

# Using Technology to Detect and Prevent Terrorism

*by Shane Ham and Robert D. Atkinson*

On December 26, 2000, a small plane piloted by Mohammed Atta stalled on the runway at Miami International Airport. Atta (alleged ringleader of the September 11 attacks) and his companion (another future hijacker) simply abandoned the plane on the runway—on one of the busiest travel days of the year—and walked to the terminal to rent a car. On May 28, 2001, a criminal warrant was issued for Atta's arrest in Broward County, Fla., after he failed to appear in court for a traffic violation. On July 5, Atta was pulled over for speeding in Palm Beach County, Fla.; the officer ran a search on Atta and found no outstanding warrants. After a trip to Spain in which he allegedly met with co-conspirators, Atta entered the United States for the last time on July 19, despite the above incidents and despite the fact that he was on a terrorist "watch list."<sup>1</sup>

One of the most painful things about examining the events leading up to the September 11 hijackings is realizing just how close the terrorists were to having their plot disrupted. Fifteen years ago, stopping terrorism relied on old-fashioned tools: strict physical security at vulnerable facilities, intelligence gathering by government agents, vigilance on the part of all citizens, and a sense of community in which we all do what we can to protect each other. These are all still very important. At the dawn of the 21st century, however, we have a powerful new weapon: technology. The information technology revolution that transformed our economy has also given us the tools, infrastructure, and commercial capabilities to make domestic defense easier, less expensive, and more effective, making all Americans safer.

If we had had advanced IT tools in place prior to September 11, it is almost certain that some of the terrorists would have been detained, and possibly some of the plots would have been foiled.

Technology has revolutionized the economy with dramatic productivity improvements and an array of new communications and information processing tools. We must bring that same revolution to domestic defense, to gain maximum security and public confidence with minimum investment. The IT revolution has given us many tools—wireless data networks, encryption, powerful miniature computer chips, the global Internet, data mining software, and many more—that weren't available for domestic security just a few years ago. Now that we have these tools, it is time to roll them out to make our nation safer. In doing so, we can also expect many significant side benefits; just as technology investments during the Cold War had spinoff effects that helped start the New Economy, many of the investments to develop and deploy technologies for modernizing and upgrading our law enforcement and public service capabilities will result in significant economic, health, and public safety benefits.

The purpose of this issue brief is not to provide a comprehensive blueprint of how technology alone can solve the terrorism problem—it can't—nor is it to suggest that every domestic defense challenge has a technology answer. There are many pieces of our domestic security system that work well now, others for which low-tech solutions are less expensive but just as effective, and still others in which technology can never replace the judgment and

experience of a person. The purpose of this brief, rather, is to stimulate thinking about how technology can take domestic defense from its old economy model—bureaucratic, hierarchical and compartmentalized, and labor-intensive—and transform it to a New Economy model—flexible, networked, and automated. Among the ways technology can help find terrorists before they strike are:

- ▶ **improved data sharing**, combining criminal records and intelligence information from a variety of federal, state, and local agencies that can be accessed wirelessly to identify wanted criminals and suspected terrorists when they encounter law enforcement or attempt to enter secure facilities.
- ▶ **“smart ID cards” with biometric identifiers**, adding chips containing thumbprint scans or other biometric data to driver’s licenses, as well as standardized security features for preventing forgery and fraud;
- ▶ **“smart visas” and improved border security**, placing biometric information on visas to identify visitors, keep track of their entry and exit, and confirm compliance with the terms of their entry, and protecting unguarded stretches of the borders;
- ▶ **digital surveillance**, extending longstanding principles of law enforcement and surveillance to the Internet by permitting surveillance of email and other electronic data while preserving traditional safeguards on searches by government agents; and
- ▶ **face recognition technology** that can detect known terrorists as they move through crowds at vulnerable events such as the 2002 Winter Olympics.

## Using Technology to Detect and Prevent Terrorism

### *Data Sharing*

The investigation of the September 11 attacks has revealed a wealth of information that might have prevented some of the hijackings, or at least limited their impact, if we had been able to intercept the terrorists in time. Of the 19 hijackers who boarded the planes on September

11, only nine had valid visas, yet all were allowed to board. Six of the hijackers had apparently snuck into the country illegally, yet were allowed to board. One of the hijackers entered on a student visa, and though he never showed up for classes, he was never reported because the Immigration and Naturalization Service (INS) had stopped taking such reports in 1988. Atta received \$100,000 in suspicious wire transfers from overseas, but a report was never filed with the government. Most chilling is the story of Ramsi Binalshibh, alleged to be the “20th hijacker” who was allegedly replaced by Zacarias Moussaoui. Binalshibh tried to get a visa to enter the United States three times, but was denied because he was suspected of involvement with the 2000 bombing of the USS Cole. Apparently the FBI was not informed of these denials; if they had been, they might have followed up by investigating the Florida flight school where Binalshibh had made a down payment for lessons. Had the FBI done so, they might have questioned the student at that flight school who had tried to bring Binalshibh into the country: Ziad Jarrah, the pilot of the plane that crashed in Pennsylvania with only four hijackers aboard.

Of course, it is always easier to detect the patterns of a terrorist conspiracy in retrospect than it is before the conspiracy happens. Intelligence agencies have to process mountains of information, and in the case of Islamic terrorists, much of the information is in Arabic, limiting the number of analysts who can work on the data. But even if a conspiracy cannot be found in advance, stronger information sharing can still have domestic defense benefits. Moussaoui’s flight school instructors reported him to the FBI as a potential terrorist. Though there was not enough evidence to warrant searches of Moussaoui’s computer, he was detained on immigration violations. That detention, unrelated to suspicions of terrorism, may be the reason United Airlines Flight 93 had only four hijackers instead of five. The smaller number of hijackers, in turn, may have been critical to the passengers’ successful battle to bring down the plane before it could kill any more victims on the ground. If any of the other

hijackers who were in the country illegally or had legal troubles had been delayed in catching their flights, perhaps even more lives would have been saved. Moreover, many terrorist organizations support their activities through crime rings—drug trafficking, stealing luggage, creating fake identification documents, and so on. Any improvement in our ability to bust up those crime rings would have domestic defense implications.

A key piece of domestic defense, then, will be more effective use of law enforcement databases. Information sharing among law enforcement agencies has been a key challenge addressed by governments at every level. The FBI operates a national criminal database system under its Criminal Justice Information Services Division (CJIS). CJIS is responsible for several national databases that are queried by law enforcement agents nationwide on a daily basis, including the National Crime Information Center (NCIC), the Integrated Automated Fingerprint Identification System (IAFIS), and the National Instant Criminal Background Check System (NICS).<sup>2</sup> These databases allow law enforcement personnel in the field to run background checks on individuals who have been stopped or detained to determine if they are wanted for crimes in other jurisdictions, or if they belong to a gang or terrorist group.

Unfortunately, this system is not as comprehensive as it could be. The state and local agencies responsible for entering data into these systems do not always do so in a complete and timely manner. NCIC generally contains information only for serious crimes. It contains no information at all regarding immigration status. (In fact, the INS information systems are notoriously outdated.) By expanding the scope of NCIC and the state databases that feed it, law enforcement officers will have a better chance of picking up the small-time criminal or illegal alien who also happens to be a terrorist, while also improving law enforcement nationwide.<sup>3</sup>

The database is only as good as the information that goes into it, however. State and local governments will need to devote resources to improving their internal information exchange capabilities to ensure that NCIC has

timely and accurate data. Many states had efforts to develop such statewide databases underway long before September 11. One of the best examples is the Commonwealth of Pennsylvania Justice Network (JNET), which began nearly five years ago under the leadership of Governor Tom Ridge.<sup>4</sup> The JNET project aims to put criminal justice information from all relevant state, county, and local agencies into a single, searchable database. These efforts improve the quality of the data searched at the national level and make the system more efficient.<sup>5</sup> If cops on the street have immediate access to a broader range of information—ongoing investigations, conditions of parole, and the like—they are better able to make decisions on how to proceed with a given suspect.

Of course, intelligence agencies also have an important role to play in populating the NCIC. The CIA and the National Security Agency (NSA) use their own classified databases to gather suspicious information and identify potential terrorists.<sup>6</sup> The fact that an individual is a suspected terrorist can be reported to NCIC, but sometimes it is not because intelligence agents fear that their investigations may be compromised.<sup>7</sup> As domestic defense assumes a higher priority, the intelligence agencies should reconsider their criteria for “watch listing” potential terrorists to allow for disrupting their operations by pursuing seemingly unrelated crimes or immigration violations. Information sharing between intelligence agencies and law enforcement personnel in the field will be a vital part of domestic defense in the coming years.

The identification system could also greatly benefit from increased data sharing. Though state motor vehicle agencies do engage in limited information exchange (typically on bad drivers), it is still relatively easy to get ID cards under multiple identities in different states.<sup>8</sup> The 1998 highway bill<sup>9</sup> made a small appropriation for a feasibility study on improving information sharing among the motor vehicle agencies, a study that is still ongoing. The integration of these databases should be greatly accelerated. Any improved system should include the capture of a biometric identifier such as a thumbprint, not only to place into the ID card

itself but to prevent issuance of multiple ID cards with different identities to the same individual. (For more information on biometric smart ID cards, see below.)

Any expansion of database technology for law enforcement or domestic defense purposes inevitably raises questions of privacy. If developed properly, however, such databases can protect privacy better than the current system. The risk of privacy violation lies not in the integration of information that is already held by various government agencies but in the improper use of that information. Establishing secure access to electronic records not only keeps the data safe from unauthorized personnel (through the use of passwords, different access levels, and perhaps biometric verification), it creates a foolproof electronic "paper trail" to let supervisors know which information is being accessed by whom, something that is much harder to do with paper files. By increasing the odds that those who abuse the databases will get caught, such abuse (and therefore privacy violations) will be reduced.

Finally, the mark of a useful and effective database is how easily users can input and extract information. Since the bulk of the interaction with these databases will be by law enforcement personnel, state and local governments should make it a top priority to modernize police work by issuing police officers handheld computers. The computers could be used to access the NCIC from the field, a task that many police officers already perform on laptop computers installed in squad cars. The advantage of a handheld computer, however, is that it can also be used to gather information. Instead of copying information from a driver's license onto a sheet of paper, an officer could simply scan the driver's license to gather data about the driver (including verifying identity with a biometric scanner; see below), and scan a bar code on the license plate to gather information about the vehicle (including whether the plates are stolen).<sup>10</sup> Police officers fill out an amazing number of paper forms on a daily basis, which only makes information sharing more difficult and more expensive. Automating information gathering would make

it easier to enter information into a database; officers would simply plug in the handheld at the station house and upload the day's work. Handheld computers have brought considerable gains in efficiency to the delivery business and other industries, and if deployed properly could revolutionize law enforcement and domestic defense.

The improvement of data sharing, therefore, consists of two key efforts:

First is the integration and expansion of the "back end" data systems.<sup>11</sup> **As stated above, the NCIC should be expanded to accept more information from federal, state, and local agencies, and other databases (such as the DMV systems) should be more fully integrated to the extent practical and currently allowed by law. In addition, the administration should undertake a comprehensive study of the continuing relevance of laws and regulations governing interagency data sharing, with the goal of permitting greater sharing where appropriate to boost domestic defense.**

Second is the deployment of devices to access the databases. **Congress should fund matching grants to the states to facilitate the purchase of handheld computers or other devices that can both query and enter information into these databases. Because this should be done as part of a larger project to digitize law enforcement operations, funding should be contingent on state efforts to develop integrated, interoperable data systems with automated data collection.**

### ***Biometric ID Cards***

The Virginia Department of Motor Vehicles came under scrutiny last summer when it was revealed that illegal immigrants had fraudulently obtained ID cards by taking advantage of the fact that the state requires only notarized identity forms rather than firm proof of identity such as passports and local utility bills, as most states do. In August 2001, a woman was convicted for exploiting that loophole by providing false forms to thousands of illegal immigrants, many of whom were shuttled in from out of state by her accomplices. At that time, officials at the Virginia DMV said they were

reconsidering their policy—exposed as a loophole by the convictions of members of the fraud ring—but claimed that it was difficult to weed out false applicants without putting unnecessary barriers in the way of legal immigrants.<sup>12</sup> Twelve days after the ringleader of the ID card scam was convicted, American Airlines Flight 77 crashed into the Pentagon. Four of the five hijackers on that flight boarded using false ID cards obtained in Virginia by taking advantage of the state's lax policy.<sup>13</sup>

Nearly everyone who has purchased alcohol while under age, and certainly the planners of the September 11 hijackings, know how easy it is to get a false ID in this country. People can falsely identify themselves by simply borrowing a driver's license from someone with a similar appearance, downloading templates for fake ID cards from the Internet, or using false underlying documents such as forged birth certificates to get a legitimately issued card. The ease with which our "official" identity cards can be falsified is a public policy failure with implications far greater than 19 year olds buying tequila. False identification leads to billions of dollars in fraud every year, it allows wanted criminals to move freely, and it allows terrorists to plot attacks on the United States from within.

Technology exists today that can make ID cards much more secure, and some of it is already in use. For instance, many states imbed holograms of their state seals in the lamination of their driver's licenses and ID cards, and many states also print digital photos directly onto the card so they cannot be cut out and replaced. That security could be greatly enhanced, however, with the use of smart cards and biometrics.

Smart cards are simply cards that have been implanted with tiny computer chips that hold data. In addition to the biometric data written on the card (photographs, height, weight, and eye color), the chips can hold an encrypted version of a unique biometric identifier, such as a digital scan of a thumbprint or an iris. In situations where additional verification of identity is needed, such as traffic stops or airport security gates, the card holder could simply place a thumb on an inexpensive scanner and, by comparing the scan to the data in the smart

card, the scanner could verify both that the card is legitimate and that the presenter is its rightful owner. Because the digital biometric data is both unique and encrypted, it would be virtually impossible to create a fake ID card, though it would still be possible to fraudulently obtain a legitimate card. However, once a person has obtained identification, it will be impossible to switch identities, because the biometric data will confirm that person as the holder of a previous card.

To be effective for domestic defense, these ID cards would have to be developed to national standards, though they could still be issued by the states.<sup>14</sup> The cards should have a common look that could identify them as legitimate at first glance. Currently, anyone with a computer and a color laser printer can create a false ID card from, say, Connecticut that looks nothing like the real Connecticut cards but looks very official nonetheless. That card would not work well in Connecticut (where everyone has an official card in their wallet and knows what they look like), but could be taken as real in Montana, where few people are likely to have seen an official Connecticut ID card.<sup>15</sup> Standardized cards make it much more difficult to create convincing fakes.

Of course, no matter how secure the cards themselves are, an ID system is only as good as the initial verification of identity. If someone were able to get an ID card under an assumed identity, the anti-fraud features of a smart card would actually lead to a false sense of security. Another candidate for standardization, then, must be the regulations for identity verification when an ID card is issued.<sup>16</sup> Without standardization, the states with the most lax regulations become registration havens for illegal aliens and criminals.

To prevent this from happening in the future, the rules for initial identity verification must be stringent. For those who are unable to sufficiently prove their identity, the federal government should step in to conduct further investigations. For an individual whose driver's license has been lost or stolen, a thumbprint should be sufficient to prove identity. Those individuals who do not want to submit to a background check—because they are illegal

aliens or wanted criminals—will not bother trying to obtain official ID cards, thereby greatly restricting their ability to work and live unnoticed in the United States. These checks would not be inexpensive, but they would protect the integrity of the ID system and the domestic defense database to which it would be linked.

Reissuing identification cards to every citizen is something that will happen naturally; driver's licenses and ID cards expire periodically, and new cards must be issued. A rollout of biometric smart ID cards could therefore begin relatively quickly, and would be completed within several years. The American Association of Motor Vehicle Administrators (AAMVA) has already recommended many of these changes, but at this point does not support smart cards because they believe the "2-D bar codes" currently on many ID cards can encode enough data to carry biometric identifiers. But while this may fulfill the more narrow needs of state DMVs, it fails to take advantage of much larger opportunities, such as being able to use these cards in airports or for cash transactions, or to hold other information. Reliance on these advanced bar codes, even as an interim step before deployment of smart cards, will fail to take advantage of the significant economic and social benefits DMVs could stimulate by jump-starting the deployment of smart cards.<sup>17</sup> In addition, given that the information on the chip cards can be encrypted, they are likely to be more secure than bar-code cards.

Unfortunately, the few states that have investigated implementing smart cards for driver's licenses have encountered strong opposition from the public.<sup>18</sup> This opposition, along with other concerns such as cost, durability, and vulnerability to hackers, has led many states to believe that there is no good reason to adopt smart cards.<sup>19</sup> Ordinarily, the Progressive Policy Institute would be in favor of the federal government offering strong incentives to the states to overcome this opposition. However, in this instance, the need to establish secure identity cards is so compelling, and the economic benefits so large, we see no choice but to advocate federal

intervention in an area traditionally considered a state prerogative.

Therefore, **Congress should mandate that any standardization efforts by the state motor vehicle agencies include upgrading all ID cards to smart cards. In addition, Congress should provide matching grants to state agencies to deploy hardware that can read smart cards, and should fund pilot programs for states that seek to integrate multiple functions into the smart cards, such as voter registration.**<sup>20</sup>

### **Smart Visas**

An ID system for U.S. citizens would not be very effective for domestic defense if the system did not also apply to foreign visitors. In December 1999, for instance, Ahmed Ressam crossed the Canadian border into the United States on a ferry from Vancouver. He presented a legitimate Canadian passport under the name Benni Norris, and though U.S. agents on the Canadian side were suspicious, a computer check of Benni Norris showed no reason to detain him. (Under his real name, Ressam had been arrested four times in Canada, had a pending warrant for deportation, and was being investigated by the French and Canadian governments for being a terrorist.) It was only because a U.S. Customs agent in Port Angeles, Wash., voiced suspicions about his demeanor—causing Ressam to flee on foot—that Ressam was arrested, his car searched, and 100 pounds of white powder impounded as suspected narcotics. Thanks to this lucky break, the truth became known: Ressam had been trained in Osama bin Laden's terrorist camps, the white powder was actually a very powerful explosive, and Ressam was planning to set off a bomb at Los Angeles International Airport on New Year's Eve. The arrest of the so-called "Millennium Bomber" led to several other arrests, which probably disrupted other planned attacks and kept the celebrations in every city safe.<sup>21</sup>

We must make it more difficult for foreign visitors to enter under false identification. The biometric smart card system proposed for driver's licenses should therefore be extended to anyone wishing to enter the United States legally. (Ideally, Canada would develop a similar

interoperable system.) The current visa program should be upgraded to issue visas as smart cards with biometric data. Those countries wishing to participate in the visa waiver program—which allows their citizens to enter the United States without obtaining a visa—would be required to issue smart passports with biometric data.<sup>22</sup>

Just as with the ID system, smart visas are only as effective as the initial identity verification. The U.S. embassies that issue the visas must become the first line of defense in keeping potential terrorists out of the country. Access to data regarding suspected terrorists is an important part of that defense, but it may become necessary to impose stricter criteria for granting visas to enter the United States. If an individual seeking to visit the United States cannot prove beyond a doubt his or her identity and good standing, a visa should not be granted. Along those same lines, the U.S. government needs to take a closer look at the countries that participate in the visa waiver program to ensure that they are taking sufficient steps to combat ID fraud.

Once a smart visa has been issued, it should be used to ensure that foreign visitors do not overstay or otherwise violate the terms of their entry to the United States. Foreign students who enter on student visas should be required to attend school as promised. The smart visas should be scanned at entry and exit, thereby creating a record of which aliens have overstayed are still in the country illegally. Aliens with expired visas should have their expired status noted and reported any time they are required to show identification. The INS believes there are roughly 2 million aliens who entered the United States legally but did not leave when they were required to do so; smart visas would make it easier to find them and either update their status or deport them.

The visa issue aside, controlling the flow of people and goods across the borders was a key challenge long before the hijackings, but has taken on new urgency. Protecting the northern border is a particularly troubling issue. Canada is our largest trading partner, with \$1.3 billion worth of goods flowing across the border every

day; it is important to keep the border as open as possible. At the same time, Canada is considered something of a haven for terrorists due to its lax rules for granting asylum and extensive welfare benefits. The “Millennium Bomber” tried to enter the United States from Canada, and nearly made it.

In December 2001, the United States and Canada signed a “smart border” agreement that will use technology to enhance security while maintaining the ease of traffic flow across the border. The plan includes proposals to speed traffic by pre-approving travelers and cargo to cross the border using electronic identification technologies and sharing information on travelers who pose a security risk. The details of the agreement will be worked out over the next several months, but the basis of the plan is sound: Use technology to improve efficiency and security. Smart cards and biometrics will undoubtedly play a crucial role in the security of the northern border.

Technology deployment along the southern border is also important. Nondesignated crossing points (on both borders) could be observed with Web-linked cameras that detect motion or heat.<sup>23</sup> (Such cameras would also be useful in protecting the perimeters of sensitive infrastructure, such as nuclear power plants or drinking water reservoirs, by enabling a single guard in a room full of monitors to patrol miles of fence line.) Improved database access could also be very useful in guarding the borders. Border patrol agents equipped with portable fingerprint readers would be able to check the files of any illegal immigrant who is apprehended while sneaking across the border. The database could report to the agent in the field whether the individual has a clean record (in which case an escort back across the border is in order) or is wanted in connection with a crime or suspicion of terrorism. Keeping biometric records of each apprehension may also serve as a deterrent to recidivist illegal immigrants, some of whom cross the border illegally several times in a day.<sup>24</sup>

In the aftermath of the attacks, Senators Edward Kennedy (D-Mass.), Dianne Feinstein (D-Calif.), and Jon Kyl (R-Ariz.), among others,

authored bipartisan legislation (S. 1749) to improve the visa system. The legislation calls for the deployment of smart visas with biometric scanners at each point of entry by late 2003. **Congress should act expeditiously on the bipartisan smart visa bill.** With respect to border security measures, in December 2001 Congress appropriated \$113.7 million to the INS for technology projects and \$245.5 million to the Customs Service for staffing and technology investments.<sup>25</sup> This is an important start, but **Congress should boost funding to deploy technology hardware to border agents in the field. Congress should also give top priority to funding the development of the technologies called for in the U.S.-Canadian “smart border” plan.**

### ***Internet Surveillance***

Just weeks before the September 11 attacks, hijackers Mohammed Atta and Ziad Jarrah (both of whom were pilots in the hijackings) checked into a motel in Florida, carrying two laptop computers and several CDs. They demanded that the motel manager provide phone access so they could connect to the Internet with their laptops. The hijackers were so desperate to connect that when the motel could not provide the connection, they demanded a refund and left. In the weeks following the attacks, the FBI discovered that the Internet had been a key tool for the hijackers. Using both public terminals and their own equipment, the conspirators researched information about potential attacks and exchanged e-mails with operational details of the attack.<sup>26</sup>

The government has long had the highly restricted authority to conduct surveillance on electronic communications. Wire taps, phone traps and traces, and listening devices are accepted tools of law enforcement, though the tools are to be employed only under strict controls and judicial oversight. The recent anti-terrorism legislation signed by President Bush<sup>27</sup> extended many of those surveillance techniques to their Internet counterparts, but unfortunately there is still a good deal of unjustified concern about the new technologies developed for law enforcement over the Internet.

Two of the tools developed by the FBI have come under intense criticism. Carnivore (which has wisely been renamed DCS 1000) is a device installed, by court order, at Internet service providers to search email traffic. (Contrary to popular belief, the system does not search through the email of every customer looking for suspicious content.) By looking only for certain specific recipients or keywords in email sent by suspects, DCS 1000 saves time for agents by letting them focus their efforts on the e-mails that are most relevant, even though they would be entitled by court order to read all of the email that DCS 1000 searches. Magic Lantern and other “key logging” programs allow agents with search warrants to record every keystroke on a targeted computer. Reading the keystrokes can give agents passwords, which are critical when criminals are using strong encryption for their data and communications.

Without tools such as these, the old system of wiretapping is rendered all but useless—criminals will simply use Internet chats and encrypted e-mails rather than telephones. Despite their necessity, privacy advocates sound alarm bells because they fear that these tools will be used indiscriminately, without search warrants or court orders.<sup>28</sup> This, of course, is a legitimate fear, but it does not relate to the technology itself. The danger posed by these technologies’ being used without a warrant is no greater than the danger posed by an FBI agent entering a residence without a warrant; in other words, the danger is with the people, not the technology. Control over government agents will have to be exercised whether or not tools like DCS 1000 or Magic Lantern are deployed. **Given the increasing reliance on the Internet by terrorists and other criminals, we should address privacy concerns through proper procedure and judicial oversight, without throwing out key tools to monitor criminal use of computers and the Internet.**

### ***Face Recognition Technology***

Few law enforcement technologies have met with more public resistance than face recognition. The concept is simple: Cameras scan crowds to capture images of faces.

Computers then translate the facial geometry—the distances between the eyes and nose, for example—into a mathematical number. Those numbers are then compared with a database containing facial geometry numbers of known terrorists and criminals. If a match is found, the police are alerted and the suspect can be questioned. This technology has been used at the Super Bowl and is planned for use at the 2002 Winter Olympics in Salt Lake City. When properly developed, it could also be used to spot potential terrorists at airports and other secure facilities.

Most protests of privacy invasion relating to face recognition software are based on a misunderstanding of the technology. Many people believe that the cameras record their faces to create a record of where they were and who they were with, which is false. The technology simply checks faces against a database of people who are known to be dangerous, to see if terrorists or other criminals are lurking in vulnerable crowds. This technology is no different in principle from putting undercover counterterrorist agents into crowds to see if they can recognize anyone from photos they have memorized. The only difference is that the computers have a better memory and are therefore much more efficient.

Some people also object to the high mistake rate, which can lead to questioning of innocent people. These “false positives” are a concern, but one that can be dealt with through policy—police can decline to investigate unless the computer turns up a match with a high degree of certainty. The false positive issue will also become less important as the technology is improved.

The primary use for face recognition systems would be at private events: sporting events, concerts, or any event with that draws crowds and media attention (thereby becoming a vulnerable target for terrorists). **There are still serious technical questions about how well this technology will work and its effectiveness in preventing terrorism, but it is a promising technology that deserves further development and testing. Governments at all levels should therefore refrain from blocking testing and deployment of facial recognition technology.**

## Policy Principles and Considerations

Defending the nation against future terrorist attacks is a national priority that will be both complex and expensive. As a result, when considering how best to develop and deploy technology for domestic defense, it will be important to keep certain guiding principles in mind.

### ***Direct Anti-Terrorism Efforts Toward Systemwide Improvements***

As we make anti-terrorism a national priority, it is important to remember that the risk of terrorist attack is relatively low compared to other risks that we face every day. To focus on terrorism as if it were the only domestic security threat would be misguided. The best way to promote domestic defense is to dramatically improve the capabilities of law enforcement and other agencies that look after our safety and well-being every day.

For this reason, any decisions to develop and deploy technology in the fight against terrorism should be made with an eye toward how it will modernize and improve the everyday functions of domestic security. Updating the systems for emergency response, law enforcement information exchange, identification, and so on will reduce the risk of terrorism, but it will also help in responding to other disasters (fires, hurricanes, earthquakes) and do a better job of thwarting crime and apprehending criminals. As governments at all levels make decisions on how to invest in technology for domestic defense, when possible they should work to make sure that their investments will be applicable in a wide range of government functions.

### ***Recognize the Economic Benefits of Investment in Domestic Defense***

Governments should also consider the potentially significant ancillary economic benefits of investments in technology in the fight against terrorism. For instance, biometric smart card driver’s licenses or ID cards could give a significant boost to e-commerce and m-commerce (mobile e-commerce), by providing digital signatures that would allow people to

sign legally binding documents online, or by carrying digital cash, which would automate functions and payments (e.g., paying in airport parking garages, transit facilities, and others). Smart cards would also make security more convenient for Americans. For example, smart cards could enable “fast lanes” for low-risk individuals at secure facilities such as airports. (In fact, many Americans would warmly embrace biometric smart ID cards if systems were engineered to increase convenience for those who held them.) Smart cards are a critical technology for boosting productivity, but are vastly underestimated due to the chicken-or-egg problem: People don’t carry smart cards because nobody accepts them, and nobody accepts smart cards because people don’t carry them. If every driver’s license were converted into a smart card, applications would explode just as the World Wide Web exploded when the browser software was introduced.

Though not all of the technologies would have such an impact on the lives of every citizen, it is clear that modernization of systems critical to domestic defense can also give a boost to the economy. By focusing on other benefits as well as the fight against terrorism, money spent on technology will improve not only safety, but quality of life and productivity growth.

### ***Keep Privacy Issues in Perspective***

Using information technology to modernize our security and law enforcement systems will inevitably lead to complaints from privacy advocates. Unfortunately, concerns over privacy have been exacerbated by the Bush administration, particularly by Attorney General John Ashcroft, who in public statements and testimony before Congress sounded almost disdainful of the concept of privacy. But anyone who says we must sacrifice privacy for security presents a false choice; information technology can—and must—be deployed in a way that respects privacy while enhancing security.

The concept of privacy, however, must be kept in perspective. PPI has long recognized that privacy is not a defined absolute standard, but rather a series of tradeoffs between allowing individuals to keep some information to

themselves while permitting other information to be used for a variety of economic and social purposes.

When considering the use of information technology to keep track of terrorists and criminals, the visceral reaction by many citizens is to think of Big Brother or the “show us your papers” demands of the Nazis in old war movies. But it is wrong to think that the technologies presented here represent a leap into a futuristic dystopia where privacy doesn’t exist. Rather, these technologies are merely improvements on systems that we live with every day. For instance, embedding thumbprints in ID cards (which are all but mandatory in modern society) merely adds one more piece of biometric information to the photo and body statistics written on the cards; the only difference is that cards with biometric chips (and standardized security features) are harder to forge. A smart card merely holds more information than printed cards; in many ways, a wallet is a smart card: a single device for holding several functional items such as credit cards, ID cards, voter registration cards, and so on. (Although a smart card is even more private than a wallet—since it can be encrypted, contain firewalls between functions, and be set to operate only when biometrically verified—making stolen cards useless.) Databases are used to run criminal checks every day; adding more information, with proper statutory controls, would not be any more intrusive than a database that can tell a state trooper in Alabama that the person he just pulled over is wanted for rape in Maine. Seen as improvements on existing systems, reasonable people would agree that the privacy tradeoffs involved in increasing domestic security are well worth it.

New technology can also help protect privacy by making the collection of information more selective and more compartmentalized; for example, a program designed to read email can use keyword matching to select only relevant email from suspected criminals and leave the rest untouched. Automated information processing—such as algorithms designed to detect suspicious patterns in seemingly unrelated events—is good for privacy; the more

information is sorted by machine and rejected as irrelevant, the less it winds up in the hands of a government agent. Many people consider “identity theft” to be a privacy issue, especially in the online world, but the harder it is to create a fake ID (due to biometrics), the fewer the people who will have their lives invaded by identity thieves.

As a general principle, technology is neutral with regard to privacy. It is the rules governing the use of technology that matter. Privacy advocates and civil libertarians are right to focus attention on the rules under which technology operates, but to dismiss these kinds of technological advances as inherently destructive of privacy is mistaken. Within the proper set of rules, we can protect privacy while using technology to modernize government systems for domestic defense.

#### ***Focus Technology Procurement on Speedy Deployment and Interoperability***

When acquiring new technology, most government agencies assess their needs and go through a complicated procurement process that more often than not leads to a highly specialized proprietary system that is expensive, takes too long to get up and running, and is unable to work with other agencies. One example is the INS system for tracking aliens that enter the country on student visas, the Student and Exchange Visitor Information System (SEVIS).<sup>29</sup> Because student visas are a major source of immigration fraud, the goal of the program is to maintain current information on student visa holders, making sure they show up for school. The INS recommended in 1995 that the system be computerized. In 1996, Congress passed a law making the computerized system mandatory. Yet the system is not set to roll out until 2003. Some of the delay can be attributed to political interference,<sup>30</sup> but the time frame still is far too long; thousands of dot-com businesses have launched systems in a fraction of the time, with “back end” systems at least as complicated as the system INS is trying to roll out. There is simply no compelling reason why the government cannot implement these systems much more expeditiously.

This model for government procurement (along with the bureaucratic culture) is largely responsible for the “stovepiped” data systems that contributed to the intelligence failure of September 11. Had the data networks been more interoperable, and had systems such as SEVIS been in place, some of the hijackings might have been prevented. Government agencies at all levels need to significantly reengineer their procurement procedures.

When acquiring technology for domestic defense and other applications, agencies should focus not only on how the technology will suit their needs, but also on how easily the technology will interoperate with other agencies that have similar missions or functions. A premium should be placed on developing systems in which data can easily be exported into or accessed by other systems. Agencies should also focus on deploying the technology as quickly as possible. As a practical matter, these two requirements point to reforming procurement processes to focus on “off the shelf” technologies that have already been developed for use in the private sector, rather than developing new government-specific technologies.<sup>31</sup>

#### ***Coordinate Domestic Defense Research and Development***

Research and development to combat terrorism has rightly been a priority for the federal government in recent years, with funding for various projects more than doubling since 1998. These increases are appropriate and necessary, but there is a general consensus in the scientific community that the biggest problem now is not a lack of money but a lack of organization.<sup>32</sup> Funding for counterterrorism R&D is spread across many programs in many agencies: Defense, Energy, Justice, Commerce, Health and Human Services, and more. This is not surprising; unlike, say, cancer research, R&D for domestic defense covers a wide variety of technologies, from vaccines to network firewalls.

The danger, however, is that, without centralized coordination, the R&D efforts may become redundant or wasteful. The funding should continue to be distributed to the

appropriate agencies, where the experts can put it to use, but a clearinghouse should be established to ensure that the money is put to good use. The logical choice would be to give coordination authority to the director of the Office of Science and Technology Policy (OSTP).

## Conclusion

The losses caused by the September 11 terrorist attacks and the anthrax attacks will be with us forever. The nation feels the grief of the families who lost loved ones, and of the victims who survived but suffered grievous injuries. Though we cannot turn back the clock, we must do everything we can to prevent future attacks, and

to prepare ourselves in the event that our prevention efforts fail.

Information technology will play an important part in our anti-terrorism efforts. Just as we could not have won the war in Afghanistan without the benefit of high-tech weaponry, we cannot win the war against terrorism at home without high-tech systems and devices. With a renewed focus on domestic defense at all levels of government, IT can be deployed not only to stop terrorists, but to modernize many of our government systems, from law enforcement to emergency response to public health. Through proper investments in technology, we can bring domestic defense into the Information Age and save lives.

*Shane Ham is the senior policy analyst for the Progressive Policy Institute's Technology & New Economy Project. Robert Atkinson is vice president of the Progressive Policy Institute and director of the Technology & New Economy Project at PPI. The authors would like to thank the following individuals for sharing their expertise during the development of this report: Gerald Epstein, scientific advisor with the Defense Threat Reduction Agency, and Mark Tanner and Roy Weise of the Federal Bureau of Investigation.*

---

For more information on this or any other PPI publication, please call: (202)-547-0001, write: The Progressive Policy Institute, 600 Pennsylvania Avenue SE, Suite 400, Washington, DC, 20003, or visit our site on the World Wide Web at <http://www.ppionline.org>.

## Endnotes

1 In the days after the attack, several published reports stated that Atta was on a CIA watch list. In the following weeks, new reports citing anonymous officials claimed that Atta was never on a watch list and that in fact the CIA does not maintain a watch list. Because this information is classified and the reports rely on anonymous sources, the general public may never know the facts.

2 For more information on these databases, see the CJIS home page at <http://www.fbi.gov/hq/cjisd/about.htm>.

3 For a comprehensive list of the information covered by NCIC, see <http://www.fas.org/irp/agency/doj/fbi/is/ncic.htm>.

4 <http://www.pajnet.state.pa.us/jnet/site/default.asp>.

5 To ensure the accuracy of a “hit” on NCIC, law enforcement agents are encouraged to verify the information with the reporting agency. Improved information systems such as JNET can streamline the verification process.

6 Intelink, the intelligence agency information sharing system, has been online since the mid-1990s. For more information, see <http://www.fas.org/irp/program/disseminate/intelink.htm>.

7 Suspected terrorists who know they are under surveillance by intelligence agencies might cease activities that could lead to undiscovered cells, or might even generate false intelligence on purpose. Intelligence agencies, therefore, are wary of reporting a suspected terrorist to NCIC lest a law enforcement agent accidentally reveal to the suspect that he is under observation.

8 An interstate compact mandates that states require all applicants who claim to have no prior driver’s license or ID card issued in another state to submit a notarized statement to that effect. However, there is no method for verifying the truth of such statements.

9 Transportation Equity Act for the 21st Century (TEA-21), P.L. 105-178.

10 To be effective, nationwide standards would have to be set for how information is encoded on driver’s licenses and license plates.

11 The term “integration” can mean either building software links between existing databases or building entirely new databases to which existing databases can publish their information. Which of these methods is appropriate is a technical question, and the answer varies depending on the application. Any federal, state, or local agencies that develop new data systems or upgrade their current systems should build their systems with both possibilities in mind, no matter how unlikely it seems in the present that a system will be integrated with others (e.g., top secret databases for which data sharing is not currently part of the plan).

12 Brooke A. Masters, “Va. Notary Convicted in ID Scam; Immigrants Bought False Documents,” *Washington Post*, August 31, 2001, p. B01.

13 Brooke A. Masters, “Hijackers Exploited DMV Loophole,” *Washington Post*, September 21, 2001, p. A15.

14 States could still use biometric ID cards the way they currently use driver’s licenses, but with the smart card capability they could also consolidate a number of other government functions into one card, such as voter registration, library cards, hunting licenses, “smart” food stamps, and so on.

15 This is why many bartenders use thick books with photos of ID cards from all 50 states to make sure the ID they're checking is a real one. It would be impractical, however, to issue such books (or CD-ROMs) to every person who looks at ID cards, from police officers to retail clerks.

16 One way driver's license bureaus have done this is by implementing instant online verification of Social Security numbers.

17 State DMVs should also leverage their identity verification into secure digital signatures, as PPI recommended in "Jump-Starting The Digital Economy." [http://www.ppionline.org/ppi\\_ci.cfm?contentid=1369&knlgAreaID=140&subsecid=288](http://www.ppionline.org/ppi_ci.cfm?contentid=1369&knlgAreaID=140&subsecid=288).

18 New Jersey and Utah both abandoned smart card plans, the latter at least in part because some Utah residents considered smart cards to be an international conspiracy or the biblical "mark of the beast." Brook Adams, "Utah Firm Advances Technology," *The Deseret News*, August 13, 1997.

19 A 1999 report by AAMVA on smart cards concludes that there is "no strong business case for the use of smart cards in either driver licensing or vehicle registration applications at this time." <http://www.aamva.org/Documents/stdSmartCardFinal.pdf>

20 Because private companies would also seek to deliver their services using smart ID cards, states could help defray the cost by charging a fee to any company that loads an applet onto the card. In turn, the companies would save money by not having to issue their own smart card or key fob.

21 The saga of Ahmed Ressay, and the weaknesses in Canadian immigration and identification policies that let him operate freely, was detailed in an episode of the PBS program *Frontline* in October. For more information, see <http://www.pbs.org/wgbh/pages/frontline/shows/trail/>.

22 Under a bipartisan compromise bill on visa reform introduced in the Senate (S. 1749), visa waiver countries would only have to report stolen passports, rather than require biometric identification.

23 Based on current use of such cameras, the coverage would not be airtight. False positives can sometimes be generated by wildlife, and a lack of manpower can make it difficult to intercept people who illegally cross the border even when detected by cameras. However, the deterrent effect of such cameras can be valuable.

24 Deterring illegal crossings on the Mexican border not only promotes domestic defense, but can also reduce the danger to the foreign citizens who risk their lives every time they make an illegal crossing through the inhospitable deserts of the Southwest.

25 The Customs Service appropriation will not be made available until the agency submits a comprehensive plan for its use.

26 David S. Fallis and Ariana Eunjung Cha, "Agents Following Suspects' Lengthy Electronic Trail; Web of Connections Used to Plan Attack," *Washington Post*, October 4, 2001, p. A24. This article provides an excellent summary of the hijackers' Internet use and the challenges faced by the FBI in following their electronic trail.

27 The USA PATRIOT Act, P.L. 107-56.

28 Some cyberlibertarians fear a general "dumbing down" of privacy expectations if we extend surveillance techniques that have long been used in the offline world to the Internet. For an excellent example of this reasoning, see [http://www.eff.org/Privacy/Surveillance/Carnivore/20000728\\_eff\\_house\\_carnivore.html](http://www.eff.org/Privacy/Surveillance/Carnivore/20000728_eff_house_carnivore.html).

29 SEVIS is being developed under the auspices of the Student and Visitor Exchange Program (SEVP). For more information, see <http://www.sevp.net>.

30 For an excellent summary of the political considerations that delayed this program, see Michael Hedges and Kathryn Wolfe, "Delayed system halted efforts to track foreign students," *The Houston Chronicle*, October 7, 2001, p. A25.

31 Procurement reform is an extremely knotty issue, as might be expected given the amount of money at stake: The federal government alone procures about \$200 billion worth of goods and services every year. Steven Kelman, administrator of the Office of Federal Procurement Policy under President Clinton, wrote a gripping account of the political struggle involved in procurement reform at the federal level. <http://www.ksg.harvard.edu/innovat/occasional/kelman.pdf>.

32 Andrew Lawler, "The Unthinkable Becomes Real for a Horrified World," *Science*, September 21, 2001, p. 2182.