

How Technology Can Help Make Air Travel Safe Again

by Robert D. Atkinson

In the wake of the September 11 terrorist attacks, Congress will likely pass needed legislation to boost security at U.S. airports. While weighing the merits of measures such as installing secure cockpit doors, expanding the air marshal program, and increasing the effectiveness of airport security personnel, Congress should also give serious consideration to significantly expanding the use of cutting-edge, advanced information technologies to help make our airports more secure. There are a host of technologies, such as biometric authentication, (for example, finger print or automatic facial recognition), radio-frequency tags (on baggage), and better luggage and passenger scanning technologies that are ready now to play key roles in enhancing security. Installing modern technology in airports sounds expensive, but it need not be. In most cases, particularly relating to passenger and personnel identification systems, the technology is already in use in commercial settings and can be deployed for a modest financial commitment. Given the other monetary, non-security benefits of technology, such investments make eminent sense.

It is too early to determine exactly how the hijackers were able to perpetrate their heinous crimes, but it is important to design a security system to thwart a wide array of threats and address a myriad of vulnerabilities. For example, even though the hijackers did not place bombs on the planes, there is still a need for a better system to match baggage to passengers on board. Likewise, we don't know if the terrorists were assisted by individuals posing as ground workers, but regardless, there is a need to be do a better job of controlling access to secure areas.

As the Progressive Policy Institute has asserted in prior reports, New Economy policy makers should turn to technology when trying to solve pressing issues.¹ And the problem of airline security is no different: To be effective, airline security in the 21st century must employ technology of the 21st century.

Recommendations

Since September 11, at least four separate bills have been introduced in Congress to enhance airport security. Congress is expected to act as early as this week to pass legislation. Most bills address issues such as deploying sky marshals, federalizing airport security screening, reducing the number of carry-on bags, and the like. We are aware of only one bill, S. 1429, introduced by Senator John Edwards (D-NC), that addresses the issue of technology. For example, the legislation requires airports to strengthen access control points in secure areas, "by using biometric or similar technologies that identify individuals based on unique personal characteristics." The Edwards bill, which deals primarily with controlling access to secure areas, also calls on the Federal Aviation Administration (FAA) to "deploy the most up-to-date technology that is available and certified for inspecting passengers, baggage, and cargo for chemical, biological, or similar substance(s)."

A new aviation security system for the 21st century must fully incorporate the latest technologies. And while installing modern technology in airports sounds expensive, in most cases it is not. As Congress and the administration consider new aviation security legislation, PPI believes that any new law should:

- ▶ **require airports and airlines to adopt advanced security technologies, including passenger identification systems using smart cards and biometric authentication systems (e.g., systems that identify a person on the basis of a unique physical characteristic, such as their fingerprint or shape of their face);**
- ▶ **direct the FAA to evaluate the technical feasibility, costs, and benefits of upgrading airport scanning technology;**
- ▶ **provide funding for the deployment of these technologies by U.S. airports and U.S. airlines;**
- ▶ **provide funding to create a facial identification system in airports linked to databases of suspected terrorists and other wanted criminals. This requires updating and integrating law enforcement databases and ensuring that they include facial biometric information;**
- ▶ **require that any biometric or smart card applications being deployed with federal funding are compatible and inter-operable with a wide array of governmental and commercial areas, not just airlines and airports.**

Scanning Technology

Most existing systems are based on 20 to 30 year old technology that scans only for metal. Available new technology can do a much better job. For example, by the end of the year, researchers at the National Institute of Standards and Technology expect to unveil the first prototype of a system that can scan passengers in airport departure lounges and/or checkpoints to identify concealed weapons, including plastic knives. And it does so without revealing inappropriate physiological details.

Another company has been working with Sandia National Laboratories through an FAA grant to develop a machine that can rapidly detect the tiniest particles of toxic chemicals, explosives, and other items as passengers go through what resembles an oversized metal detector. Other companies have developed advanced X-ray machines based on computer tomography technology used in hospital CT scanners.

It is not clear which systems should be deployed for what applications. However, Congress should direct the FAA to evaluate the technical feasibility and costs and benefits of upgrading airport scanning technology.

Biometrics

A key technology for airport security in the future will be biometrics, i.e. recognizing and authenticating individuals based on unique biological data. Everyone is familiar with fingerprint identification. Like fingerprints, biometric applications are based on a unique

biological identifier, but through the use of advanced information technologies, biometrics can perform identification and authentication almost instantaneously. There is a wide array of biometric systems, including electronic fingerprint identification, facial geometry (e.g., some use over 60 unique measurements related to a human face, such as distance between the eyes; others use facial recognition algorithms), hand geometry, non-invasive retinal scans, signature recognition (everyone writes their name differently), and voice recognition. Most Americans are familiar with these technologies from watching James Bond movies but think that they are the province of a science fiction future. In reality, they are being used today in a wide variety of applications, including airports, to boost security.

Passenger and Personnel Control/Authentication Systems

Biometrics can serve as a form of “one-to-one” authentication. For example, when a pilot receives a license to fly, he could be issued a smart card (a plastic card the size of a credit card with a powerful computer chip on it²) containing the pilot information and unique biometric information (e.g., facial profile, fingerprint, etc) embedded on the chip with virtually unbreakable encryption software. When the pilot tries to enter a secure area, including the cockpit, he or she would put a smart card in a slot and submit to a biometric identification (e.g. they could look at a camera).³ If the person and the encrypted image on the card do not match, the person would not be allowed entry. Of course, such a system could work with a password, the way ATM machines issue cash, but in this case, the individual himself is the password. While not 100 percent foolproof, such systems appear highly accurate. The most advanced facial biometric systems, for example, can identify a person if they shave their beard, wear glasses, etc.

For passengers, such a system might work as follows: The first time a passenger flies after the system is in place, he appears at the main check-in counter, shows a proper government-issued ID like a driver’s license, and undergoes biometric identification (a camera could automatically take a picture of his face or his retina or he could place his thumb print on a reader). Within less than a minute, the agent issues the passenger a smart card containing, in encrypted electronic form, the flight information and the file containing the biometric scan. Additional information, such as frequent flier numbers, meal and seating preferences, etc., could also be kept on the card.

As the person passes through security, he would insert and remove the smart card in a slot as he goes through a detector (for metal and possibly other substances such as chemical traces from explosives). In order to be permitted past the security checkpoint, the person’s authentication must match that on the card (e.g., his face or retina could be scanned, or he could put his thumb on a reader). If the card and the person holding it do not match up, the individual would not be allowed to go through.

Moreover, as the person enters the boarding ramp to the plane, he would be required to again be authenticated. For example, with facial authentication, a camera could automatically take a picture of the person. If he was not on the electronic data file of passengers who had checked in and gone through security, he would not be allowed to board the plane. Such a system would prevent individuals from getting a boarding pass and then handing that pass off to a different person without a ticket to get on the plane.⁴

Authentication measures such as these would allow fully accurate and real-time passenger manifests. Currently, according to the Airline Pilots’ Association, it is not uncommon

for planes to leave with fewer people on them than the number of people who checked in. The APA testified before Congress that they know of at least one airline that routinely allows the flight to leave the gate with a two-person error. As they stated, “Unless we know that the person boarding the aircraft is the same as the one who bought the ticket, we cannot positively ascertain that the individual has been through the security checkpoint and is not carrying a weapon.” Using this technology would enable airline personnel to immediately identify individuals who have checked in but have not boarded the plane.

The system could also be used to let pilots know if individuals aboard have special capabilities that might be needed in emergencies. Individuals could voluntarily put this information on the card, and in the case of an emergency, the crew would be able to query the on-flight passenger database to determine if there were any doctors, bomb specialists, etc., on board who could provide assistance.

Such a system could also enable airlines to jointly track passengers and their baggage. When a person with luggage checks in, their bags would be tagged with either a very cheap (costing pennies) radio frequency (RF) transmitter emitting a unique code, or a special bar code. These would be linked in the computer to the passenger authentication code on the smart card. As the luggage is put on the plane, it would be scanned (automatically in the case of the radio frequency tags), and entered into the computer system managing that particular flight. If someone’s luggage is on the plane, but the person is not, the flight would not be allowed to take off until that person’s luggage was removed. While this would not deter a suicide bomber, it would dramatically reduce the threat of other types of hijackings. In addition, as the luggage is checked in, the RF tag would record the exact time, and if the bag fails to reach subsequent RF readers by a particular time (suggesting that someone might have taken the bag off and implanted explosives or other prohibited items), the baggage is redirected to a special location for separate handling. Such baggage systems have the additional benefit of facilitating more automated baggage handling systems.

Cards could be issued in several ways. Passengers who seldom fly might be issued cards that they would turn in as they board a plane. Frequent fliers could be issued a card that they use repeatedly and on different flights. Each time they check in with an airline, their frequent flier numbers would be put on the same card.

These systems could also be used to control access to secure sections of an airport, such as baggage handling areas. In the wake of September 11, security concerns have come to light. Current systems need to be upgraded, as shown by a recent GAO effort where GAO inspectors were able to carry weapons around two airport security checkpoints using phony credentials. Given how easy it is to lose or obtain such ID badges, it suggests that we need a new system. For example, at Logan Airport in Boston, hundreds of airport personnel ID badges have been lost in the last year. It would be relatively easy for terrorists to obtain such badges and alter them in order to gain entrance to secure areas. The advantage of smart card ID’s containing biometric authentication is that if an ID card is lost, it cannot be used by another person. Such a system would aid in detaining and investigating any individual who attempted to use someone else’s authentication smart card.

Such technologies are already being deployed to control personnel access to secure areas.⁵ For instance, Chicago’s O’Hare airport recently installed a system that uses fingerprint biometrics to speed access and enhance cargo security for truck drivers at the airport. The system is two to four times faster than the existing manual system and more secure. In addition, the Charlotte/Douglas International Airport in North Carolina, along with U.S. Airways, uses iris recognition technology to verify its employees’ identities before they are allowed to

enter the airport's secure areas. In addition to ensuring that only authorized people get through, some systems can also prevent "tailgating" (where two people go through a door opened for one person), for example, by employing facial biometric scanning (the camera would see two faces go through). Such systems can be designed to keep any inconvenience to a minimum.

Biometrics would enable airports and airlines to develop real-time, networked flight information systems that identify passengers and baggage. It would also enable a much higher level of security for access to secure and restricted areas. It is distressing to realize that the credit card information system used to buy a pair of pants in a store is more networked than our airport security, ticketing, and baggage systems. It is time to change that.

Passenger and Personnel Identification Systems

If the only goal of a system is to authenticate individuals and ensure that they are the actual ticket holders, or that they are indeed on the plane, any number of different biometric authentication systems would work. However, in order to identify potential terrorists or wanted criminals, facial biometrics capabilities are needed.

Facial biometrics can be used to make "one-to-many" identification. For example, cameras located at airports could instantaneously scan all the faces of persons in the airport and if any are on known lists of suspected terrorists (or criminals on wanted lists) the system would automatically alert police. In the case of at least two of the hijackers of the September 11 crashes, authorities had pictures of them as suspects prior to the attack, and airport cameras actually photographed them. However, because the cameras were not based on facial biometric identification systems, airport security was not alerted. A facial biometrics recognition system could possibly have identified these individuals as they entered the airport, allowing security to detain them.

Facial biometric systems can scan faces of individuals in a crowd, or those passing through particular points (such as a security check point) and within seconds compare the face with a database of hundreds of thousands of wanted criminals or suspected terrorists. Such a system would then automatically send a voice message through a wireless communications device to airport security personnel, and as the suspect walked through the airport, continuously monitor them, providing constant updates to security (e.g., "the suspect is at Gate 22"). The technology is so powerful that it could also send wireless images to security guards through simple hand held devices (like Palm Pilots) or even project the image on one lens of a guard's glasses so they can positively ID and detain the suspect for questioning and possibly arrest.

Such camera systems can also be used in places where only authorized personnel are allowed, such as baggage sorting, air traffic control operations, maintenance, and catering delivery areas, and crew lounges. If persons are found in an area where they do not belong, the system would alert security. Facial biometrics can also be used to control private aviation so that individuals entering corporate jets and other private airplanes are also authenticated.

In order for facial biometrics systems to work, however, law enforcement agencies around the nation, and indeed the globe, would need to develop integrated databases that feed in facial images of suspected terrorists or wanted criminals, which is a major networking and software challenge. Currently, the FBI, CIA, and various state agencies maintain their own records, and no common databases exist.

The FAA is currently working on its Computer-Assisted Passenger Prescreening System

(CAPPS), designed to use the passenger information system in airline databases to determine if an individual poses a security risk. This system needs to be widely deployed, but also integrated with facial databases so that a suspect whose name is not known but whose face is, can be identified before he boards a plane. In some cases, authorities have pictures of persons associating with known terrorist leaders, but do not know their names. Entering these faces into a system would increase the likelihood of their being detained if they entered U.S. airports.

Such technology is not science fiction. It is currently being used successfully by British law enforcement who deploy cameras to scan certain public places to compare faces with faces of known wanted criminals. It is also being used at airports, including Keflavik International Airport in Iceland, which installed face recognition biometrics in its closed circuit TV infrastructure linked to a database of criminals and potential terrorists compiled by the European Union.

Nor are such systems a panacea. For example, they would not deter a suicide terrorist from getting on a plane if intelligence and law enforcement had no prior knowledge of that person. However, they would make it easier to prevent entry by individuals who are known or suspected.

These systems can be used in an array of situations where it is important to authenticate, track, and/or identify individuals, not just airports. For example, the Edwards bill has proposed using biometric identification systems to secure our nation's water ports. Similarly, such systems could also be used for passenger trains, and perhaps at rental car and other transportation facilities. In addition, facial biometrics systems can be used by the Customs Bureau to deny entry of suspected foreign terrorists or foreign nationals with immigration violations to the nation or to airplanes whose destination is the United States.

It is not clear how much such systems would cost, though one source estimates the price of installing a facial biometric system in an airport to be between \$300,000 and \$750,000. Smart card systems would add to the cost, but overall, installing such systems at all U.S. airports should not be prohibitively expensive.

The Potential Benefits Extend Beyond Enhanced Airport Security

The decision to deploy advanced security technology at airports should be made on the basis of how it improves airport security. But, it is also important to realize that such technology investments could have three important supplemental benefits that policy makers should take into consideration, particularly at a time when it appears that the economy is likely to enter a recession.

First, these technologies can actually increase convenience at airports. After the September 11 attacks, the airline industry is in dire financial straits, with planes running between 20 percent and 40 percent of capacity. Better airport security will help restore confidence in flying and increase the number of airline travelers. However, if tighter security is achieved in ways that severely inconvenience flyers, (i.e. forcing passengers to check in hours before a flight, and prohibiting check in at the gate, etc.), fewer Americans will get back in the air. It is important, if possible, to build an aviation security system that protects Americans in a way that sacrifices little of the convenience of flying Americans now enjoy. Employing advanced technology is one way to achieve greater security while reducing loss of convenience.

These technology systems can in fact enhance security and speed access. For example, Israel's Ben Gurion Airport, with arguably the highest level of security in the world, uses

biometrics to speed customs clearance. Israeli citizens and frequent travelers who are approved for travel enroll in a system that measures their hand geometry. Upon reentry at the airport, authorized users place their hand on a device which validates that they indeed are enrolled and should be permitted to enter. The system not only saves the airport money, but it reduces the wait for passengers, which at peak times could reach one hour, to 15 seconds. Airport officials there report that biometrics allows customs officials to spend more time on other people who may pose a greater risk.

Biometric authentication could also reduce the reported risks related to e-tickets and self-serve check-in kiosks. Airline Pilots' Association recently testified in Congress arguing for the elimination of kiosk-based check in. Given current authentication procedures at kiosks, their concerns should be considered. However, kiosks have important benefits, including convenience and increased airline productivity. Biometric authentication devices can provide high levels of security while still allowing kiosk check in. Once an individual has checked in with an airline and received a smart card with their encrypted biometric information on it, checking in at a kiosk the next time they fly should be no less secure than with an airline agent, if the machine uses biometric authentication. The person could go to the kiosk, put in their smart card and be scanned to prove he is actually the person who was originally issued the card and purchased the ticket.

The current ban in some airports on remote and curbside check in is another new development that, while maybe needed in the short run, increases the inconvenience of flying. Using a smart card system to track bags with passengers getting on flights may make it possible to reinstate remote and curbside check in without adverse security consequences.

Such systems could also be used to address concerns with e-tickets. After their first flight, individuals could use the smart cards they were issued by a U.S. airline to book follow-up flights on the Internet. Biometric security devices can be easily installed on personal computers. For example, a small camera (or fingerprint ID mechanisms) can be attached to the PC (in fact, some new Sony PCs come with such a camera installed, and many other PCs come with a fingerprint reader for a small additional cost) along with a smart card reader. Before the person can purchase an e-ticket and have the ticket loaded onto their smart card, their biometric ID would be sent to the airline issuing the ticket to confirm that the person whose smart card is in the machine is indeed the same person at the terminal.

Second, aggressive deployment of biometric, smart card-based authentication systems at airports could give a significant boost to breaking out of the "chicken and egg" conundrum holding back the deployment of these technologies in the wider marketplace. For example, ubiquitous deployment of smart cards and digital authentication systems could have extremely large economic and productivity benefits, but their use is limited because it is dependent upon adoption by users and providers at the same time.

A case in point is online authentication. The full benefits of the digital era will not be realized until individuals can easily and securely authenticate themselves over the Internet. Currently, few Americans can do this; that is, they are unable to fully represent themselves over the Internet in a way that securely tells other people and companies that they are who they claim to be, or allows them to be taken seriously when they state their intentions. As a result, few companies or governments have developed applications that could use online authentication; and likewise, since few online applications require authentication, consumers have little reason to obtain the means to sign contracts, applications, and other documents digitally.

Smart cards are another chicken and egg technology. If airlines were to issue biometric authentication smart cards that were multi-functional (e.g., could contain not just biometric

information, but financial and other transactional information), this would jump start the market for these applications. For example, people could use them to book a flight online and at the same time check into hotels on the Internet, choose the room they want, and download the key code information directly to their smart card, allowing them to enter their room without physically checking in. When they return home, they could exit the parking garage by simply putting their smart card in the automated reader at the gate which would bill their credit card.⁶

Widespread deployment of biometric authenticated smart cards would also boost Internet security, since most sites now require little more than password identification. These cards could contain a host of different passwords, all of which would be activated once the biometric authentication proves the person is indeed the card holder.

This suggests that ***it is critical that any smart card or biometric technology employed at airports with federal funding be multi-functional and interoperable with other government or commercial systems.*** If these technologies are limited to only letting passengers board airplanes, the broader spillover economic benefits from such a significant investment will be vastly diminished. It is relatively easy to build these capabilities into a system at the beginning so that all related applications can be used with airport smart cards. Doing so would in no way reduce airport security, and would actually enhance security in other areas, most notably the Internet.

Such interoperability should also work the other way. Smart cards issued by U.S. government entities for other applications (e.g., as part of the processing of getting a state drivers license, or, as some have begun to propose, a national biometric ID card) should be allowed to be used for airports, as long as the appropriate level of authentication was used when issued. Such cards could also have multiple authentication certificates on them, each with a differing level of assuredness that the card holder is indeed who they are.

Third, at a time when the U.S. economy will almost surely enter recession, investments in new airport security technology will provide a needed stimulus to the economy generally, and the information technology sector specifically. It appears that the terrorist attacks will push an already weak U.S. economy into a recession in the third quarter of 2001, and that recovery, while inevitable, may not come for a while. Congress and the administration need to consider appropriate tax cuts and public expenditures to stimulate the economy. In this context, it is important to realize that technology investments to upgrade airport security will provide a needed stimulus to an industry already suffering.

Potential Concerns with Deploying Airport Security Technology

There are likely to be a number of concerns about a federal initiative to deploy advanced technologies to boost airport security. First, some may say that it is not needed and is instead expensive overkill. There is no doubt that employing advanced technology in airports, including facial biometrics, will not solve all security problems. More than technology alone is needed. However, what is clear is that as this technology gets more powerful and cheaper, it will eventually be deployed at airports. The question is whether we should deploy it now in response to these attacks, or wait for natural "market forces" to bring uneven and gradual adoption.

Second, some may be concerned that such technology is inaccurate. Clearly, any technologies deployed by the FAA, airports, and airlines would have to be thoroughly tested before any particular system is chosen. However, biometric technologies have improved

dramatically in the last few years as computer processing power has grown, and as a result, error rates have declined dramatically. In any case, if these systems make mistakes regarding passenger or personnel entry, they are much more likely to report false negatives than false positives. In other words, they are more likely to reject the right person than to accept that wrong one. In this case, the rejected person can be verified by human means. For example, AcSys Biometrics claims that in tests, their facial biometrics system demonstrated a false acceptance rate of 0 percent (it didn't let a known criminal slip through) and a false rejection rate of 3.1 percent (it misidentified non-criminals three times out of 100). In the case of fingerprint technology, the odds of a fingerprint being identical is approximately one in 900 million, suggesting almost no false acceptances.

Third, while the idea of “being a password” instead of remembering a password is intriguing to many Americans, and will go a long way toward boosting security, some, especially privacy advocates, find it disconcerting. Such systems are already in use to identify criminals in other public spaces, including Super Bowl XXXV in Tampa in 2001, and in public spaces in Britain. Privacy advocates and civil libertarians have complained that these systems represent the first step to an Orwellian big-brother state. Whether that is true, or whether it is simply a case of using technologies to automate legitimate police work, is beyond the scope of this paper. What is clear is that the use of authentication technologies in airports is fundamentally different. Individuals in airports, especially in spaces beyond security checkpoints, have no rights to privacy in the sense that they have already revealed their identities to get beyond security check points.

It is important to note that such systems can be used to minimize privacy concerns. For example, any multi-function smart cards that are used would almost certainly contain encrypted information and could not be read by the government. For example, airport scanners could not read a person's medical or financial records, which might exist on their card. In cases where information is not encrypted, it would be important to pass regulations stating that airport security (and other security systems) can only read the information needed to process the person (e.g. ticket and flight information, their biometric information, passport information, etc). Some camera systems only record images of “matches” with the crime databases. Other systems could be designed to delete all images that don't match up to crime databases after a certain period of time so that law enforcement could not track the movement of citizens around the nation at airports. Finally, if these systems are put in place, governments, airports, and airlines will need to educate the public on how these systems enhance security while protecting privacy and civil liberties.

Conclusion

New technologies, including better scanning and biometric authentication and identification are not a panacea to airport security problems. However, correctly deployed, they can play a key role in enhancing airport security, along with working to minimize the added inconvenience that new security measures will involve. In drafting and passing an airline security bill, Congress needs to take seriously the promise of technology, and allocate sufficient funds to upgrade the nation's airports for the 21st century.

Rob Atkinson is vice president of the Progressive Policy Institute and director of PPI's New Economy and Technology Project.

Endnotes

1. The New Economy Task Force, *Making the New Economy Grow: An Action Agenda*, Progressive Policy Institute, July 2000, www.ppionline.org.
2. To give a sense of the capabilities of smart cards, current generations contain more computer memory in a tiny, thin chip than was on the original Apple personal computers. Current generations of smart cards contain 32K of memory (a face scan may take up to only 5K of memory on the chip), while 64 K cards are now coming on the market. Given the fact that Moore's law shows no signs of slowing down, smart cards are likely to continue to expand their storage capabilities.
3. Biometric pilot authentication systems are clearly overdue, as it appears that at least one of the terrorists had a phony pilot's license.
4. Such a system would have the more mundane benefit of not allowing people, including unaccompanied minors, to board the wrong flight.
5. Limited versions of such systems are also in use to do background checks on ground personnel. An airline security bill passed last year required airports to streamline FBI background checks on personnel. In response to the bill, at least four airports, including Boston's Logan and Washington's Dulles, had already upgraded to an automatic fingerprint system for background checks (but not for access control). The system takes fingerprint images of prospective employees electronically, and instantaneously checks with FBI databases. However, neither airport, to our knowledge, uses these technologies to control access to secure areas.
6. Similar technology is now in use in commercial applications, most notably Mobil and Exxon gas stations, which use a small radio frequency transponder that automatically sends information to the pump about the credit card to be charged for the gas.

For further information about this or any other PPI publications, please call the publications department at 202/547-0001, write the Progressive Policy Institute, 600 Pennsylvania Ave., S.E., Suite 400, Washington, DC, 20003, or visit PPI's Web site at <http://www.ppionline.org>.