillance. All private surveillance creates data that, in the current legal environment, government authorities may readily seize.

Uniform identification systems expose consumers and citizens to significant dangers. Our national identifier, the Social Security Number, and traditional second identifiers like the mother's maiden name are used too often by too many institutions. This makes identity fraud easier and more profitable. It means that a fraud on one identification system can multiply and by used in many systems, including security systems. If each institution used distinct identification mechanisms, identity fraud would drop in number and in both cost and consequence. (This measure is not without costs itself, of course.)

Likewise, uniform identification systems expose citizens to the risk of official confiscation. Currently, access to more and more goods, services, and infrastructure is being made contingent on showing a single identification, the driver's license. With this trend, there is an increasing risk that authorities may – legally or illegally – take away identification documents, effectively depriving people of their ability to function in society.

Most totalitarian governments in history have used uniform identification systems as a powerful administrative tool. Totalitarianism does not arise because of uniform identification, but uniform identification systems help totalitarian governments be that way. We are better off, and our freedom stands on stronger footing, if we have heterogeneous identification systems, including things like the Clear identification card.

Privately issued identification cards like the Clear card slated for use in Orlando will help create the heterogeneous identification system that we need in the United States. Though not entirely sufficient – not by a long shot – diversity of identification systems is one bulwark of liberty that will pay Americans enormous dividends in freedom and autonomy during the rapidly advancing digital age.

Private identification systems can put people, as both consumers and citizens, in a better position to control information about themselves. The alternative is massive, uncontrolled information sharing and data pooling that empowers governments and corporations over individuals.

Clear Under the Microscope

I have sung the praises of private identification cards like Clear, noting particularly that they are subject to law rather than the whim of lawmakers. This does not mean they are flawless. Along with some particular benefits, there are potential drawbacks to the Clear identification system, particularly in its interaction with the TSA program.

Foremost, the Clear system appears designed for resistance to surveillance of travelers' movements. This is an attractive feature, laid out in the privacy policy as a firm contract with members. Specifically, Verified Identity Pass tells us:

> For purposes of real-time maintenance and customer support (e.g., if your card doesn't work, we need to be able to run tests to understand why), we will maintain "log files" of entrances to local venues. However, we keep such records only at that location, we purge these records automatically every 24-48 hours, and we have designed our network so that neither Verified ID nor its subcontractors, including Lockheed Martin Corporation, can track and record Members' activities from location to location.

Assuming the Clear system works as stated – and if it does not Verified Identity Pass is on the hook for deceiving its customers – this is a tremendous anti-surveillance feature that has never been seen in government operated programs.

To the extent they revealed information in their Privacy Act notices, programs like CAPPS II and Secure Flight have been ambiguous about how long they would maintain information about Americans' travels in their records. Indeed, the Privacy Act notice for the Registered Traveler pilot, covering TSA's portion of the program, says that data will

be retained "in accordance with a schedule to be approved by the National Archives and Records Administration." This is both perfectly ambiguous *and* subject to change by a subsequent *Federal Register* notice, whether or not participants in Registered Traveler might object.

Clear's contractual promise to use a surveillance-resistant data destruction policy is a major improvement over the alternatives we have seen so far.

Clear's system is not unambiguously good. I note that they collect and store digital images of applicants' fingerprints and irises, apparently passing those on to the TSA as well. The data used to compare a Clear member with biometric data on a Clear card is not an image of the biometric itself but a sort of mathematical *description* of the biometric. Keeping a copy of fingerprint and iris images themselves may expose Clear members to future high-tech iterations of identity fraud if Verified Identity Pass' systems or TSA's systems are hacked or otherwise compromised. There is no obvious rationale for saving images of these biometrics or for sharing copies with the TSA.

Another concern is an apparent conflict between different sections of the Verified Identity Pass privacy policy. In section 5, it says it will comply with valid subpoenas, court orders, or other legal processes that require sharing of Member information with others. This suggests, without stating clearly enough, that it will share information *only* in these cases. In section 8(C), the policy says that Verified Identity Pass will share information "[i]f the government asks us" in cases when a member is removed from TSA's list of approved Registered Travelers. Loose wording in these two sections combine to create flimsy privacy protections against government entities for users of the Clear card.

Of greatest concern, of course, Clear passes identity and background information to the TSA, which is subject to none of the obligations in the Clear privacy policy. This problem arises from, and inheres in, government-provided security programs, discussed in detail below.

It is not for me to decide whether Clear provides adequate privacy-protective terms to prospective members. Privacy advocates, a watchdog press, the exposure brought by this Subcommittee's hearing, and many other actors and events will shape whether this product meets with the acceptance of consumers. Happily, though, these questions will be decided in a marketplace, where consumers have choices, as opposed to a government process where they do not.

Next, I will discuss how this marketplace can be improved.

Avoid Picking Winners and Losers

Too often with government programs and regulations, winners and losers are chosen through superior lobbying or luck rather than the merits of how well they serve consumers. In at least two respects, Registered Traveler, and the Orlando version of it, can be improved so that competition forces providers to serve consumers better.

Below, I will discuss the relatively large expense of Registered Traveler and Clear cards, particularly for people who travel rarely. This could create the impression of inequity – a class system – that carries the apparent approval and backing of the TSA. I have written above about concerns with the privacy terms offered by Verified Identity Pass to Clear users, though they are generally good. Competition can both lower the price and broaden the appeal of Registered Traveler, and potentially improve the privacy protections in private identification systems like Clear.

Registered Traveler should operate using uniform, neutral, and published (though, of course, secure) standards and protocols for biometric algorithms and for communication between cards and readers. This would enable other identification card issuers to enter the market, competing to serve Orlando customers and travelers at other airports as they come into the program. Uniform standards and protocols would also allow the identification cards used for Registered Traveler to be used in other settings such as office buildings.

Under the monopoly granted by the Orlando airport authority, Verified Identity Pass appears positioned to collect a relative windfall of $80 to $100 per customer per year, according to reports and the company's Web site, just for issuing the Clear card. (Some of this may go to the TSA to pay for investigations.) In the face of competition among identification card issuers, the price to the Orlando air traveler could drop quickly. Competitive identification card issuers would also likely pick at each others' privacy and anti-surveillance offerings and try to cater better to consumers' concerns, to the extent the TSA's terms allow them to do so.

Imagining further what might happen in a competitive environment, airlines might offer branded Registered Traveler cards to their customers for free to build loyalty. They may group cards with other concierge services for their best travelers. This is fine for private companies to do, though not for the government to affiliate itself with (as discussed

below). Other card issuers may seek the low end of the market and offer Registered Traveler cards as inexpensively as possible to the occasional vacation traveler.

There is a wide array of possibilities and I cannot predict how the market for identification services would take shape. None of these beneficial practices would overcome the deep flaws in the current government-provided air security system discussed below. The background investigations done by the TSA could and should also be competitively provided based on full permission from travelers. But, so long as this system exists, there are potential benefits to consumers and to society as a whole from a private identification market. These benefits should be harvested.

Likewise, if it expands Registered Traveler, TSA should offer the programs to airports based on neutral standards rather than superior lobbying and relationships. It should expand into markets rather than airports, so that one airport in a market is not given competitive advantage over another.

People often confuse free-market advocacy like mine with pro-business advocacy. In fact, unhampered markets are very tough on businesses because they force businesses into sharp competition with one another to serve consumers. Subjecting the identification business to competition will help ensure that it is attractive to consumers and oriented to serve their interests, including privacy. Doing whatever is possible to prevent distortion of competition among airports should also be a goal of Registered Traveler.

Registered Traveler has some merits – in particular, the use of a privately issued identification card. It has plenty of demerits that must be considered as well.

Problems with Registered Traveler

Having sought the good from Registered Traveler, I now turn to the bad. There a variety of problems that attach to the program, some of which have been alluded to above. It is difficult to intermingle the government and private sector as closely as Registered Traveler does. In the final sections of my testimony I argue against that entire approach. What follows here is a discussion of several issues that arise from that policy as it manifests itself in Registered Traveler.

Inequity

Users of the Registered Traveler system to date have been invitees of the airlines and regular business travelers much more than average or occasional flyers. It appears that Registered Traveler will ultimately be funded by fees, and the version of Registered Traveler being adopted in Orlando will be based on an $80 annual fee. In light of the fees and inconvenience of joining the program, Registered Traveler will probably not be used by occasional travelers and travelers of limited means. Thus, Registered Traveler will have all the hallmarks of a benefit reserved for the wealthy.

It is discomforting that TSA agents will be actively involved in, and associated with, segregating "preferred" passengers from everybody else in the flying public. Airlines should be free to segment their customers, of course, and business travelers are certainly a valuable segment, but Registered Traveler appears likely to put the government's imprimatur on these divisions.

According to the Washington Post, Verified Identity Pass, the company that will be providing Clear cards for Orlando, will share 29% of the revenue with the airport authority and as much as 22.5% in succeeding years, as well as 2.5% of Clear's future nationwide revenue. This puts the airport authority in a position to benefit from moving travelers from the regular line into Registered Traveler.

The easiest way to do this is to maintain consistent long lines for non-Registered Travelers. Eliminating wait times and uncertainty for the general public would reduce the attraction of the Registered Traveler program and the airport could lose Clear revenues by doing so.

At the least, the Orlando airport's incentive structure will be clouded by this arrangement. The incentives created by the arrangement between Clear and the Orlando airport authority may exacerbate long lines and the sense of inequity created by the Registered Traveler program, a sense that will be inextricably linked to the TSA and U.S. government.

If airline security were handled by airlines themselves, of course, this problem would disappear. Some airlines specifically target the business segment and others target the low-fare traveler. Each could customize their security programs to meet the tastes and demands of their customers.

Fairness, Due Process, and Privacy

According to the Privacy Impact Assessment for the Registered Traveler program's pilot phase, applicants for the Registered Traveler program who are denied will not be given the opportunity to appeal or have other redress. As the program expands, a significant number of people may be unable to participate in Registered Traveler.

If the system goes forward without a full-fledged redress procedure, this will be at least unfair to many people. When government action affects property or important liberty interests, this triggers the requirements of the constitution's Due Process clause. Given the long-recognized liberty interest in travel, it is likely that denying people the right to participate in the Registered Traveler program without appeal or redress will violate Due Process. Attempting to participate in the program, but being denied, may mark a traveler for future difficulties when he or she attempts to fly.

This would be equally true in the Orlando version of the program, in which a private company would collect personal information from applicants, forward it to the government for the investigation, and deny an application based on the government findings. The interposition of a private company does not affect the constitutionality or fairness of denying applications without recourse.

There are many other interests that Registered Traveler denies to volunteers. Indeed, in a Federal Register notice published just yesterday, TSA exempted the system from many protections of the Privacy Act, including the right to an accounting of disclosures, the right to access one's records, and the requirement that information in a traveler's file be relevant and necessary to the TSA's statutory purpose.

Volunteers for the Registered Traveler program may be seeking better treatment at airports, but they may end up getting substantially worse treatment by their government.

Voluntariness

Speaking of volunteering, the Registered Traveler brochure on the Transportation Security Administration's Web site calls participation in the program "completely voluntary." This is true at the present time, of course, and nobody intends for Registered Traveler to be mandatory – just like no one intended the Social Security Number to be used for identification.

No one can predict the future and no one – lawmaker, bureaucrat, or seer – can say for certain that the Registered Traveler program would never become mandatory. Indeed, there is good reason to object to the program in its entirety simply because it builds a traveler surveillance infrastructure and conditions people to accept government investigation as a prerequisite for traveling within the United States. After some future attack on the United States with significant loss of life, Registered Traveler may quickly be extended in any number of directions and made mandatory – without regard to its real utility in terrorism prevention.

In addition to the possibility that registration might be mandated directly in the future, the "voluntariness" of Registered Traveler can be eroded by maintaining consistently bad, slow service in the non-Registered Traveler lines at airports. As discussed above, the Orlando airport will have mixed incentives under its arrangement with Verified Identity Pass. Were airports and the Transportation Security Administration to continually maintain sub-standard service in the standard passenger lanes, Registered Traveler could remain voluntary in the technical since while becoming practically mandatory if a traveler actually wants to get somewhere on an airplane.

The risk that Registered Traveler could become mandatory is grave.

Registered Traveler has some merits that I have featured above. A number of problems with the program exist. They are rooted in the provision of air security to the airlines by the government. This premise is a deep and fundamental flaw that I have reserved to the latter part of my testimony.

Providing Government Security Services to Private Industry is Error

Though I have done my best, the Registered Traveler program can not be discussed in isolation. The program is intimately bound up with the provision of government security services to the airline industry, at taxpayer expense. It is also premised on the existence of government checkpoints that condition Americans' access to travel, an important and long-recognized liberty interest. To travel by airplane today, one must submit to seizure and search by government officials and one must show identification to government officials as well.

Though there are plenty of emotional and political justifications for it, there is no principled security-based or economic rationale for it. Putting government in the private

security business opens the door to substantial incursions on civil liberties, which are occurring at airports daily.

The instinct to bring the full weight of the government into securing air travel is understandable. Attacks on air transportation have often had political motivations. The first recorded attack, in May 1930, saw Peruvian revolutionaries seizing a Pan American mail plane with the aim of dropping propaganda leaflets over Lima.

Hijackings and other terrorist acts often spur knee-jerk, and often wasteful or misdirected, responses. In that sense, terrorists often succeed at injuring their targets even when the direct effects of their actions may be small.

Because it is so important to understand this, I have attached to my testimony an article from the Fall, 2004 issue of *Regulation* magazine called "A False Sense of Insecurity?" In it, Ohio State University national security expert John Mueller shows that leadership in the fight against terror involves informing the public of the real risks from terrorist acts rather than just catering to public fears.

The rash of hijackings to and from Cuba in the late 1960s had obvious political motivations and consequences. A spate of eight hijackings in January 1969 brought the Federal Aviation Administration into the air security business with the creation of the Task Force on the Deterrence of Air Piracy. The Task Force developed a hijacker "profile" to be used along with magnetometers to screen passengers.

In the first few days of September 1970, two American planes, a Swiss plane, and a British plane were hijacked and destroyed with explosives on the ground in Jordan and Cairo. The perpetrators in the Popular Front for the Liberation of Palestine had an obvious political motive. They elicited a super-prompt response in the United States which was very unlikely to have been carefully calculated for optimal terrorism suppression. On September 11, 1970, just days after these bombings, President Richard Nixon rushed out a comprehensive anti-hijacking program that included a Federal marshal program. Since then, the federal government has had its hand in airline security, mandating various security practices and supplying guards at taxpayer expense to commercial passenger airlines.

The attacks of September 11th, 2001 – thirty-one years to the day from President Nixon's move to bring the government into commercial air security – horrified all Americans and filled us with anger and dread. Congress reacted to the provocation with natural protectiveness. The Aviation and Transportation Security Act, signed into law a little

more than two months after the attacks, increased the government's role in airline security even further.

This politically appealing response was not necessarily the best. Had the lines of authority for transportation security never been blurred by federal government involvement, the Al Qaeda killers planning the 9/11 attacks might have faced a heterogeneous and unpredictable security system operated by multiple airlines, each one motivated by the fact that their continuing operations relied on keeping their passengers safe and secure.

This is not to say that airlines with full responsibility for security would have had perfect anti-terror records or even would have defeated the 9/11 plot. The weaponization of planes – a destructive technique not seen since the kamikaze attacks by Japanese forces in World War II – was a risk that no institution, public or private, seems to have considered. At best, though, the responsibility for airline security was mixed on 9/11. Unclear responsibility tends to degrade results.

The situation got worse with the airline bail-out, creation of the victims' compensation fund, and creation of the Transportation Security Agency. These steps have contributed to "moral hazard" (in the lexicon of insurance economics) around terrorism prevention: Decision-makers in the companies that control most of America's important infrastructure have seen that *failing* to protect themselves from terrorist threats may result in substantial immediate subsidies, release from liability, and an ongoing government subsidy of their security operations. The fate that the airlines "suffered" after 9/11 was a substantial infusion of various kinds of corporate welfare.

Airport Checkpoints and Identification Requirements Are Suspect

With good intentions and for good reasons, the Registered Traveler program seeks to overcome flaws in the Transportation Security Administration's screening program. But it addresses only a narrow part of one flaw: the substantial time delay for travelers. There are many others.

Foremost, TSA screening areas are government checkpoints that may be unconstitutional and that are certainly defective policy. When government officials stop and inspect citizens and their belongings, these are Fourth Amendment searches and seizures which, according to the terms of that Amendment, must be reasonable.

Two lines of Supreme Court cases are relevant. In one line (*Terry v. Ohio*), authorities have some level of suspicion about particular people that they have stopped. This is clearly not applicable to TSA checkpoints at which government officials stop and search everyone. The other line addresses checkpoints – in which everyone passing through a particular area is seized, if briefly, based on no particular suspicion whatsoever.

The most recent case, *Indianapolis v. Edmond* (2000), struck down a checkpoint set up for general law enforcement purposes. The Supreme Court specifically declined to decide whether its decision applied to airports or government buildings.

The future case that addresses checkpoints at long-distance transportation centers will have high stakes on both sides if it squarely addresses whether exercising the liberty to travel can be conditioned by government officials on submitting to search and seizure. If suspicionless searches and seizures at airports are reasonable under the Fourth Amendment because of the substantial danger to the public involved, this limitless rationale will validate checkpoints wherever some gross crime could or does occur: shopping malls, tunnels, factories, subways and so on. This is a roadmap for terrorists who wish to sap our economic strength and the vitality of our free people.

Overlaying these issues is the question of government-mandated identification at checkpoints. The recent *Hiibel* case which validated the requirement that someone tell an officer his or her name tracks to the *Terry v. Ohio* Fourth Amendment cases because the subject in that case was under suspicion. Suspicionless identification requirements have not been tested in the courts. A prominent case called *Gilmore v. Gonzales* pending in the Ninth Circuit may reveal what law or regulation, if any, actually requires the showing of identification at TSA checkpoints, and whether such a law is constitutional.

The constitutional questions about checkpoints and government-mandated identification underscore important policy questions that deserve careful, rational consideration. The Fourth Amendment is a constitutional rule, but also a sensible policy guideline. Searching the 99.99% of Americans who are 110% in support of the United States against the terrorists may be a waste of resources and time. These resources might be better devoted to far more selective and particularized searching, developing human intelligence, following leads, and tracking down genuine suspects of crime, terrorism, and related conspiracies.

The theory of identification-based security has significant flaws. People tend to believe that knowing who a person is reduces that person as a threat. This is true in normal life because in normal life people who are known can be held accountable. Terrorists are not

accountable, however. They are willing to die. Capturing the identity of all who would board an airplane does nothing to thwart committed terrorists. Checking identification may prop up the mistaken feeling the general public has of being safer sitting next to someone who the government has "checked out." It is disrespectful folly to deceive the American people this way.

Checking identification for the purpose of comparing air travelers to lists of suspects or no-flyers is also deeply flawed and unlikely to interdict committed terrorist groups. An MIT study called "Carnival Booth: An Algorithm for Defeating the Computer-Assisted Passenger Screening System," has shown that terrorists can defeat screening programs. By traveling multiple times before carrying out an attack, terrorists can determine whether or not they are subject to special screening. Those who are not subject to screening can be assigned to act. Again, this brittle security policy provides a roadmap to terrorists.

If terror suspects are known, watch lists are analogous to placing wanted posters in Post Offices – *and then waiting for the criminals to go to the Post Office*. True terror suspects should be sought out, investigated, arrested, and prosecuted. Non-suspects should be free to travel.

Identification can have some role in suppressing the risks of terrorist attacks. There is probably a close, but imperfect inverse correlation between "depth" in the community – children, family, ownership, liberal education, etc. – and propensity to terrorism. Identification and investigation can reveal such background, but people have consistently rejected the background checks envisioned for CAPPS II and Secure Flight. Background checking should be a consensual service, provided by airports and airlines. Because the correlation is imperfect, of course, securing infrastructure against tools and methods of attack will always be needed. Searching for weapons or bombs should probably remain a part of the security practice in commercial aviation for the indefinite future.

This all presumes that weaponization of a plane remains a risk. It does not. Hardened cockpit doors have driven that risk down substantially. In fact, that risk was virtually eliminated by 9:57 a.m. on the morning of September 11, 2001. That was the time that the passengers on United 93 attacked the cockpit. They realized that the airline security system had failed them and cooperating with the hijackers would not save them. Indeed, it would take the lives of others. These passengers at least ensured that their flight would not be used as a giant bomb like the others. No joy comes from recounting this event, but it does illustrate the better result when security is provided by interested parties with a real stake in the outcome.

To do airline security best, it should be done by the airlines themselves, in ways that they find to best protect their, and their passengers', interests. They are the ones who have something on the line. In case that is a subject of doubt: no air carrier is insurable post-9/11, and thus no air carrier is operable, if it does not take precautions fully sufficient for the risks to passenger aviation we all now recognize.

Likewise, in a fully private system, every major investigative news operation would be poring over airline security and sneaking dangerous items onto planes so that they could report on airlines' failings. The threat this publicity would bring to passenger levels and revenues would put airlines in a security frenzy. Airline security would be better and more creatively tested by the nation's enterprising reporters under a private system than it is today in the monolithic government systems we are limping along with. The strongest tools our society has to fight terror are still lying on the ground, unused.

Airlines are not subject to constitutional limitations like the Fourth Amendment. Were airline security restored to private hands, the airlines could condition travel on search, identification, or whatever other measure they thought would protect their airplanes and passengers. They would implement these security practices in ways that nest with and balance passenger comfort and privacy, good customer service, profitability and all the other interests that businesses must serve in order to survive. Each passenger, informed by our watchdog press, could choose the airline which he or she believed to be most secure.

Despite my deep reservations about the current stance of airline security, I have endeavored to constructively highlight what is good and bad about the Registered Traveler program. The emergence of a privately issued identification system, subject to contractual obligations that protect privacy and resist travel surveillance, is a welcome innovation. Whether it will appeal to the public is an open question that has many facets. And whether Registered Traveler will or should survive is another question. Probably, it should go away as airlines retake responsibility for a security role that is properly theirs.

*How does the risk of terrorism measure up
against everyday dangers?*

A False Sense
of Insecurity?

By John Mueller
Ohio State University

ETERMINING HOW TO RESPOND TO
the terrorist challenge has become a
major public policy issue in the United
States over the last three years. It has
been discussed endlessly, many lives
have been changed, a couple of wars
have been waged, and huge sums of
money have been spent — often after little contemplation —
to deal with the problem.

Throughout all this, there is a perspective on terrorism that
has been very substantially ignored. It can be summarized,
somewhat crudely, as follows:

- Assessed in broad but reasonable context, terrorism
generally does not do much damage.

- The costs of terrorism very often are the result of
hasty, ill-considered, and overwrought reactions.

A sensible policy approach to the problem might be to stress
that any damage terrorists are able to accomplish likely can be
absorbed, however grimly. While judicious protective and
policing measures are sensible, extensive fear and anxiety over
what may at base prove to be a rather limited problem are mis-
placed, unjustified, and counterproductive.

TERRORISM'S DAMAGE

For all the attention it evokes, terrorism actually causes
rather little damage and the likelihood that any individual
will become a victim in most places is microscopic. Those
adept at hyperbole like to proclaim that we live in "the age
of terror." However, while obviously deeply tragic for those

directly involved, the number of people worldwide who die
as a result of international terrorism is generally only a few
hundred a year, tiny compared to the numbers who die in
most civil wars or from automobile accidents. In fact, in
almost all years, the total number of people worldwide who
die at the hands of international terrorists anywhere in the
world is not much more than the number who drown in
bathtubs in the United States.

Until 2001, far fewer Americans were killed in any group-
ing of years by all forms of international terrorism than were
killed by lightning, and almost none of those terrorist deaths
occurred within the United States itself. Even with the Sep-
tember 11 attacks included in the count, the number of
Americans killed by international terrorism since the late
1960s (which is when the State Department began counting)
is about the same as the number of Americans killed over the
same period by lightning, accident-causing deer, or severe
allergic reaction to peanuts.

Some of this is definitional. When terrorism becomes real-
ly extensive, we generally no longer call it terrorism, but war.
But Americans seem to be concerned mainly about random
terror, not sustained warfare. Moreover, even using an expan-
sive definition of terrorism and including domestic terrorism
in the mix, it is likely that far fewer people were killed by ter-
rorists in the entire world over the last 100 years than died in
any number of unnoticed civil wars during the century.

Obviously, this condition could change if international ter-
rorists are able to assemble sufficient weaponry or devise new
tactics to kill masses of people, and if they come to do so rou-
tinely. That, of course, is the central fear. As during the Cold
War, commentators are adept at spinning out elaborate dooms-
day and worst-case scenarios. However, although not impos-
sible, it would take massive efforts and even more stupendous
luck for terrorists regularly to visit substantial destruction upon
the United States.

John Mueller holds the Woody Hayes Chair of National Security Studies at the Mershon
Center at Ohio State University. His most recent book, *The Remnants of War,* has just
been published by Cornell University Press. He may be contacted by e-mail at
bbbb@osu.edu.

HISTORICAL RECORD It should be kept in mind that September 11 continues to stand out as an extreme event. Until then, and since then, no more than 329 people have ever been killed in a single terrorist attack (in a 1985 Air India explosion). And extreme events often remain exactly that — aberrations, rather than harbingers.

A bomb planted in a piece of checked luggage was responsible for the explosion that caused a Pan Am jet to crash into Lockerbie, Scotland in 1988, killing 270 people. Since that time, hundreds of billions of pieces of luggage have been transported on American carriers and none have exploded to down an aircraft. (And millions of passengers who checked bags at hotels and retrieved them before heading to the airport have routinely lied to airline agents when answering the obligatory question about whether their luggage had at all times been in their possession.) This does not mean that one should cease worrying about luggage on airlines, but it does suggest that extreme events do not necessarily assure repetition any more than Timothy McVeigh's Oklahoma City bombing of 1995 has.

Since its alarming release of poison gas in the Tokyo subway in 1995, the apocalyptic group Aum Shinrikyo appears to have abandoned the terrorism business and its example has

sequent punishment. And terrorism likely will never go away completely; it has always existed and presumably always will.

A central issue, however, is whether such spectacularly destructive terrorist acts will become commonplace. Although there have been many deadly terrorist incidents in the world since 2001, all (thus far, at least) have relied on conventional methods and have not remotely challenged September 11 quantitatively. If, as some purported experts repeatedly claim, chemical and biological attacks are so easy and attractive to terrorists, it is impressive that none have so far been used in Israel (where four times as many people die from automobile accidents as from terrorism). Actually, it is somewhat strange that so much emphasis has been put on the dangers of high-tech weapons in the first place. Some of that anxiety may come from the post-September 11 anthrax scare, even though that event killed only a few people. The bombings of September 11, by contrast, were remarkably low-tech and could have happened long ago; both skyscrapers and airplanes have been around for a century now.

RESPONDING TO TERRORISM

Frantz Fanon, the 20th century revolutionary, contended that "the aim of terrorism is to terrify." If that is so, terrorists can be

> Terrorists can be defeated simply by not becoming terrified — that is, anything that enhances fear effectively gives in to them.

not been followed. Some sort of terrorist inoculated Tylenol capsules with cyanide in 1982, killing seven people. However, that frightening and much-publicized event (it generated 125,000 stories in the print media alone and cost the manufacturer more than $1 billion) failed to inspire much in the way of imitation.

I do not want to suggest that all extreme events prove to be the last in their line, of course. At its time, the "Great War" of 1914–18 was the worst war of its type, yet an even more destructive one followed. Moreover, while Aum Shinrikyo may be under control, Al Qaeda and like-minded terrorist groups are unlikely to die out any time soon; September 11 marked, after all, their second attempt to destroy the World Trade Center.

Much of the current alarm is generated from the knowledge that many of today's terrorists simply want to kill, and kill more or less randomly, for revenge or as an act of what they take to be war. At one time, it was probably safe to conclude that terrorism was committed principally for specific political demands or as a form of political expression. In the oft-repeated observation of terrorism expert Brian Jenkins, "Terrorists want a lot of people watching, not a lot of people dead." Moreover, the suicidal nature of many attacks, while not new, can be very unsettling because the would-be perpetrator cannot be deterred by the threat of sub-

defeated simply by not becoming terrified — that is, anything that enhances fear effectively gives in to them.

The shock and tragedy of September 11 does demand a focused and dedicated program to confront international terrorism and to attempt to prevent a repeat. But it seems sensible to suggest that part of this reaction should include an effort by politicians, officials, and the media to inform the public reasonably and realistically about the terrorist context instead of playing into the hands of terrorists by frightening the public. What is needed, as one statistician suggests, is some sort of convincing, coherent, informed, and nuanced answer to a central question: "How worried should I be?" Instead, the message the nation has received so far is, as a Homeland Security official put (or caricatured) it, "Be scared; be very, very scared — but go on with your lives." Such messages have led many people to develop what Leif Wenar of the University of Sheffield has aptly labeled "a false sense of insecurity."

HYPERBOLIC OVERREACTION For example, there is at present a great and understandable concern about what would happen if terrorists were to shoot down an American airliner or two, perhaps with shoulder-fired missiles. Obviously, that would be a major tragedy. But the ensuing public reaction to it, many fear, could come close to destroying the industry.

Accordingly, it would seem to be reasonable for those in charge of our safety to inform the public about how many airliners would have to crash before flying becomes as dangerous as driving the same distance in an automobile. It turns out that someone has made that calculation: University of Michigan transportation researchers Michael Sivak and Michael Flannagan, in an article last year in *American Scientist,* wrote that they determined there would have to be one set of September 11 crashes a month for the risks to balance out. More generally, they calculate that an American's chance of being killed in one nonstop airline flight is about one in 13 million (even taking the September 11 crashes into account). To reach that same level of risk when driving on America's safest roads — rural interstate highways — one would have to travel a mere 11.2 miles.

Or there ought to be at least some discussion of the almost completely unaddressed but patently obvious observation that, in the words of risk analyst David Banks, "It seems impossible that the United States will ever again experience takeovers of commercial flights that are then turned into weapons — no pilot will relinquish control, and passengers will fight." The scheme worked in 2001 because the hijackers had the element of surprise working for them; previous airline hijackings had mostly been fairly harmless as hijackers generally landed the planes someplace and released the passengers. The passengers and crew on the fourth plane on September 11 had fragmentary knowledge about what had occurred earlier that day and they prevented the plane from reaching its target. Similar responses are likely for future attempted hijackings. Nonetheless, notes Banks, "enormous resources are being invested to prevent this remote contingency." There is a distinction, he argues, "between realistic reactions to plausible threats and hyperbolic overreaction to improbable contingencies."

Moreover, any problems caused by radiological, chemical, or perhaps biological weapons are likely to stem far more from the fear and panic they may cause than from the weapons themselves. While a "dirty bomb" might raise radiation 25 percent over background levels in an area and therefore into a range the Environmental Protection Agency considers undesirable, there ought to be some discussion about whether that really constitutes "contamination" or much of a danger at all, given the somewhat arbitrary and exceedingly cautious levels declared to be acceptable by the EPA. The potential use of such bombs apparently formed the main concern during the Orange Alert at the end of 2003. Because the bombs simply raise radiation levels somewhat above normal background levels in a small area, a common recommendation from nuclear scientists and engineers is that those exposed should calmly walk away. But this bit of advice has not been advanced prominently by those in charge. Effectively, therefore, they encourage panic. As one nuclear engineer points out, "If you keep telling them you expect them to panic, they will oblige you. And that's what we're doing."

POOR RESULTS For their part, biological and chemical weapons have not proven to be great killers. Although the basic science

about them has been well known for a century at least, both kinds of weapons are notoriously difficult to create, control, and focus (and even more so for nuclear weapons).

To this point in history, biological weapons have killed almost no one. And the notion that large numbers of people would perish if a small number of chemical weapons were to be set off is highly questionable. Although they can be hugely lethal when released in gas chambers, their effectiveness as weapons has been unimpressive. In World War I, for example, chemical weapons caused less than one percent of the total combat deaths; on average, it took a ton of gas to produce one fatality. In the conclusion to the official British history of the war, chemical weapons are relegated to a footnote that asserts that gas "made war uncomfortable...to no purpose." A 1993 analysis by the Office of Technology Assessment finds that a terrorist would have to deliver a full ton of Sarin nerve gas perfectly and under absolutely ideal conditions over a heavily populated area to cause between 3,000 and 8,000 deaths — something that would require the near-simultaneous detonation of dozens, even hundreds, of weapons. Under slightly less ideal circumstances — if there were a moderate wind or if the sun were out, for example — the death rate would be only one-tenth as great. The 1995 chemical attack launched in Tokyo by the well-funded Aum Shinrikyo (attempted only after several efforts to use biological weaponry had failed completely) managed to kill only 12 people.

Thus far at least, terrorism is a rather rare and — in appropriate, comparative context — not a very destructive phenomenon. However, the enormous sums of money being spent to deal with the threat have in part been diverted from other, possibly more worthy, endeavors. The annual budget for the Department of Homeland Security, for example, now tops $30 billion, while state and local governments spend additional billions. Some of that money doubtless would have been spent on similar ventures under earlier budgets, and much of it likely has wider benefits than simply securing the country against a rather limited threat. But much of it, as well, has very likely been pulled away from more beneficial uses.

Accordingly, three key issues, set out by risk analyst Howard Kunreuther, require careful discussion but do not seem ever to get it:

- How much should we be willing to pay for a small reduction in probabilities that are already extremely low?

- How much should we be willing to pay for actions that are primarily reassuring but do little to change the actual risk?

- How can measures such as strengthening the public health system, which provide much broader benefits than those against terrorism, get the attention they deserve?

As Banks puts it, "If terrorists force us to redirect resources away from sensible programs and future growth in order to pursue unachievable but politically popular levels of domes-

tic security, then they have won an important victory that mortgages our future." For instance, measures that delay airline passengers by half an hour could cost the economy $15 billion a year, calculates economist Roger Congleton.

Filmmaker Michael Moore happened to note on CBS' popular *60 Minutes* last year that "the chances of any of us dying in a terrorist incident is very, very, very small." His interviewer, Bob Simon, promptly admonished, "But no one sees the world like that." Both statements, remarkably, are true — the first only a bit more so than the second.

It would seem to be reasonable for someone in authority to try to rectify this absurdity. In Kunreuther's words, "More attention needs to be devoted to giving people perspective on the remote likelihood of the terrible consequences they imagine." That would seem to be at least as important as boosting the sale of duct tape, issuing repeated and costly color-coded alerts based on vague and unspecific intelligence, and warning people to beware of Greeks bearing almanacs.

What we need is more pronouncements like the one in a recent book by Sen. John McCain (R-Ariz.): "Get on the damn elevator! Fly on the damn plane! Calculate the odds of being harmed by a terrorist! It's still about as likely as being swept out to sea by a tidal wave. Suck it up, for crying out loud. You're almost certainly going to be okay. And in the unlikely event you're not, do you really want to spend your last days cowering behind plastic sheets and duct tape? That's not a life worth living, is it?"

But admonitions like that are exceedingly rare, almost nonexistent. What we mostly get is fearmongering, some of it bordering on hysteria. Some prominent commentators, like David Gergen, argue that the United States has become "vulnerable," even "fragile." Others, like Sen. Richard Lugar (R-Ind.), are given to proclaiming that terrorists armed with weapons of mass destruction present an "existential" threat to the United States or even, in columnist Charles Krauthammer's view, to "civilization." A best-selling book by an anonymous CIA official assures us that our "survival" is at stake.

The cosmic alarmism reached a kind of official pinnacle during last winter's Orange Alert. At the time, Homeland Security czar Tom Ridge declared that "America is a country that will not be bent by terror. America is a country that will not be broken by fear." Meanwhile, however, Gen. Richard Myers, chairman of the Joint Chiefs of Staff, was telling a television audience that if terrorists were able to engineer a catastrophic event that killed 10,000 people, they would successfully "do away with our way of life." The sudden deaths of that many Americans — although representing less than four-thousandths of one percent of the population — would indeed be horrifying and tragic, but the only way it could "do away with our way of life" would be if we did that to ourselves in reaction.

All societies are "vulnerable" to tiny bands of suicidal fanatics in the sense that it is impossible to prevent every terrorist act. But the United States is hardly "vulnerable" in the sense that it can be expunged by dramatic acts of terrorist destruction, even extreme ones. In fact, the country can readily, if grimly, overcome that kind of damage — as it overcomes some 40,000 deaths each year from automobile accidents. As RAND's Bruce Hoffman put it, "Unfortunately, terrorism is just another fact of modern life. It's something we have to live with."

A problem with getting coherent thinking on the risk of terrorism is that reporters and politicians find extreme and alarmist possibilities so much more appealing than discussions of broader context, much less of statistical reality. That is, although hysteria and alarmism rarely make much sense, politicians and the media are often naturally drawn to them.

There is no reason to suspect that President Bush's concern about terrorism is anything but genuine. However, his approval rating did receive the greatest boost for any president in history in September 2001, and it would be politically unnatural for him not to notice. His chief political adviser, Karl Rove, declared last year that the "war" against terrorism will be central to Bush's reelection campaign. The Democrats, scurrying to keep up, have stumbled all over each other with plans to expend even more of the federal budget on the terrorist threat, such as it is, than President Bush.

This process is hardly new. The preoccupation of the media and of Jimmy Carter's presidency with the hostages taken by Iran in 1979 to the exclusion of almost everything else may look foolish in retrospect, as Carter's secretary of state, Cyrus Vance, conceded in his memoirs. But it doubtless appeared to be good politics at the time — Carter's dismal approval rating soared when the hostages were seized. Similarly, in the 1980s the Reagan administration became fixated on a handful of American hostages held by terrorists in Lebanon. At the time, Reagan's normally judicious secretary of state, George Shultz, was screaming that we needed desperately to blast somebody somewhere "on a moment's notice" — even without adequate evidence — in order to avoid looking like the indecisive "Hamlet of nations." He apparently preferred the King Lear approach. Normally, however, only lunatics and children rail at storms; sensible people invest in umbrellas and lightning rods.

Since September 11, the American public has been treated to endless yammering about terrorism in the media. Politicians may believe that, given the public concern on the issue, they will lose votes if they appear insensitively to be downplaying the dangers of terrorism (though this fear does not seem to have infected Sen. McCain). However, the media like to tout that they are devoted to presenting fair and balanced coverage of important public issues. I may have missed it, but I have never heard anyone in the media stress that in every year except 2001, only a few hundred people in the entire world have died as a result of international terrorism.

As often noted, the media appear to have a congenital incapacity for dealing with issues of risk and comparative probabilities — except, of course, in the sports and financial sections. But even in their amazingly rare efforts to try, the issue — one that would seem to be absolutely central to any rounded discussion of terrorism and terrorism policy — never goes very far. For example, in 2001 the *Washington Post* published an article by a University of Wisconsin economist

that attempted quantitatively to point out how much safer it was to travel by air than by automobile, even under the heightened atmosphere of concern inspired by the September 11 attacks. He reports that the article generated a couple of media inquiries, but nothing more. Gregg Easterbrook's cover story in the October 7, 2002, *New Republic* forcefully argued that biological and chemical weapons are hardly capable of creating "mass destruction," a perspective relevant not only to terrorism but also to the drive for war against Iraq that was going on at the time. The *New York Times* asked him to fashion the article into an op-ed piece, but that was the only interest the article generated in the media.

In addition, it should be pointed out that the response to September 11 has created a vast and often well-funded terrorism industry. Its members would be nearly out of business if terrorism were to be back-burnered, and accordingly they have every competitive incentive (and they are nothing if not competitive) to conclude that it is their civic duty to keep the pot boiling.

Moreover, there is more reputational danger in underplaying risks than in exaggerating them. People routinely ridicule futurist H.G. Wells' prediction that the conflict beginning in 1914 would be "the war that will end war," but not his equally confident declaration at the end of World War II that "the end of everything we call life is close at hand." Disproved doomsayers can always claim that caution induced by their warnings prevented the predicted calamity from occurring. (Call this the Y2K effect.) Disproved Pollyannas have no such convenient refuge.

The challenge, thus, is a difficult one. But it still seems sensible to suggest that officials and the press at least once in a while ought to assess probabilities and put them in some sort of context rather than simply to stress extreme possibilities so much and so exclusively.

KNOW YOUR AUDIENCE It is easy to blame politicians and the media for the distorted and context-free condition under which terrorism is so often discussed. In many respects, however, that circumstance arises not so much from their own proclivities, but rather from those of their customers. Hysteria and alarmism often sell.

The record with respect to fear about crime, for example, suggests that efforts to deal responsibly with the risks of terrorism will prove difficult. Fear of crime rose notably in the mid-1990s, even as statistics were showing crime to be in pronounced decline. When David Dinkins, running for re-election as mayor of New York, pointed to such numbers, he was accused by A. M. Rosenthal of the *New York Times* of hiding behind "trivializing statistics" that "are supposed to convince us that crime is going down." New Yorkers did eventually come to feel safer from crime, but that was probably less because crime rates actually declined than because of atmospherics as graffiti, panhandlers, aggressive windshield washers, and the homeless were banished or hidden from view. So it may have made sense in the months after the September 11 attacks to have armed reservists parading around in airports. It is not clear how they prevented terrorist attacks, and pulling them from productive jobs hardly helped the economy. But if they provided people with a sense of security, their presence may have been worth it.

In the end, it is not clear how one can deal with the public's often irrational — or at least erratic — fears about remote dangers. Some people say they prefer comparatively dangerous forms of transportation like the private passenger automobile (the cause of over 3 million American deaths during the 20th century) to safe ones like commercial airliners because they feel they have more "control." But they seem to feel no fear on buses and trains — which actually are more dangerous than airliners — even without having that sense of control and even though derailing a speeding train or crashing a speeding bus is likely to be much easier for a terrorist than downing an airliner. And people tend to be more alarmed by dramatic fatalities — which the September 11 crashes certainly provided — than by ones that cumulate statistically. Thus, the 3,000 deaths of September 11 inspire far more grief and fear than the 100,000 deaths from auto accidents that have taken place since then. In some respects, fear of terror may be something like playing the lottery except in reverse: the chances of winning the lottery or of dying from terrorism may be microscopic, but for monumental events that are, or seem, random, one can irrelevantly conclude that one's chances are just as good, or bad, as those of anyone else.

The communication of risk, then, is no easy task. Risk analyst Paul Slovic points out that people tend greatly to overestimate the chances of dramatic or sensational causes of death, that realistically informing people about risks sometimes only makes them more frightened, that strong beliefs in this area are very difficult to modify, that a new sort of calamity tends to be taken as harbinger of future mishaps, that a disaster tends to increase fears not only about that kind of danger but of all kinds, and that people, even professionals, are susceptible to the way risks are expressed — far less likely, for example, to choose radiation therapy if told the chances of death are 32 percent rather than that the chances of survival are 68 percent.

But risk assessment and communication should at least be part of the policy discussion over terrorism, something that may well prove to be a far smaller danger than is popularly portrayed. The constant, unnuanced stoking of fear by politicians and the media is costly, enervating, potentially counterproductive, and unjustified by the facts.

CONCLUSION

The policy perspective toward terrorism I suggest may not be more valid than other ones, and no one knows, of course, how the problem will play out in future years. However, the policy advanced here seems to me a sound and sensible one, and for there to be a really coherent policy discussion, it should be part of the mix.

Deep concern about extreme events is not necessarily unreasonable or harmful. Thus, efforts to confront terrorism and reduce its incidence and destructiveness are justified. But hysteria is hardly required. As always, there are uncertainties and risks out there, and plenty of dangers and threats. But none are existential. The sky, as it happens, is unlikely to fall anytime soon. **R**