Defusing AIRLI

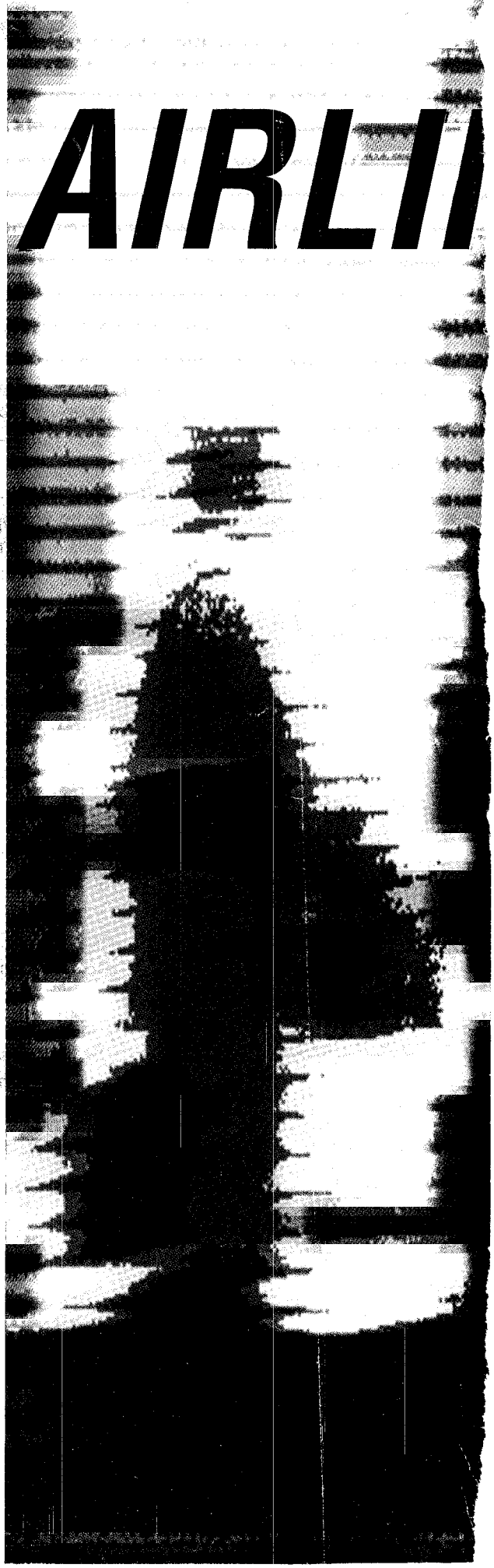
A variety of high-tech bomb detectors are under study, but certification, cost, and privacy dilemmas could keep them from your local airport.

By Mark Fischetti

THOUGH it takes a sick mind, it isn't hard to bomb a U.S. airliner. The security equipment in place at the nation's airports was mandated in the 1970s, when the chief concern was hijackings, not terrorist bombings. So while the metal detectors we all step through can uncover guns, knives, and other metal weapons, they can't find hidden explosives. Neither can the x-ray machines that scan carry-on bags, as well as checked luggage for international flights. Checked luggage and mail for domestic flights are not examined at all.

But recent bombings in Oklahoma City and Atlanta's Olympic Park, the FBI's discovery of plots to blow up U.S. airliners, and speculation about the downing of TWA Flight 800 in July have produced strong calls for protection against demolition-minded terrorists. Politicians have been jolted into action. After years of little legislative attention, Congress on October 9 suddenly appropriated $160 million for the Federal Aviation Administration (FAA) to rush more than 500 bomb detection units of various types into airports for a year of testing.

Some observers say this action is long overdue. Others say it is too hasty. No fewer than 10 detection schemes are vying for position—from x-ray machines and magnetic resonance imagers to chemical-vapor sniffers. Although they have different pros and cons, no single machine is both fast enough and accurate enough to meet the FAA's certification criteria. All the proposed systems are expensive. They also raise serious social concerns. The National Research Council (NRC) recently concluded that ultimately "limitations on the technology will be imposed as a result of passenger intoler-



PHOTOGRAPH: TONY STONE IMAGES/MARTINE MOUCHY
DIGITAL COLORIZE: LORI NOLLET DAMON

NE TERRORISM

ance for invasion of privacy, delays, or discomfort."

Even if the technical and human issues are resolved, the biggest question remains: Who will pay to protect the skies, and is the price worth paying?

The drive to screen for bombs gained momentum after the 1988 downing of Pan Am Flight 103 over Lockerbie, Scotland, which killed all 259 people on board. R&D accelerated on technology that could detect less than a pound of explosives hidden on a person's body or in luggage. Legislation directed the FAA to find automated machines that could uncover explosives without human operators.

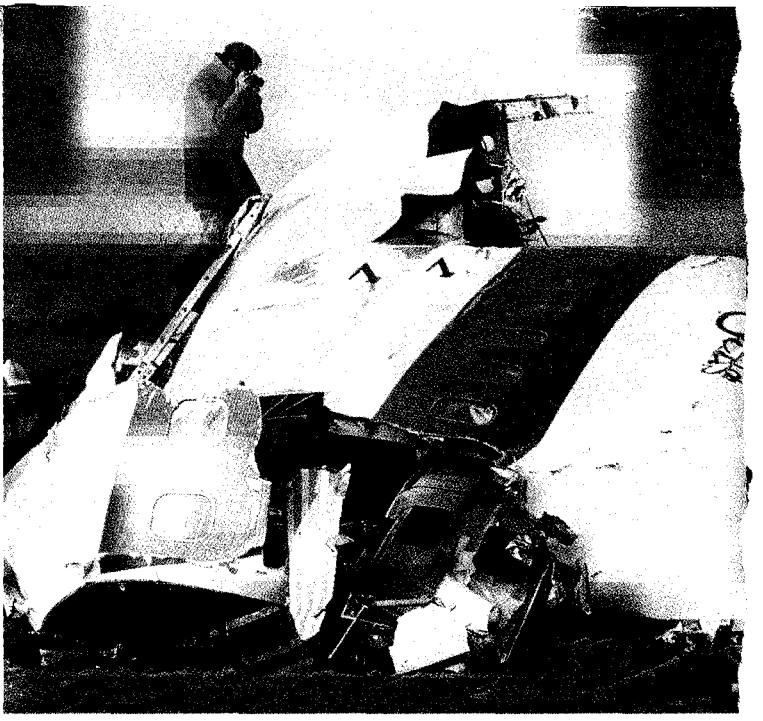
In 1993 the FAA set two key standards. To become certified, a machine would have to process 450 people or bags an hour, the approximate "throughput" of current carry-on bag scanners. It would also have to have a low false-alarm rate, reportedly 10 to 20 percent of all inspections. Meeting both numbers proved difficult, and the automation requirement was an obstacle that few manufacturers were able to overcome (most of the latest systems still need people to run them). But U.S. manufacturers didn't seem concerned; they were selling systems to Israel and Europe, where standards are less stringent. Besides, no further bombings had occurred, so U.S. airlines were not buying.

The heat increased in 1995 after Ramzi Ahmed Yousef, the suspected mastermind behind the 1993 World Trade Center bombing, was implicated in a plot to blow up a dozen U.S. airliners. His laptop computer, confiscated in the Philippines, stored flight schedules and detonation times. Accordingly, the NRC formed a committee on detection technologies. It issued its first report, pointing out relative strengths and weaknesses of various systems, in June 1996. The FAA responded by assembling a security task force on the morning of July 17; that evening, TWA Flight 800 blew up over Long Island Sound, killing all 230 people aboard.

Although the cause has yet to be determined, the July catastrophe set off a flurry of activity that is rapidly putting new technology into airports. The White House set up a Commission on Aviation Safety and Security under Vice-President Al Gore and gave it a mere 45 days to present a national technical strategy. In the frantic last days of its fall session, Congress banged out the October 9 Federal Aviation Reauthorization Act. The legislation earmarked $160 million for aviation security, tracking the Gore commission's recommendations that a variety of new detection techniques be tried out in real settings to identify the ones that are most ready for deployment.

Just like that, the FAA had money and a mandate. It quickly decided to purchase and deploy more than 50 special x-ray units, 400 chemical-sniffing machines, and other instruments to screen passengers and bags at 75 of the country's largest airports. Tests would be held over the next year. The first contracts were let the week before Thanksgiving. This infusion has rekindled widespread work—and debate.

MARK FISCHETTI, a freelance technology and business writer based in Great Barrington, Mass., has written for Smithsonian, Scientific American, *and many other magazines.*



SEE THE EVIL, HEAR THE EVIL, SMELL THE EVIL

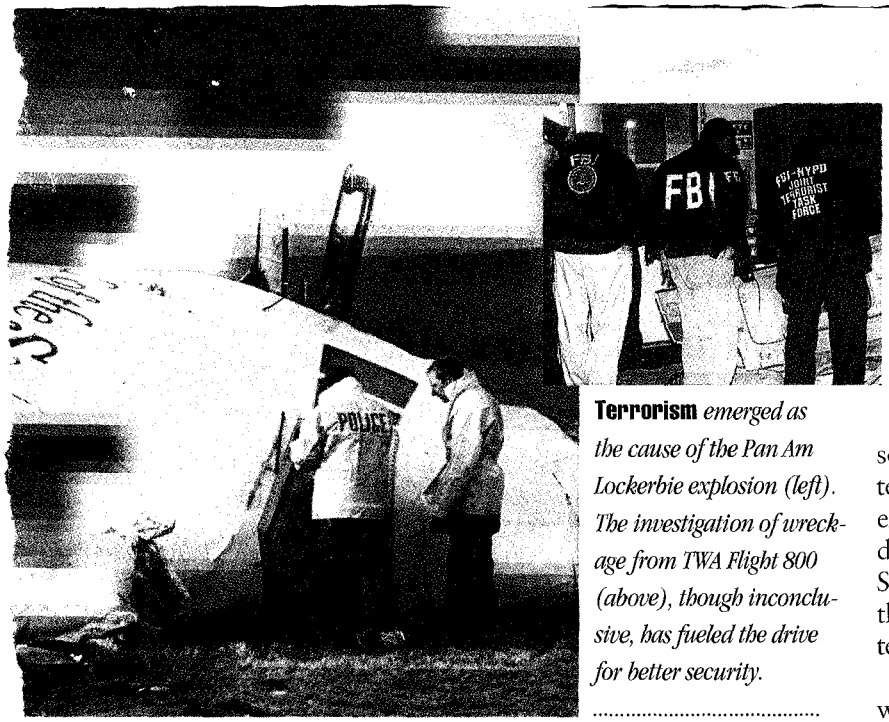
Explosives can be "seen" with imaging equipment that peers through clothing or baggage, "smelled" with instruments that react to vapors or particles, or "heard" with machines that pick up radio-frequency echoes of the material.

Although the densities of explosives—and plastic weapons, for that matter—are too low to be detected by conventional "transmission" x-rays, where a single beam of energy passes through an object, other types of x-ray machines can do the job. American Science and Engineering (AS&E) in Billerica, Mass., and Nicolet Imaging Systems in San Diego make machines that analyze "backscatter" x-rays. Different materials reflect x-rays in different ways. This backscatter is captured by sensors in the walls of a hatchway surrounding a bag or a person. It is then analyzed by software that looks for signatures of lower-density items (a plastic knife, for example) and those of substances with low atomic numbers, such as nitrogen, which are characteristic of explosives. These objects are shown on the operator's screen. By isolating questionable items, this scheme can thwart the common terrorist tactic of concealing explosives amongst clutter.

AS&E's machines are installed at numerous prisons, U.S. Customs checkpoints, airports in Europe, and the White House. The 101ZZ, which requires an operator, can scan up to 600 bags an hour, exceeding the FAA throughput standard. But its false-alarm rate is above the FAA limit; it's difficult to distinguish a roll of plastic explosives from a rolled up magazine or a salami. The machine costs from $80,000 to $120,000; an automated version costs about $300,000.

The darling of the x-ray contenders for screening bags is the CTX-5000, made by InVision Technologies in Foster City, Calif. The computed-tomography machine, similar to the CT scanners used in hospitals, takes cross-sectional slices and combines them into a three-dimensional image.

PHOTOS: REUTERS/CORBIS BETTMANN



Terrorism *emerged as the cause of the Pan Am Lockerbie explosion (left). The investigation of wreckage from TWA Flight 800 (above), though inconclusive, has fueled the drive for better security.*

Although its false-alarm rate meets the FAA's criteria, the system is slow; two machines must operate in parallel to process 450 bags an hour—an expensive configuration at about $1 million a machine. Nevertheless, the FAA has granted certification for systems comprising at least two CTX-5000 machines. In late December the agency signed a $52.2 million contract with InVision to install more than 50 machines at major airports, including Chicago's O'Hare.

EG&G Astrophysics in Long Beach, Calif., makes a lower-cost variant that takes just two, orthogonal slices. While better than a standard transmission x-ray photo, the image is less refined than that of the CTX-5000.

Vivid Technologies in Woburn, Mass., uses x-rays of two different energies, each absorbed most strongly by materials of a different density. By comparing the relative attenuation of the two beams, the system can distinguish objects from background clutter, and also determine a mean atomic number for a given object delineated in the image. If, for example, the system spies a mysterious brick, it can give an average number for the entire object (which may consist of several different materials). It then compares this number to those of explosives. If there is a correlation, a guard opens the bag to see whether the brick is a chunk of explosive or a block of cheese. The difficulty is that the atomic numbers of the 12 or more common explosives, including TNT, nitroglycerin, and RDX and PETN plastics, are similar to those for common compounds, from foodstuffs to books, so again false alarms are high. Vivid's machines cost from $250,000 to $400,000.

Another unit, made by Millitech Corp. in South Deerfield, Mass., exploits the fact that all objects not at absolute zero emit electromagnetic energy. The scanner differentiates objects by analyzing their emission patterns in the extremely high frequency range (near 100 gigahertz). Interpreting the rather grainy images requires highly trained operators, however. The benefit is that passengers are not exposed to x-rays.

Explosives that aren't seen might be smelled with "trace detectors" that react to small quantities of tell-tale vapors or particles. In this approach, people or bags pass through a closed portal. Air is blown over them, and the vapors or particles are collected for chemical analysis. In some machines, passengers push open "saloon" doors, or walk through brushes, which pick up particles left on their clothing or hands. Alternatively, an operator can rub a wand along the person or bag to vacuum up vapors and particles. This technique is attractive for analyzing laptop computers, radios, and other electronics, which set off metal detectors but cannot be taken apart for inspection. Since x-ray machines can't distinguish objects amid the cluttered circuitry, electronic devices are among terrorists' favorite hiding places for explosives.

The most widely deployed trace detector is the wand-style EGIS system, made by Thermedics Detection in Woburn, Mass. The machines are used at 42 airports in 12 countries to scan bags and are also used at border crossings in Israel. At the end of November, the FAA placed a $1 million initial order for the machines—which sell for $150,000 to $200,000 apiece—under the October 9 appropriation.

With EGIS, an operator passes a vacuum wand the size of a compact umbrella over the bag. The wand is then inserted into an analysis unit, which uses gas chromatography to separate the elements in the sample and determine their concentrations. This enables the system to distinguish between nitrogen compounds in plastic explosives and those in foodstuffs. The unit displays a red light if explosives are found, and indicates whether it is TNT, nitroglycerine, or plastic. According to Thermedics, EGIS has a "false positive" rate of less than 1 percent, better than other sniffers. The rate has been verified at the Frankfurt/Main Airport in Germany, where 2,500 EGIS screenings are performed each day.

Throughput is the problem. The average analysis takes 18 seconds, and the entire procedure can take several minutes, far below the FAA's threshold.

In November, Thermedics conducted a two-week field test of its first passenger sniffer, the SecurScan, at Boston's Logan International Airport. More than 2,000 travelers volunteered to walk through a portal where 10 wands brushed over their clothing, drawing in an air sample. Three people were stopped: a bomb squad employee, a traveler who had been on a firing range, and an FAA official who had earlier cleaned his gun. SecurScan costs about $300,000.

Meticulous terrorists who shower, change clothes, and seal explosives in airtight containers might fool a trace detector. But a unique signature of the explosive might still be "heard" using a novel technique called quadropole magnetic resonance, similar to the magnetic resonance imaging used in medicine.

Once inside the QScan-1000, made by Quantum Magnetics in San Diego, a bag is zapped with a pulse of low-

intensity radio waves. Nuclei in the bag and its contents are momentarily tipped out of alignment. As each material realigns, it reradiates a characteristic radio signal, which is picked up by a receiver and compared with the echoes for explosives. If a match is found, a red "fail" light goes on. The company says the process will not damage magnetic media such as computer disks or credit cards.

QScan costs about $300,000 and can inspect some 600 bags an hour. During a week-long trial at Los Angeles International Airport in November, only four false alarms occurred among 4,000 bags, an error rate of 0.1 percent. This newest of the detection technologies works well for plastic explosives, but not for all other types (the echo is not as strong), and the FAA has no certification procedures in place for it yet.

The only other detection technology the FAA has investigated is a scanner that bombards bags with neutrons to sense the density of specific elements, such as oxygen, nitrogen, carbon, and hydrogen. After $20 million in research, the agency has found the hardware to be far too costly, large, and heavy.

MILLITECH'S *Contraband Detection System, which measures natural electromagnetic emissions, can find objects that metal detectors and standard x-rays might miss, such as a 9-millimeter automatic pistol made almost entirely of ceramic (the lower weapon shown). But like all the new systems under study, it has pros and cons: while it avoids exposing passengers to x-rays, it produces grainy images that are sometimes hard to interpret.*

Each of the technologies under consideration can detect explosives, but what matters is how fast and how accurately. Conventional x-ray scanners process 600 bags an hour—six seconds each, on average. The 450-bag-an-hour mark was chosen because anything slower would discourage people from flying, according to Lyle Malotky, science adviser for civil aviation security at the FAA.

While the new x-ray scanners can meet the throughput limit, false alarms are high. Trace detectors are more accurate but need time to analyze samples. And there's the rub: the technologies trade speed for accuracy, or vice versa. The FAA demands both.

Real-life trials point out unforeseen weaknesses. The FAA checks new equipment at its William J. Hughes Technical Center in Atlantic City, N.J., with a standard "test-bag set." Although the CTX-5000 computed-tomography system passed at the Tech Center, its false-alarm rate rose above the FAA limit when used on actual passenger bags at San Francisco Airport. The rate was between 20 and 30 percent, according to Malotky, who is generally regarded as the country's most prominent expert in aviation security. Among the culprits, says Malotky, were certain food products that are similar in shape and density to a ball of plastic explosive and were not included in the FAA's test-bag set.

"False alarms are the bottom line," says Lee Grodzins, professor of physics at MIT and vice-president of AS&E, which makes backscatter x-ray scanners. "Only one bag in a billion might contain a bomb. So in a real airport, every alarm will be a false alarm." Each alarm will require a security guard to search the person or bag, shifting the detection burden to people, which slows the overall movement of passengers and bags. Metal detectors have a 10 percent false-alarm rate, Malotky notes, but most alarms are easy to resolve: just empty your pockets.

Experts acknowledge, too, that each of the new detection methods has an Achilles' heel—some way in which a knowing person can fool the system. Any of the machines might catch a careless terrorist, Grodzins says, "but none of them will stop the Unabomber."

RUNNING THE GAUNTLET

There is no magic bullet. The FAA and the manufacturers are only now accepting the notion that different inspection systems will have to work together, channeling luggage and people through multiple layers of scrutiny. "A gauntlet is really the way to go," says Thermedics president Jeffrey Langan. He is now marketing his EGIS trace detector for examining people already identified as suspicious or for inspecting bags that have triggered alarms in x-ray machines. EG&G and Quantum are jointly producing a large unit that can perform both x-ray and quadropole tests. Quantum will also offer the QScan-1000 as an add-on to an EG&G x-ray baggage scanner; x-rays are still the only way to find metal weapons.

A gauntlet might improve speed as well as detection. Langan figures the new generation of x-ray machines would clear 80 percent of the people and 90 percent of the bags. The remainder would be more closely scrutinized by operators, who might ask passengers to step aside and turn on electronics or open luggage. This would clear all but 1 per-

PHOTO: MILLITECH CORP. / AS&E

cent of the people and bags. These would be analyzed with the more precise but time-consuming trace detectors or quadropole machines. Britain's Heathrow Airport is trying this approach with InVision's CTX-5000 and Thermedics' EGIS machine.

Gauntlets would be costly, since the airlines would have to install several new expensive machines at each checkpoint. Better software would also be needed to coordinate the machines. But ganging machines together could help manufacturers pass FAA criteria. Langan says the FAA "should come up with a standard set of test bags and a dummy with materials hidden under its clothes, give them to the manufacturers, and say, 'You pick your combination of technologies and run these through. If you meet the criteria, you can put this system on the market.' "

LINKING BAGS TO PASSENGERS

Not all solutions to terrorism require state-of-the-art technology. The Gore Commission, which released its final report on February 12, is pushing two decidedly low-tech ideas: bag matching and passenger profiling.

Bag matching could be a powerful deterrent but could prove to be an operational nightmare. Each checked bag is tagged with a bar code that matches a code on its owner's ticket. If the passenger does not board a plane, his or her bags are removed before takeoff. The Lockerbie explosion was caused by a bomb in a piece of luggage that had been checked by a passenger who never boarded. Congress subsequently required the airlines to use bag matching on all international flights. It is not used on domestic flights.

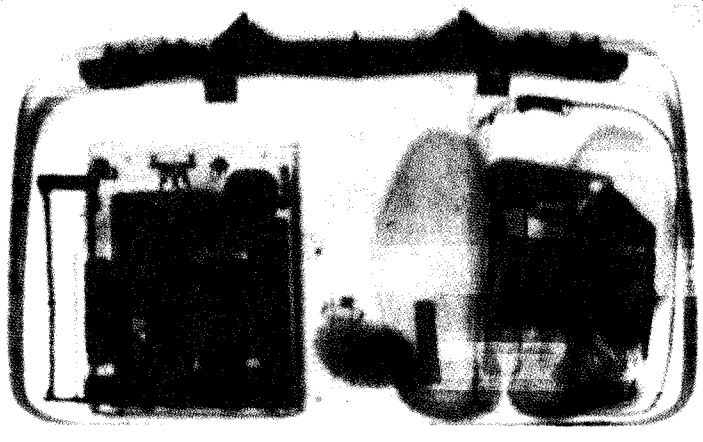
In September, President Clinton directed the FAA to quickly start a month-long bag-matching test at a major hub airport. The airlines objected strenuously on the grounds that bag matching would add significant delay to boarding procedures. Bag matching is doable on international flights because bags must be checked well ahead of boarding, and because there are few tricky connections to coordinate. But in the domestic hub-and-spoke system, which handles 850 million bags a year, connections are frequent and fast. David Fuscus, spokesperson for the Air Transport Association, an airline industry group, says that during peak times at O'Hare, 20 planes dock every 15 minutes. Thousands of passengers race to connecting flights, which depart on the average only 25 minutes later. Tracking every bag, instead of containers of bags, and checking each one against a passenger manifest in that time would be "impossible," Fuscus says.

Furthermore, if a passenger gets sick and must leave the plane, or a late arrival doesn't show, the ground crew would have to tunnel into the plane's luggage bays to find that person's bag, remove it, and resecure the hold. FAA audits indicate that it takes 20 minutes to find and remove this needle in the haystack—if the process is done efficiently. Delays incurred with bag matching could cost the airlines more than $2 billion a year in lost revenue, according to an FAA study.

Bending to airline pressure, the White House agreed to let the FAA stretch out the test program, which it had begun with Northwest Airlines. But the Gore Commission didn't buy the airlines' argument. During a September 1996 press conference on security, Elaine Kamarck, Gore's senior policy adviser, said, "We believe that with technology, some ingenuity, and reengineering we can move to full passenger bag match."

If bags were tagged with disposable radio transmitters, they would be easier to locate once in a cargo hold, according to Jesse Beauchamp, professor of chemistry at the California Institute of Technology. Beauchamp chairs the NRC's Committee on Commercial Aviation Security and is a member of the Gore Commission. There could even be some side benefits, he says: recent tests in Britain have resulted in fewer lost bags.

"Passenger profiling" could also speed up bag match-



BALLS *of simulated plastic explosive that are all but invisible in an ordinary x-ray image (top) show up clearly in an image made by AS&E's "backscatter" x-ray system (bottom). The latter compares reflected x-rays with the signatures of low-density materials such as explosives.*

ing—and the gauntlets—by predetermining which people are suspicious, and thus who should be more closely inspected and which bags should be tracked. By clearing the plainly "innocent" in advance, security people could focus their time and machines on the "unknowns."

Profiling is done by comparing what the airlines know about a passenger against an abstract list of factors that warn of possible danger. A frequent business traveler on his or her usual route might be sent directly to the plane, while a passenger from a country known to support terrorism—and who pays cash for a one-way ticket—will likely be x-rayed and sniffed. Northwest is developing a profiling scheme with FAA funding that would complement its bag-matching plan. The October 9 legislation authorizes the FAA to adapt a system used by Customs officials to zero in on drug traffickers. And the final Gore Commission report urges implementation of some degree of bag matching coupled with passenger profiling by year's end. Gore said bag matching for all luggage is the eventual goal.

THE FOURTH AMENDMENT TEST

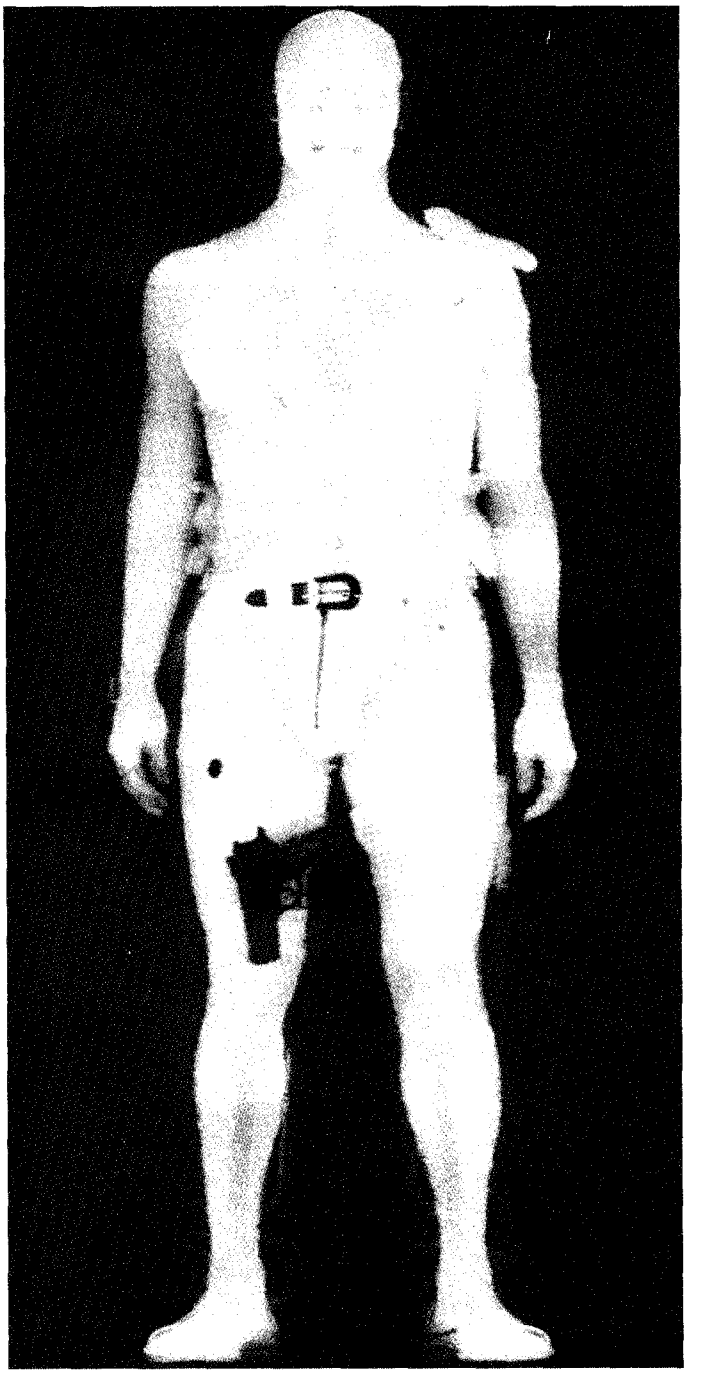
You may not know it, but if you flew recently you might already have been profiled. Since the downing of TWA Flight 800 in July, U.S. Customs' profiling procedures have been extended to some domestic flights. If you feel a bit uneasy that you were never told you had been profiled, you have hit upon one of the most critical and widely debated obstacles to better security: the potential violation of civil rights. If detection schemes discriminate on the basis of people's nationalities, or expose too much of their bodies, passengers won't accept them and airlines won't use them.

Even if the profiling criteria do not specify race, religion, or nationality, it doesn't take much imagination to see how a search might zero in on these categories. Passengers whose ultimate destination is Syria, for example, might be targeted because of the country's sponsorship of terrorism. But who flies to Syria besides Syrians? This amounts to de facto discrimination, says Gregory Nojeim, legislative counsel at the American Civil Liberties Union (ACLU) in Washington, D.C. "Reduced to its essentials," he says, "profiling is a stereotype."

Nojeim can cite many horror stories to prove his point. After the Oklahoma City bombing, Abraham Ahmad boarded a plane from that city bound for Chicago, en route to visiting his family in Jordan. He was detained by government agents in Chicago and London and forced to answer questions about his religion, friends, and family members. At various times he was handcuffed and paraded through the airports. He was strip-searched. His name was given to the media, who drove his wife out of their house. All because he "fit the profile" of a terrorist. For similar reasons, Sam Husseini, a consultant to the American-Arab Anti-Discrimination Committee, was singled out and missed flights three times in the summer of 1993 alone.

"When travelers check in at an airline ticket counter," says Nojeim, "they don't check their rights to personal security, privacy, and equality. The Fourth Amendment provides that people and their property shall not be subjected to unreasonable searches and seizures."

The ACLU also maintains that new x-ray techniques constitute an invasion of privacy. Look at the image of the man on this page. Sure, it shows a gun and explosives. It also



MACHINES *that peer through clothing may turn up explosives and weapons, as in this image produced by AS&E's BodySearch system, but such techniques also reveal the naked truth in ways passengers would rather avoid. Image-modifying software could help.*

PHOTO: AS&E

shows his penis. Would you want a similar image of *your* body displayed on a screen for other people to see as you wait to board your flight? "The airport is not a 'no-privacy zone,' " Nojeim says. "We may have catheter tubes in place, evidence of mastectomies, penile implants, and artificial limbs. We expect that we will not be required to show these to others as a condition to boarding an airplane."

The National Research Council agrees. "Displaying an image of the body on a monitor will be a concern to a significant percentage of people," its report concludes.

Problems could be lessened by masking portions of the display, using operators of the same sex as the subjects being scanned, and displaying images in closed monitoring rooms. Each approach would add even more cost, however. Software could help by making a Picasso out of a person being scanned, or by making images generic, but progress has so far been limited. Image recognition software that could discern weapons and explosives without operators would help too, but the amount of artificial intelligence required makes this an even tougher challenge, says MIT's Grodzins.

Though not a civil rights issue, worries about health risks could also make passengers wary. The NRC cites numerous studies indicating that none of the techniques pose health risks to passengers or operators, and that x-ray levels are well within the allowable limits for routine exposure. But both the FAA and the manufacturers acknowledge that some passengers may nonetheless be wary of the new technologies.

AT WHAT PRICE SECURITY?

Even if the technical and social challenges posed by the new technologies can be resolved, costs will have to come down. Most of the detection machines sell for several hundred thousand dollars apiece. Various estimates put the cost to deploy bag scanners alone at the 75 busiest U.S. airports at about $2 billion. That's four times the $500 million in profit the U.S. commercial carriers made in 1995, according to the FAA's Malotky. If a gauntlet were used, the tab would be much higher. And there would still be 300 more airports to go.

Operational costs could be even greater. If slow throughput, false alarms, and bag matching lengthen preboarding time, each airline will schedule fewer flights per day, slowing down the air transportation system. "There are huge feedback effects for even a slight added delay," says Robert Hahn, a regulatory economist at the American Enterprise Institute in Washington, D.C., and author of *Risks, Costs, and Lives Saved* (Oxford University Press, 1996). According to the *Wall Street Journal*, an internal Northwest study concluded that bag matching would add 10 minutes to processing time, a delay that would force the airline to cut its schedule by around 10 percent.

Delay would also hurt the U.S. economy. Adding a half-hour to preboarding time would cost almost $10 billion annually in lost productivity, according to Hahn.

Airports would be pinched, too. More than half their revenue comes from parking and concessions. "More floor space for detection machines means fewer coffee bars," says Malotky, "and longer lines for security checks mean fewer people will have time to buy coffee." Gateways at older airports, already cramped, would have to be expanded and reinforced to support the big, heavy new machines.

All these numbers raise a bald question: Is the price worth paying to save precious, but few, lives? In the past 15 years—a time frame that economist Hahn picks more or less arbitrarily—548 people have died in U.S. airline crashes linked to sabotage (nearly half on Pan Am 103). Dividing this number into the $2 billion needed for bag scanners alone yields a capital cost of $54 million per life saved—if, indeed, the technology could cut bombings to zero.

Whether this is a "good" investment is a distasteful question, but one that government must ask all the time. The money could be used to make safer highways, which are 20 times more dangerous per mile than air travel, according to federal estimates. "We should think about what we're getting for the money," Hahn argues.

Several years ago, the FAA analyzed the idea of requiring children under age two to fly in car seats—instead of sitting on a parent's lap—forcing parents to buy another ticket, then averaging $400. The study showed that more families would drive, which would result in more highway fatalities than the in-flight car seats would save, says Malotky.

In analyzing such tradeoffs, experts are reluctant to quantify how "good" or "bad" the nation's security is. Malotky did say that in the last few years, the airlines have found "fewer than 10" bombs or suspect weapons. Presumably some were missed. Though 100 percent detection is statistically impossible, the process can always improve. But the cost-benefit relationship may run up against diminishing returns. Malotky says if going from 90 to 95 percent detection would cost x dollars, improving from 95 to 98 percent would cost x dollars again. Economist Hahn concludes that "all this new technology would reduce the risk of death by only a very small amount."

The FAA is now developing a cost-benefit analysis. For the time being, Malotky will say only that "if a bombing were to occur every six months, the cost-benefit would certainly make sense. If a bombing took place once every 10 years, it would not make sense." Assuming that terrorism didn't down TWA Flight 800, then the last U.S. airline bombing was Pan Am Flight 103 in 1988. "Despite all the headlines, the chance of getting blown out of the sky is vanishingly small," says George Swenson, professor emeritus of electrical and computer engineering at the University of Illinois and chair of the NRC panel on passenger screening.

Whether heightened security is worth the cost comes down to whether the public perceives a real threat. No one has surveyed passengers to see how they feel.

Still, the technology has intrinsic value as a deterrent. Fighting terrorism is an endless game of threats and countermeasures. "We have no idea how many terrorists have been deterred because they were afraid they'd get caught," says MIT's Grodzins. "Personally, I'd love to see more

bomb-sniffing dogs out there. Nothing is more directly worrisome to a would-be bomber."

Unfortunately, dogs are worrisome to travelers as well. Security experts acknowledge the public's reservations about the military atmosphere that canine teams impart, and about the prospect of being sniffed in sensitive areas by a high-strung Doberman. Dogs also cannot keep up with a systematic, 450-bag-per-hour search regimen. So even though the October 9 legislation encourages the FAA to add as many as 100 canine teams to airports nationwide, it is unclear whether this approach will be a viable substitute for new high-tech detection schemes.

WHO PAYS?

It's also unclear who will end up paying for the latest technology. The actors are in a classic standoff, eyeing each other to see who'll make a move. The airlines are responsible for security, but they don't want to buy advanced equipment if it is not FAA certified; if the FAA mandates a different technology a year later, the airline will have wasted its money. The manufacturers aren't motivated to get certification because they fear the FAA specs will change. The airports have no incentive to take over duties that now fall to airlines. Congress doesn't want to mandate technology.

The irony is that the cost to passengers for better technology would be small. People take about 530 million flights in the United States each year. Raising $2 billion would add $4 a ticket. But even at that price, the financially weak airlines want the government to pay.

Spending tax dollars to buy equipment headed to for-profit companies rankles many Americans. But Grodzins says the public and Congress have to take a broader view. "These attacks are not against Pan Am or TWA," he says, but against the United States. "It is the government's responsibility to fight this war, not the airlines'." The FAA's recent appropriation of $52.2 million to install CTX-5000 scanners may bolster this position.

Thermedics president Langan says the airport authorities should foot the bill, with government funding R&D. "That's how it's done in the rest of the world," he notes. The logic is that security is a policing function that should be performed throughout the airport—not just at airline gates, but at every door—and should be extended not just to passengers, but to every ground-crew member, security guard, and employee of caterers and freight handlers. In the United Kingdom, Langan says, airports have found cost-effective ways of discharging their responsibility for security. Most British airports contract security functions to commercial companies, which purchase better detection equipment and pay and train operators more than the government ever did, because they are competing to provide the best service.

To implement this model, Congress would have to widen the FAA's jurisdiction to include airports. Airports would likely be owned by quasipublic corporations like the Port Authority of New York and New Jersey, which operates Kennedy, LaGuardia, and Newark airports. Evidently, Congress is game. The reauthorization act directs the FAA administrator to report on whether to transfer certain security functions from airlines to airports, and if so, how.

Given the technical, social, and financial issues, some are tempted to wait to deploy a more perfect technology. But Grodzins says the government has already waited too long. "We have a real, live enemy here. We should deploy the best we have, and upgrade it later. We have to put these machines out there to find their real strengths and weaknesses. In the meantime their very presence will deter more terrorists."

A clearer deployment strategy may emerge in the next few months. In February, President Clinton urged Congress to approve an additional $100 million a year to implement recommendations of the Gore Commision. By June, the National Research Council will issue its second annual report, which will advise the FAA on what to implement. And the year-long trial of hundreds of machines sprung by the October 9 appropriation will soon be in full swing.

In order for new technology to do its job properly, some other holes in airport security will have to be plugged. A moderate-sized airport is a veritable sieve, with more than 200 doors and passageways; many security experts say they have wandered into restricted areas unencumbered. In addition, no technologies or procedures are in place for inspecting mail or freight, and none are planned. NRC panel chair Swenson adds that "background checking of airline and airport employees, and potential new hires, is also loose."

Another problem area is operator training. The NRC feels operators could be the weakest link in future systems. "Low wages, high turnover, inadequate training, and poor working conditions need to be addressed," security committee chair Beauchamp told Congress in September.

Maintaining tight security also depends on testing the system. The FAA uses "red teams" to try to foil security at random airports. They have sneaked suspicious packages, fake bombs, and weapons past guards and x-ray machine operators, then reported back to the airline that security had better shape up. But the FAA needs to watch its own back. A 1996 audit by the Department of Transportation's inspector general on red team activities at 26 airports revealed that a few FAA special agents appeared to tip off airline personnel, or failed to report breeches of security, perhaps because of quid-pro-quo deals with airline employees.

It's too early to predict when new technology may be permanently installed. Although the October 9 appropriation jump-starts the process, it could fizzle. "The FAA pays a lot of attention to the political winds," says MIT's Grodzins. "Manufacturers have gotten burned before. Lots of legislation was rapidly passed after the 1988 Pan Am bombing, but we're still using the same technology on domestic flights now as we were using the day before it happened."

So the standoff may continue until Congress commands the FAA to require new technology. What would prompt legislators to do so? George Swenson fears the simple, terrible answer: "A few more bombings."■