

# BALANCING SECURITY AND LIBERTY IN THE WAR ON TERROR

**Gregory F. Treverton**

The debate over civil liberties in the war on terrorism remains remarkably ill-defined.<sup>1</sup> It sometimes has been shrill but almost always has been unfocussed. For some critics, looking at specific instances, the country is already far down the slippery slope to losing cherished liberties. Others, looking at the same evidence, see mistakes and over-reactions but conclude that, on balance, the nation has done pretty well at not trampling on those liberties. In part, the difference reflects differing interpretations of particular events: What for some is a mistake of the sort inherent in large organizations looks to others like the tip of a sinister iceberg.

More fundamentally, however, the nation is rethinking a set of organizational distinctions and procedural restraints that it developed during the Cold War. It came, haltingly but in the end firmly, to a striking of the balance between security and civil liberties. September 11th demonstrated that the nation faces a very different threat, one that compels a rethinking of the balance, which is and will be as halting as the Cold War process of striking it. Moreover, the balance that was struck combines organizational distinctions with constitutional protections with restraints on official discretion. As a result, the rethinking involves how government organizations relate to each other, to the Constitution and to citizens.

## STRIKING THE COLD WAR BALANCE

By the mid-1970s, if the period still seemed one of high Cold War, at least the Communist threat on the home front had faded. In that context, the nation's firstever investigations of intelligence uncovered

abuses of the rights of Americans, especially in a curious mixing of intelligence, or counterintelligence, and law enforcement at the FBI during J. Edgar Hoover's long tenure as director.<sup>2</sup> The justification and ostensible target of these "counterintelligence programs," COINTELPRO in Bureau acronym, was the operations of hostile foreign intelligence services.<sup>3</sup> But most of COINTELPRO's specific targets were American citizens, in civil rights and anti-war groups. People like Rev. Martin Luther King were not only surveilled but harassed, and worse.

In reaction to the revelations, if the Communist threat at home had ever justified intrusive surveillance of Americans, it was judged to do so no longer. The domestic intelligence activities of the FBI were sharply restrained, and the Chinese wall separating intelligence from law enforcement was built higher. A compromise between presidential discretion and civil liberties resulted in the creation of the Foreign Intelligence and Surveillance Court (FISC), a court operating in secret to grant covert wiretap and other surveillance authority for intelligence – as opposed to law enforcement – purposes. Before FISC, presidents had claimed the right of searches for national security purposes with no warrants whatsoever.

Yet if the investigations of the 1970s were the final act in striking the Cold War balance between security and liberty, they rested on a longer history of postwar institution building. In an important sense, it should not be surprising that cooperation between the CIA and the FBI before September 11 was ragged at best. We wanted it that way. Out of concern for our civil liberties, we decided the two agencies should not be too close. The FBI and CIA sit astride the fundamental distinctions of the Cold War – distinctions between intelligence and law enforcement, between foreign and domestic and between public and private. The distinctions run very deep.

Those distinctions were not imposed by nature; rather, the United States mostly chose them for good, practical and constitutional reasons. They did not serve us badly during the Cold War, but they set us up to fail in an era of terror. Now, the rebalance means not just reshuffling intelligence and law enforcement organizations, and refashioning their cultures, it means rethinking basic categories of

threat and response.

Law enforcement and intelligence are very different worlds, with different missions, operating codes and standards. Intelligence, what John Le Carré refers to as "pure intelligence," is oriented toward the future and toward policy – that is, it seeks to inform the making of policy.<sup>4</sup> Living in a blizzard of uncertainty where the "truth" will never be known for certain, it seeks to understand new information in light of its existing understanding of complex situations. Thus, its standard is "good enough for government work." Because intelligence strives above all to protect sources and methods, its officials want desperately to stay out of the chain of evidence so they will not have to testify in court.

By contrast, law enforcement is oriented toward response. It is after the fact. Its business is not policy but prosecution, and its method is cases. It strives to put bad guys in jail. Its standard is high, good enough for a court of law. And law enforcement knows that if it is to make a case, it must be prepared to reveal something of how it knows what it knows; at least it is aware that it will face that choice. It has no real history of analysis; indeed, the meaning of the word "intelligence" is different for law enforcement, where it means "tips" to finding and convicting evil-doers more than looking for patterns to frame future decisions. Law enforcement and policing also traditionally have been defined in geographical units. These definitions are more and more mismatched to threats, like terrorism, that respect no geographical boundaries.

A second distinction, that between foreign versus domestic, magnifies the intelligence-law enforcement disconnect. American institutions and practices both during and prior to the Cold War drew a sharp distinction between home and abroad. The FBI had conducted wartime espionage and counterespionage in Latin America, and in December 1944 Hoover had proposed that the FBI run worldwide intelligence operations on the lines of its Latin American operations.<sup>5</sup> The proposal had some support outside the FBI, at the State Department in particular. But President Harry Truman worried openly that giving the intelligence mandate to the FBI would risk creating a "Gestapo-like" organization, and so foreign operations went first to the Central

Intelligence Group, CIA's predecessor, and then to the CIA. Both, however, were barred from law enforcement and domestic operations.

Relations between the two agencies were ragged from the start, and by the 1970s, it was literally true that the directors of the CIA and FBI didn't speak to one another. The National Security Act of 1947 was clear in proscribing the police function for the CIA. The National Security Agency (NSA), created later, was and is also barred from law enforcement and from domestic spying, so if the trail of conversations or signals it is monitoring becomes "domestic" – that is, involves a U.S. person, corporation or even resident alien – then the trail must end. The FBI was required to provide information to the Director of Central Intelligence but only if that information was "essential to the national security," and only "upon the written request" of the DCI. The FBI also was responsible for protecting material before federal grand juries, and while sharing was possible, in practice information came to be shared only with a court order. Both these sets of provisions were an invitation for the FBI to hoard information.

A third distinction is public versus private. During the Cold War, national security was a government – federal government – monopoly. To be sure, private companies and citizens played a role, but for most citizens, fighting the Cold War simply meant paying their taxes. That does not seem likely to be so for the campaign against terrorism and for homeland security. Civilians' lives will be affected – ranging from the inconvenience of waiting in long lines at airports, to harder questions about how much security will make use of pre-screening, national databanks and biometrics. Across the country, there are three times as many "police" in the private sector as in governments.

All three of these distinctions were all too vividly on display before September 11. According to the joint Senate-House investigation of September 11, the CIA's procedures for informing other agencies – FBI, State, NSA and the Immigration and Naturalization Service (INS) – of suspected terrorists were both restricted and haphazard.<sup>6</sup> By its own guidelines and later by a January 2001 memorandum of understanding, the CIA was supposed to notify at least the FBI and NSA of all people it suspected as terrorists. In fact, it seems only to have put people on the watch list if it also had information that they

were about to travel to the United States – a much more restrictive criterion. Moreover, in the investigation's words, the CIA "apparently neither trained nor encouraged its employees to follow its own rules on watchlisting." The number of names the CIA put on the watch list soared after September 11, from 1,761 during the three months before September 11 to 4,251 in the three months afterwards.

The ragged connections between the CIA and FBI were all too graphically illustrated by their misdealings over the Al Qaeda-affiliated terrorists Khalid al-Mihdhar and Nawaf al-Hazmi. Needless to say, the saga of what the two agencies told each other and when was played out in leaks and counter leaks during 2002.<sup>7</sup> The two men attended a terrorist meeting in Kuala Lumpur, Malaysia, in early January 2000. This meeting was known to – and surveilled by – the CIA, which already knew that al-Mihdhar possessed a multiple-entry visa permitting him to travel to the United States. NSA had independent information that linked al-Hazmi to Al Qaeda. Neither the CIA nor NSA, however, saw fit to provide their names to the main watch list, the so-called TIPOFF database.

There is apparently some confusion over whether the CIA told the FBI anything about al-Mihdhar and al-Hazmi. CIA e-mail traffic reviewed by the joint congressional investigation, however, suggests that the CIA did brief the FBI in general terms. The CIA, however, still did not bother to tell the FBI that al-Mihdhar had a multiple-entry visa that would allow him to enter the United States.

In early March 2000, the CIA learned that al-Hazmi had arrived in Los Angeles on January 15. Despite having just learned of the presence in this country of an Al Qaeda terrorist, the CIA apparently did not inform other agencies. Indeed, the internal cable transmitting this information contained the notation: "Action Required: None, FYI." This information came at hard on the heels of the intelligence community's alarm over possible "millennium plots" by Al Qaeda. Al-Hazmi arrived, moreover, at about the same time the CIA knew that Al Qaeda terrorist Ahmed Ressam was also supposed to have arrived in Los Angeles to conduct terrorism operations. Still, however, the CIA refused to notify anyone of al-Hazmi's presence in the country.

By this point, both al-Mihdhar and al-Hazmi – both terrorists known to the CIA – were living in San Diego under their true names. They signed these names on their rental agreement, both used their real names in taking flight school training in May 2000, and al-Mihdhar even used his real name in obtaining a motor vehicle identification card from the State of California. In July 2000, al-Hazmi even applied to the INS for an extension of his visa, sending in this application using both his real name and his current address in San Diego (where he would remain until that December). INS, of course, had no reason to be concerned, since the CIA had withheld the two terrorists' names from TIPOFF. Nor did the FBI have any reason to look for them – for instance, by conducting a basic Internet search for their names or by querying its informants in Southern California – since the last it had heard from CIA was that these two terrorists were overseas.

The CIA's failure to put al-Mihdhar and al-Hazmi on the watch list became even more inexplicable in January 2001, when the CIA discovered that a suspect in the *USS Cole* bombing also had attended the Malaysia meeting. This might have been taken as some confirmation that the two terrorists had links to Al Qaeda operational cells, thus making them still more of concern – but the CIA still did not bother to inform TIPOFF. This failure was particularly damaging because al-Mihdhar was overseas at the time: putting his name on the watch list would have enabled INS agents to stop him at the border.

Even when given the opportunity to tell the FBI – in face-to-face meetings – about the presence of these two terrorists in the United States, the CIA refused. At a meeting in June 2001 with FBI officials from the New York Field Office who were working on the *USS Cole* case, a CIA official refused to tell them that al-Mihdhar and al-Hazmi had come to the United States.

Meanwhile, Khalid al-Mihdhar, in Jeddah, Saudi Arabia, applied for a new U.S. visa in June 2001. But since neither man was on the TIPOFF list, his name did not appear when the State Department officials who took this application checked his name against their database, which incorporates TIPOFF watch list information. And so al-Mihdhar was given a visa and returned to the United States unmolested in July.

The CIA finally put al-Hazmi and al-Mihdhar on the watch list in late August 2001, by which point they were already in the United States and in the final stages of preparing for the September 11 attacks, and it also added the names of two others who were expected to try to enter the United States. Apparently, the FBI did little with the information, and also failed to share it with INS until the INS had already admitted the other two into the country. Questioned about its failure to follow up on this cable, one FBI official said, “If the cable says, “Don't let them in the country, and they were already in the country, what's the point of bringing this up now?” In any event, the FBI failed to locate Khalid al-Mihdhar and Nawaf al-Hazmi, who hijacked the jet that crashed into the Pentagon on September 11.<sup>8</sup>

The FBI did try to find the two but was hampered by some combination of its own regulations and the prevailing view that terrorism was a second-order mission, especially in the United States. The Bureau did not shift agents to counterterrorism from its primary law enforcement mission. Nor did it search the Web for information that would have revealed al-Hazmi and al-Mihdhar living under their true names in San Diego. On October 18, the *Los Angeles Times* reported that a simple check of public records and addresses through the California Department of Motor Vehicles would have disclosed the correct location of the two hijackers. A check with credit card companies would have shown air ticket purchases and given their correct addresses.<sup>9</sup> (According to testimony before the congressional investigation from an FBI agent in New York who also conducted such a search after the September 11 attacks, finding al-Mihdhar's address could have been done “within hours.”) The Bureau also did not ask help from Treasury officials in tracking down al-Mihdhar and al-Hazmi through their credit card or banking transactions.

A State Department official testified that the FBI had refused for a decade to provide the INS with access to its National Crime Information Center Database, on the grounds that the INS is not a “law enforcement” organization. Nevertheless, an internal FBI review concluded that “everything was done that could have been done.”<sup>10</sup> Before September 11, the “standard FBI line” according to one source who spoke to *New Yorker* writer Joe Klein was that “Osama bin Laden wasn't a serious domestic security threat,” pre-

sumably because his earlier attacks had been abroad, not at home.<sup>11</sup>

No agency told the Federal Aviation Administration (FAA) to be on the lookout for the four men, apparently because it, too, was not in the law enforcement business. And the airlines were not informed because they were private, not public. A European official testified to the effect of these oppositions on the sharing of information with the United States: “those we have been arresting are people we knew about before [September 11] but never thought were particularly dangerous to us inside our national boundaries.”<sup>12</sup> And so the two hijackers flew their plane into the Pentagon on September 11.

This sad tale is often taken as one of fights over bureaucratic turf or the control of information as power (or, perhaps, simple incompetence). Both turf and secretiveness played roles, but from my interviews and experience, the story really is one of very different cultures that were not used to cooperating closely and were not sure how much they should.<sup>13</sup> Cautious interpretations of the wall between intelligence and law enforcement had let that wall become very high. For instance, former CTC chief Cofer Black later testified before Congress that the CIA’s refusal to tell the FBI about the two terrorists loose in the United States had been entirely consistent with “rules against contaminating criminal investigators with intelligence information.”<sup>14</sup> Apparently, part of the reason the FBI did not shift law enforcement investigators to the search for the two was its interpretation of the wall: information could be passed from intelligence to law enforcement only if it contained strong indications that a law had been broken.

Very different cultures compounded the effect of the wall. For instance, FBI agents have Top Secret clearance, but few are cleared into the Special Compartmentalized Information (SCI) that is the woof and warp of intelligence. So, when faced by unfamiliar FBI counterparts in meetings, CIA officers would be sincerely uncertain how much they could say, and vice versa for different reasons for the FBI agents. The safest course was to say nothing. If the conversation turned to matters domestic, then the CIA officials would also be uncertain how much they should *hear*.

Cooperation between the two was probably best in the DCI’s Counterterrorism Center (CTC), and the limits even there were suggested by the handling of the terrorist watch list. Because CTC was an intelligence organization, it was and is oriented abroad. It was also heavily operational, seeking to disrupt terrorist networks, again abroad. To the extent that law enforcement was a tool in that foreign task, that, too, was welcome – though CIA agents would be careful to stay out of the chain of evidence. The CTC was terrain on which cooperation between the two agencies was easier than it was in following terrorists in and out of the United States.

## **THE FBI AND THE PRIMACY OF LAW ENFORCEMENT**

If the story of the two Pentagon hijackers is testimony to the limited cooperation across intelligence and law enforcement, and across foreign and domestic, the Phoenix memorandum and the Moussaoui case speak to other aspects of the Cold War legacy, in particular the mission and practices of the FBI. The Bureau was – and is yet – pre-eminently a law enforcement organization, though Director Robert Mueller is driving a change in the FBI mission to prevention and intelligence. It was and is dominated by special agents, and those agents naturally were attracted to where there were “collars” to be made – that is, criminals to be caught – and that was not terrorism, for terrorists ultimately might commit but one crime. Accordingly, the FBI viewed the world through the lens of the *case* and *case file*. If information was not relevant to making a case, it was not of much account.

An FBI special agent in the Phoenix field office sent the electronic communication, or EC in FBI parlance, to FBI headquarters on July 10, 2001.<sup>15</sup> The EC warned about potential dangers from Al Qaeda-affiliated individuals training at U.S. flight schools. The memo was sent to the Usama bin Laden Unit (UBLU) and the Radical Fundamentalist Unit (RFU) within the Bureau’s counterterrorist organization. Headquarters personnel, however, decided that no follow-up was needed, and no managers actually took part in this deci-

sion or even saw the memorandum before the September 11 attacks. The CIA was made aware of the Phoenix special agent's concerns about flight schools, but it offered no feedback despite the information the CIA possessed about terrorists' interest in using aircraft as weapons.

Nor did the new FBI officials who saw the Phoenix EC at headquarters ever connect these concerns with the body of information *already in the FBI's possession* about terrorists' interest in obtaining training at U.S. flight schools. The full contents of the "Phoenix Memo" have yet to be made public, but it is stunning that so little was made of it, especially since it drew attention to certain information already in the FBI's possession suggesting a very specific reason to be alarmed about one particular foreign student at an aviation university in the United States.

That student was Zaccarias Moussaoui, the suspected "20th hijacker," who was arrested on August 16 in Minneapolis for a visa violation. FBI agents at the field office suspected him of terrorism and sought, with increasing desperation, to search his laptop computer but were denied permission by FBI headquarters. To get permission for a FISA search or wiretap, FBI field offices request them through headquarters and the Department of Justice's Office of Intelligence Policy and Review (OIPR), with formal requests approved in secret by the FISC. Reportedly, the FISC has turned down just one Justice Department request for authority, out of 12,000.<sup>16</sup> All of the 1228 requests submitted in 2002 were eventually approved.<sup>17</sup>

That raises the concern that the FISA bar may be too low. The Moussaoui case, however, suggested that in practice, if not in law, the Bureau and Justice Department may have set the bar too high. In the event, headquarters and FBI lawyers briefed orally by the agent handling the case felt there was not enough evidence for a FISA search.<sup>18</sup> In the process, the standard apparently applied was that there had to be "probable cause" that Moussaoui was an "agent of a foreign power," which in turn was interpreted to mean linked to an already "recognized" terrorist organization – which Moussaoui was not because his link to Al Qaeda was as yet unknown.

In fact, the standard applied was more demanding than the law, which required probable cause (that is, substantial basis) that the targeted person be an "agent of a foreign power," which in turn was defined as "any person who...knowingly aids or abets any person in the conduct of [certain] activities." Those activities include "international terrorism," and one definition of "foreign power" includes groups that engage in "international terrorism."<sup>19</sup> Moreover, those making decisions on the Moussaoui case never saw the now-famous electronic communication from the Phoenix field office, which arrived at headquarters in late July. The warnings in that communication about suspicious activity at U.S. flying schools would have buttressed concerns about Moussaoui's own flying lessons.

The Moussaoui case can be seen as a testament to sloppy procedures, poor information technology, tensions between FBI field offices and headquarters, excessive caution or simple ignorance about complicated points of law, or all of those in some combination. It also may be that previous tensions between the FBI and the FISC had a "chilling effect" and made for more caution. So it was alleged in the letter from Special Agent Coleen Rowley to FBI Director Robert Mueller, May 21, 2002.<sup>20</sup> In any event, the case surely bespeaks considerable, perhaps excessive, caution on the part of the FBI and Justice in venturing FISA requests onto new terrain. Foreign spies were one thing; foreign "students," even ones with worrying connections, were quite another.

The Moussaoui case underscores what Senator Richard Shelby labels the "tyranny of the case file."<sup>21</sup> That culture, if not tyranny, can hardly be overstated. Because the FBI was and still is a law enforcement organization, its agents are trained and acculturated, rewarded and promoted within an institutional culture whose primary purpose is to catch and prosecute criminals. Within the Bureau, information is stored, retrieved, and simply *understood* principally through the conceptual prism of a "case" – a discrete bundle of information that is constructed to prove elements of crimes against specific potential defendants in a court of law.

That culture is powerful and it pervades the entire organization. It is reflected at every level and in every area. It contributes to the

autonomous, decentralized authority and traditions of the field offices, which is sharper in the FBI than in any government organization I have known. It is that way for a good reason: the criminals to be caught are in the field, not at headquarters. Before September 11th, money was allocated and careers made through criminal investigations, not long-term analysis or other work. “Intelligence” in the Bureau’s practice was tips to finding and catching evil-doers; it was not the assembling of a broad mosaic of understanding. Producing clear, evidence-based narratives that would indict criminals was prized; drawing “iffy” inferences based on fragmentary information in order to support decision-making was not. Given a choice between more agents on the street and better technology, the culture opted for the former, resulting in the FBI’s famously backward technology. It is, in the words of one investigator, “where the [IBM] 360s went to die,” or as an FBI agent put it to me, “we took the dirt road alternative to the information superhighway a generation ago.”

Given the tyranny of the case file, suppose, as a senior FBI counterterrorism agent put it to me, the FBI had done better at connecting the dots about flying lessons in the summer of 2001. His account is self-serving but with merit. What could the FBI have done? No crime had yet been committed, for taking flying lessons is not a crime, not even for Middle Easterners and not even if they are uninterested in landings and take-offs. Suppose then that the FBI had started knocking on doors of flying schools asking to interview Middle Eastern students – all without a crime or case. How far would it have gotten, at a time when Justice was suing local police departments over racial profiling? The question is a haunting reminder of the force of the Cold War distinctions and the law enforcement mission of the FBI.

In addition, while the distinctions have softened over time, still the gap at the FBI between special agents and “support” is a yawning one. Activities not primarily performed by agents have been given less priority and resources, never mind whether those other activities are filing, or doing science or analyzing intelligence. Put more crudely, if you don’t carry a gun at the Bureau, as agents do, you are a second-class citizen. The agents are a “Band of Brothers,” now including many sisters. The Band makes for powerful capacity. As one agent put it to me: “when you go out the door on an operation, you don’t

have to look over your shoulder to see if anyone is with you. They are.”

As with most powerful cultures, however, the pluses and minuses of the FBI culture are the same attributes. Agents shared information easily within the Band – perhaps too easily, as is suggested by the case of agent Robert Hanssen, who spied for the Soviet Union and Russia. However, FBI agents were not distinguished before September 11 by their willingness to share *outside* the Band. The Bureau brought, and brings, state and local police officers to work with it but does so very much on its terms, as members of FBI joint task forces, with clearances to match.

The culture and case file mind-set meant that information the FBI collected either was or wasn’t relevant to the case it hand. If it was, it often disappeared into federal grand juries. Before the USA Patriot Act of November 2001, it took a court order to share that information with anyone, including CIA analysts (who of course usually would not know what information was there and thus might be requested). If the information collected wasn’t relevant to the case at hand, it often was simply discarded.

For instance, the FBI knew that convicted terrorist Abdul Hakim Murad had been involved in an extremist Islamic plot to blow up 12 U.S.-owned airliners over the Pacific Ocean and crash an aircraft in to CIA Headquarters.<sup>22</sup> Murad was not charged with a crime in connection with the CIA crash plot, apparently because that plot was merely at the “discussion” stage when he was apprehended. Because the CIA crash plot did not appear in the indictment, however, the FBI effectively forgot all about it, and Murad’s case file essentially ignored it. FBI agents interviewed by the joint congressional investigation confirmed that Murad’s only significance to them was in connection specifically with the crimes for which he was charged: “the other aspects of the plot were not part of the criminal case and therefore not considered relevant.”<sup>23</sup>

Convinced that the only information that really matters was information directly related to the criminal investigation at hand, the FBI thus ignored this early warning sign that terrorists had begun planning to

crash aircraft into symbols of U.S. power. Thus, rather than being stored in a form that would have permitted information to be assessed and re-assessed in light of a much broader set of information about terrorist plans and intentions over time, the Murad data-point was simply forgotten. Like all the other tidbits of information that might have alerted a sophisticated analyst to terrorists' interest in using airplanes to attack building targets in the United States, the episode disappeared into the depths of an old case file and slipped out of the FBI's usable institutional memory.

## **RESTRIKING THE BALANCE**

The nation is just beginning the process of striking anew the balance between liberty and security. As one observer put it: The war on terrorism put "two vital, deeply grounded principles of American government on a collision course."

On the one hand, the president has an unquestioned responsibility to protect the nation against foreign attack and to prevent hostile foreign powers from conducting covert intelligence activity within our borders. On the other hand, law enforcement power, always potentially dangerous to a free society, may operate only within boundaries established by the Bill of Rights.<sup>24</sup>

The civil liberties issues of concern after September 11th range from constitutional to administrative.<sup>25</sup>

### **CONSTITUTIONAL**

American constitutional law distinguishes quite sharply between "U.S. persons" – that is, U.S. citizens and resident aliens – and others, and so most attention focused on U.S. citizens. Nonetheless, the large numbers of non-citizens affected, especially in the immediate aftermath of the war in Afghanistan, raised concerns those rose to "constitutional".

### ***Detaining foreign nationals in the United States.***

In the immediate aftermath of the attack, some 1200 foreign nationals living in the United States were arrested and detained in considerable secrecy. Some 460 were still in detention in January 2002, their identities and locations undisclosed. Only 93 who were charged with a crime were ever identified. The Justice Department's own internal report, released in June 2003, was critical of the process: bureaucratic inertia left a number of innocent people languishing in jails for months while systematic understaffing left them with little chance to prove their innocence. Often no distinction was made between serious suspects and immigrants who had no connection to suspect groups.<sup>26</sup>

### ***Detaining foreign nationals in Guantanamo.***

At the beginning of 2004, some 650 foreigners who had been captured in Afghanistan were still being held at the U.S. prison camp in Guantanamo Bay, Cuba. The U.S. government labeled them "enemy combatants," not prisoners of war, though it also argued that the prisoners' condition was fully compatible with the Geneva Convention covering prisoners of war. The government also argued that the prisoners could be tried by military tribunals. While the detaining of foreigners in the United States declined in visibility as they were released, deported or charged, the Guantanamo prisoners are a continuing embarrassment at least, and a foreign policy nightmare at worst. Once captured, they turn out to be hard to release. In 2004 the United States released seven to Russia, to serve in continued detention there, and it was discussing with Pakistan the release of some 60 Pakistanis. In late 2003, the U.S. Supreme Court agreed to hear an appeal from foreigners held at Guantanamo.

### ***Detaining and confining American citizens without judicial review, and restricting access to counsel.***

This small sub-set of the detentions is of particular concern because of citizenship. One, Yasser Esam Hamdi, had left the United States with his Saudi parents when he was less than a year old and so may have lost his American citizenship, but the citizenship of the other, Abdullah al Muhajir (born José Padilla) was undisputed. When Padilla was transferred to military detention, one of the justifications for doing so was to prevent him from communicating with his lawyer

lest he advance terrorist activity. An October 31, 2001 order by the attorney general established that restriction more widely. In late 2003, a federal court ordered the government to charge or release Padilla, setting off a government appeal to the Supreme Court, expected to be decided in 2004.<sup>27</sup> A related appeal for Hamdi, who was captured in Afghanistan, was also proceeding through the courts.

#### ***Retaining names of U.S. persons in databases and watchlists.***

As the government tries to do better by way of keeping tabs on potential terrorists, officials in several agencies report concern that, under the pressure of acting, they are collecting names of U.S. persons willy-nilly. So far the government has provided little guidance to those agencies in dealing with them— a concern echoed by a Markle Foundation task force.<sup>28</sup> If a U.S. person has been implicated as a suspected terrorist in an FBI investigation, he or she can be included in, say, a database. But what if the FBI investigation is only preliminary? Should there be restrictions on how widely the U.S. person's inclusion is shared? These issues, and many others, remain to be settled.

#### ***Enhancing surveillance by expanding FISA.***

Modern presidents had claimed, but the courts had called into question, warrantless searches for national security, as opposed to law enforcement, purposes. The Foreign Intelligence Surveillance Act (FISA) was a compromise, establishing a special secret court to review applications for national security search and wiretaps, of both citizens and non-citizens. The USA Patriot Act, passed in the immediate aftermath of September 11th, widened the scope for FISA warrants.<sup>29</sup>

FISA and its court, the FISC, are the prominent tools the FBI and other federal agents have for pursuing the war against terrorism *in the absence of probable cause that a crime has been committed*. They or something like them probably are necessary because by the time terrorists commit a crime, it is too late. Ideally, the United States would prevent all terrorist acts, and there never would be a crime to prosecute. By contrast, drug traffickers commit a stream of crimes.

In any case, the handling of the Moussaoui case spurred action to loosen FISA, which the Patriot Act put into effect. Some of the Act's provisions simply corrected oversights in statutory language or update the law to match new technology. For instance, FISA wiretaps were designed for an era of analog telephones, and the Act authorized the use of "roving" or "multi-point" wiretaps, which allow monitoring of all devices a suspect might use – and practice of long standing in criminal investigations.

Other parts of the Act were more controversial. FISA taps always were permitted to be longer than law enforcement counterparts – 90 days rather than 30, with extensions easier to obtain. The Patriot Act extended them further, to 120 days, and it doubled, from 45 to 90 days, the period in which foreign agents, including U.S. citizens, can be subject to clandestine physical searches.

Perhaps of greater concern, the Act made an apparently small change that is feared will have large consequences. Before September 11, obtaining foreign intelligence information had to be "*the purpose*" of FISA surveillance.<sup>30</sup> If evidence of crime was uncovered in the course of the tap, that evidence was admissible in court, but the foreign intelligence purpose was paramount. The Patriot Act loosened the requirement to "a *significant purpose*."<sup>31</sup> Because FISA taps do not require probable cause of a crime, and are longer, more flexible and less controlled by judges than are law enforcement taps, there is concern that FISA taps will be used to troll for law enforcement purpose.

#### **LEGISLATIVE**

Because surveillance has the potential to touch the lives of so many Americans, it is the core concern, even if those concerns do not always reach the constitutional.

#### ***Monitoring the source and destination of e-mail and Internet traffic.***

These so-called pen, and trap and trace techniques, were previously limited to telephones but were extended by the Patriot Act. They do

not record content but can be put in place by a court order short of a showing relevance to an investigation. They are not considered searches under the Fourth Amendment, the Supreme Court having ruled that people have no expectation of privacy about their phone numbers, which are used by phone companies for billing.

However, intercepted email also contains a subject line, thus blurring the line between “communications attributes” and content. Content is protected and requires a warrant. The concern is all the greater because the technology for emails – unlike phone calls – also has the ability to intercept the entire message.

### ***Expanding clandestine searches.***

The Patriot Act also extended the scope of these “sneak and peak” searches, which have little to do with terrorism since FISA confers much broader powers.

### ***Enlarging access to financial, education and other records.***

Before September 11, the FBI was permitted, for national security purposes, access to bank accounts without the holders’ knowledge and without a court order. The Patriot Act expanded that access beyond banks and loosened the criterion to any foreign intelligence or counterterrorism purpose.<sup>32</sup> Before September 11, the letter of request had to certify that the information was for foreign intelligence purposes and that there were facts showing that the targeted customer was a foreign agent. Under the Patriot Act, it is sufficient that the request has a foreign intelligence or counterterrorism purposes.<sup>33</sup> A parallel change opened access to telephone records on the same bases.<sup>34</sup> And yet another change opened up access to educational records on roughly the same basis.<sup>35</sup>

### **ADMINISTRATIVE**

Some of the issues of concern reflected neither constitutional nor legislative provisions, but rather administrative guidelines. In particular, Attorney General John Ashcroft relaxed guidelines issued by his predecessors, especially Edward Levy in 1976 and Benjamin Civiletti in 1980.

### ***Allowing more discretion to officers in the field.***

Here, Moussaoui is the celebrated case and argument for more discretion to the field. On the other hand, critics see the shadows of COINTELPRO in the prospect of giving more discretion to field officers who already have a great deal. On May 30, 2002, the attorney general relaxed the prevailing guidelines to permit FBI agents to search the Net, mine open data and attend public meetings, including those of political and religious groups.<sup>36</sup>

The expansion of FISA also led to tensions between the FBI and the FISC over who can approve the sharing of FISA data with FBI law enforcement agents. However, in November 2002 a federal court ruling upheld more sharing of intelligence across the intelligence-law enforcement divide within the Bureau, and in October 2003, new guidelines went to the Field Offices confirming the change.<sup>37</sup> Before the Patriot Act, the Bureau would have had to open separate wiretaps – a criminal one based on a court order and a FISA one for intelligence purposes – and would have been sharply constrained in sharing information between the two. Under the new guidelines, it could open, for example, a single FISA surveillance looking both at whether a suspect was part of a terrorist organization, an intelligence purpose, and whether he planned to buy explosives, a law enforcement one. Agents working on the two aspects of the case could cooperate closely.

### ***“Connecting the dots” about individuals.***

Here, the *câuse celebre* was the Pentagon’s program for Total Information Awareness. It was a public relations nightmare, seen by much of the public as “Big Brother” while still in its infancy. Its director, John Poindexter, was a lightning rod for critics, for he was convicted (later overturned) for lying to Congress during the Iran-Contra affair of the 1980s. A research project, not an operation, it builds on previous artificial intelligence and data mining research sponsored by the Defense Advanced Research Projects Agency.<sup>38</sup> It would use modern computer power to scan public and private databases against templates of terrorist attack scenarios.<sup>39</sup> More fundamentally, need technology and process raises fundamental questions about what constitutes a “search” if that process can assemble a detailed mosaic of information – about a person, for instance – that is

in principle available publicly.

Yet if the concerns are visible, so, too, the need for domestic information is plain. The September 11 terrorists not only trained in Afghanistan, they also used European cities like Hamburg and Brixton as “staging” areas where they could live, train and recruit in a protective environment. Similarly, they mixed easily in some areas of the United States, “hiding in plain sight” in south Florida and southern California, and perhaps also in Lackawanna. The need for information extends beyond simply following individuals, it also requires knowledge of what is being said on the streets and in the mosques of Brixton or Boston – it is doing “foreign intelligence” domestically.

In March 2003, for instance, a prominent Yemeni cleric was apprehended in Germany on charges of financing terrorism used a Brooklyn mosque to help funnel millions of dollars to Al Qaeda and boasted that he had personally delivered \$20 million to Osama bin Laden, according to federal officials. The cleric, Sheik Muhammad Ali Hassan al-Mouyad, told an FBI informant that he was a spiritual adviser to bin Laden and had worked for years to provide money and weapons for a terrorist “jihad.”<sup>40</sup> Sheik Mouyad boasted that *jihad* was his field and said he received money for *jihad* from collections at the Al Farooq mosque in Brooklyn.” As New York Police Commissioner Raymond W. Kelly put it, Al Qaeda operatives “did their fund-raising right here in our own backyard in Brooklyn.”

The collision of values runs through the war on terrorism. For instance, stories abound of people continually harassed when they try to fly because they are on one of the watch lists.<sup>41</sup> At the same time, Congress’s General Accounting Office criticized the various agencies for not sharing their watch lists. Nine federal agencies maintain lists to spot terrorist suspects trying to get a visa, board a plane, cross a border or engage in similar activities – the FBI, the Immigration and Naturalization Service, the Department of Homeland Security, the Pentagon, the State Department and other agencies.

All keep such lists and share information from them with other federal officials as well as local and state police officials as needed. But

the Congressional study found that some agencies did not even have policies for sharing watch list information with other agencies, and that those that did often required complex, labor-intensive methods to cull information. Agencies often have different types of databases and software that make sharing information next to impossible. As a result, sharing of information is often fractured, “inconsistent and limited,” the study reported.<sup>42</sup>

## LEARNING THE RIGHT LESSONS

In this case, both efficiency *and* citizens’ rights might be served by more effective and more connected systems. The Terrorist Threat Information Center (TTIC), created in 2002, is meant to consolidate more than a dozen previous lists, including the State Department’s TIPOFF database of more than 110,000 known and suspected terrorists. The first lesson, then, is to assess any proposed measure for indications that it might be pain for no gain. That is, will it cause citizens inconvenience if not damage to their privacy for scant or no gain in the war on terrorism?

Most of the financial reporting requirements expanded under the Patriot Act fall into that category. Before September 11, financial institutions had been required to submit a Currency Transaction Report (CTR) for any cash transaction over \$10,000 and a Suspicious Activity Report (SAR) when the “had reason to suspect” that a transaction was “not the sort in which the particular consumer would be expected to engage.”<sup>43</sup> Already before September 11 there were concerns over the sheer volume of such reports. However, the Patriot Act has increased that flow by expanding the requirements – from financial institutions to securities brokers and dealers in the case of SARS, and from financial institutions to any business or trade in the case of CTRS.

Those financial reporting requirements may have value for other threats, like drug trafficking. But they are pain for no gain in the war on terrorism because, alas, terrorism isn’t expensive. Estimates for the total cost of the September 11 attacks are in the thousands of dol-

lars, not millions.

So, too, if we are honest, many of the airport safety measures are in the pain-for-little-gain category. In any case, it isn't obvious that airport security is worth the upwards of \$6 billion or so the nation is now spending on it.<sup>44</sup> Indeed, one of the real failures is that while the strategic warning that existed well before September 11 pointed to one fairly cheap fix – reinforced airplane cockpit doors – even that was judged too expensive before September 11. To be sure, the real purpose of many of airport security measures is public confidence as much as real security, but, in the end, measures that don't add much to security will not build confidence either.

Second, part of the reason for the striking cleavage in the public debate is the absence of any *compared to what? And for what gain?* It is imperative to begin to develop a systematic framework for assessing the value of particular intelligence-gathering measures, the civil liberties involved in them, and costs that arise from the measures. That hard-headed assessment is all the more necessary the sharper is the clash of values; the assessment will not settle the argument over values but can at least put it in a clearer focus.

Take the issue of profiling, for instance. On the one hand, it is offensive to our values. On the other, it seems common sense. So far – thought surely not forever – the terrorists of most threat to the nation have come from or had roots in one part of the world. Not to give special concern to people, so far men, who fit that description seems plain silly. Worse than silly, it seems to impose gratuitous costs on all those light-skinned grandmothers who are searched as potential terrorists. There is a considerable cost, including in privacy if not liberty, to *not* profiling.

The first need is to be more open about costs and benefits. The civil liberties costs are usually argued in terms of individual cases, and those are provocative. But any system will make mistakes, and while it is a shame that those will fall disproportionately on one set of people, that shame does not eliminate the need to assess the over-all costs carefully. The same is true of benefits. As with watch lists, more sophisticated profiling can be better than less. Searching every dark-

skinned young male airline traveler is both offensive and wasteful. Making watch lists more discriminating by noting those who bought one-way tickets, or paid in cash or other relevant indicators can reduce the numbers who are singled out.

To be sure, collecting the information to make still more discriminating watch lists – for instance, by identifying people who had been associated with one another before but had made entirely separate arrangements to travel on the same flight – can itself invoke privacy concerns. Yet if the information is public in any case – as is true of most business and other associations – the value of permitting watch lists to assemble it probably outweighs the cost.

A third lesson is the possible value of a separate domestic intelligence agency, separately overseen. As U.S. Senator Bob Graham (D-FL) recently observed: “I think [it is time] to look seriously at an alternative [to the FBI approach], which is to do as...many other nations have done, and that is to put their domestic intelligence in a non-law enforcement agency.”<sup>45</sup> Indeed, the joint congressional investigation into the September 11 attacks recommended that the administration “consider promptly . . . whether the FBI should continue to perform the domestic intelligence functions of the United States Government or whether legislation is necessary to remedy this problem, including the possibility of creating a new agency to perform those functions.”<sup>46</sup>

The arguments for a separate domestic intelligence agency are two. The first is that the FBI is likely to remain – and perhaps should remain – primarily a case-based law enforcement organization. It is good at that. Yet pursuing cases the way the FBI does simply is contrary to building a comprehensive intelligence picture. If the FBI identified a suspected terrorist in connection with a Hamas investigation, for example, the suspect would be labeled a Hamas terrorist with relevant information kept in a separate “Hamas” file that would be easily accessible to and routinely used only by “Hamas”-focused FBI investigators and analysts. The Usama bin Laden unit would be unlikely to know about the FBI's interest in that individual. In the case of Moussaoui, when agents from the local field office began, in August 2001, looking into his flying lessons at a Norman, Oklahoma school, they did so in ignorance that the same field office had been

interested in the same flight school two years earlier because a man thought to be bin Laden's pilot had trained there.

Second, while domestic intelligence services in other countries have been willfully misused for political purposes – Italy and Peru are two cases in point – the lesson of COINTELPRO is that dangers to democracy can arise from mixing domestic intelligence with law enforcement. For similar reasons, Canada took its Royal Canadian Mounted Police (RCMP) out of the domestic intelligence business, replacing it with a separate service, the Canadian Security Intelligence Service (CSIS). Other states have been successful in creating domestic intelligence bodies that have operated effectively within the constraints of liberal democracy, including the United Kingdom (Security Service, MI5), France (*Direction de la Surveillance du Territoire*, DST), Germany (*Bundesamt für Verfassungsschutz*, BfV), and Australia (Australian Security Intelligence Organization, ASIO).

In all of these democracies, the intelligence function remains subject to legislative oversight and supervision yet retains the latitude to aid government crisis decision-making through covert and, often, unorthodox means. They, along with the COINTELPRO history, suggest that domestic intelligence might be both better and safer for democracy if it is separate, not the tail of a law enforcement dog. The United States is probably not ready yet to create such a service, but it is time to begin discussing it. The new Department of Homeland Security (DHS) would be the logical place for such a homeland security intelligence service. The experiences of other countries also can provide useful ideas about how relationships among federal, state, and local law enforcement agencies can be strengthened. In Canada, for example, CSIS has established a network of regional liaison officers, who help facilitate the flow of information between local and provincial police agencies and the federal authorities.

Yet the downsides of a new agency are also apparent. Purely practically, it would have all the teething pains of any new agency – pains on vivid view at DHS – and would, to boot, need to duplicate the range of offices and infrastructure that the FBI now has. Moreover, a new agency is hardly a panacea; in the United Kingdom, MI-5 and Scotland Yard were for years locked in a turf battle over who had pri-

mary responsibility for counterterrorism in the United Kingdom outside Northern Ireland. Indeed, the United Kingdom is planning to consolidate its fragmented anti-crime efforts into a “British FBI.”<sup>47</sup> Finally, the idea of a domestic intelligence service completely unhitched from cases, and perhaps from investigation as well, does raise civil liberties concerns. A more modest version would underscore the transition the FBI is already trying to make, by creating distinct career tracks for counterterrorism and intelligence within the Bureau – a kind of MI-5 within the FBI.

The fourth lesson is that some caution, and some slowness, is no bad thing as the nation rethinks the “oppositions” on which Cold War institutions and processes were based. The values at stake are powerful. And we have yet to calibrate the terrorist threat. Indeed, we still do not understand what happened to the nation on September 11. We are learning, but there are still large unknowns about the terrorists’ logistics, their own intelligence and so on. We sense, but do not yet know, that terrorism against the homeland will be, for the United States, serious but not in a class with the threat faced by Israel. Thus, we suspect but do not yet know that the nation will not be forced to shift the balance as far toward security as Israel has had to do.<sup>48</sup>

Because of the controversy surrounding them, many (but not all) provisions of the USA Patriot Act are “sunset” powers that will expire in 2005 if not specifically re-authorized. That seems wise, given that the terrorist threat is yet to be calibrated and serious assessment of the costs and benefits of particular measures is yet to be done. It seems all the wiser given that, with the benefit of some hindsight, some of the Act’s provisions seem only tangentially connected to the war on terrorism.

Moreover, building domestic intelligence is a formidable task. In the first place, while local authorities collect a lot of information, they, like the FBI, mostly do so in response to crimes, not threats. That information then becomes part of cases, and may then disappear into grand juries. (It is rumored that the information about the domestic Al Qaeda cells did not come from law enforcement at all but rather from CIA officials assigned to FBI Joint Terrorism Task Forces.) Only the several largest police departments, New York and Los

Angeles, have intelligence components. For the rest, intelligence means tips to catching criminals, not assembling patterns of threat. None of the other departments has capacity for intelligence *analysis*.

At the federal level, much is in motion but not much is settled. For instance, FBI director Robert Mueller is determined to turn the mission of the Bureau from law enforcement to prevention and intelligence, but doing so runs against the powerful grain of organizational culture that has run through this paper. The new DHS was to have an intelligence unit, but that has been very slow to emerge.<sup>49</sup> TTIC was created as the place to “put the dots together.” It reports to the Director of Central Intelligence, so, quite apart from its composition, its domestic reach will be limited, including by law. TTIC prepares the President’s Terrorism Threat Report (PTTR), a highly classified assessment of developments bearing on the threat of terrorism, sent to the President six times a week.

Perhaps the slowly turning wheels of bureaucracy can provide time for reflection on the threats and values at stake. The “oppositions” are not to be discarded lightly. We do not yet have consensus on where to strike the balance between security and liberty. And so we are at the beginning of a decade of rethinking and reshaping as we calibrate the terrorist threat against the homeland. As with fighting the Cold War, we probably will come to settled new arrangements for fighting terrorism – just as the threat has moved to something else!

## ENDNOTES

<sup>1</sup> This article updates and extends my “Terrorism, Intelligence and Law Enforcement: Learning the Right Lessons,” in the special issue on *Terrorism, Intelligence and National Security*, 18, 4 (Winter 2003), 121-40.

<sup>2</sup> In the spirit of full disclosure, I was a staff member of the Senate Select Committee, chaired by Sen. Frank Church (D, ID), my first job in government, a fascinating introduction and the beginning of my abiding interest in intelligence.

<sup>3</sup> See *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities of the United States Senate*, 94th Congress, 2nd Session, 1976, Book II, *Intelligence Activities and the Rights of Americans*, and Book III, *Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans*. For links to these reports, as well as to a rich range of other documents, both historical and contemporary, see [www.icdc.com/~paulwolf/cointelpro/cointel.htm](http://www.icdc.com/~paulwolf/cointelpro/cointel.htm).

<sup>4</sup> John le Carré, *The Night Manager* ( New York: Knopf, 1993 ), p.42.

<sup>5</sup> See my *Reshaping National Intelligence for an Age of Information*, (Cambridge: Cambridge University Press, 2001), p. 139ff.

<sup>6</sup> The findings of the joint House-Senate investigation of September 11 outlines the basic story. It is *Final Report*, Part I, The Joint Inquiry, The Context, Part I, Findings and Conclusions, December 10, 2002. A fuller account is contained in Senator Richard Shelby’s long supplementary document, *September 11 and the Imperative of Reform in the Intelligence Community*, Additional Views, December 10, 2002. Both are available at [www.fas.org/irp/congress/2002\\_rpt/index.html](http://www.fas.org/irp/congress/2002_rpt/index.html). See, in particular, Shelby’s report, p. 15ff., from which this account is drawn, unless otherwise indicated.

<sup>7</sup> See Walter Pincus and Don Eggen, “CIA Gave FBI Warning on Hijacker,” *Washington Post*, June 4, 2002, p. A1.

<sup>8</sup> *Ibid*.

<sup>9</sup> Bob Drogin, Eric Lichtblau, and Greg Krikorian, “CIA, FBI Disagree on Urgency of Warning,” *Los Angeles Times*, October 18, 2001.

<sup>10</sup> *Ibid*.

<sup>11</sup> Joe Klein, “Closework: Why We Couldn’t See What Was Right in Front of Us” *The New Yorker*, October 1, 2001, pp. 44-49.

<sup>12</sup> <<http://specials.ft.com/attackonterrorism/index.html>>

<sup>13</sup> This discussion and this paper are enriched by a RAND project I led for the Security Division of the FBI. The final report of that project, *Reinforcing Security at the FBI*, DRR-2930-FBI, (Santa Monica: RAND, January 2003) has been briefed to the FBI and to Congress but is not yet publicly released.

<sup>14</sup> Quoted in Shelby, Additional Views, cited above, p. 30.

<sup>15</sup> This episode is also discussed in the joint congressional investigation *Final Report*, and in Shelby's Additional Views, p. 18, both cited above.

<sup>16</sup> See <http://fly.hiwaay.net/~pspoole/fiscshort.html>. See also Ronald Kessler, *The Bureau: The Secret History of the FBI*, (New York: St. Martin's Press, 2002), pp. 438-43.

<sup>17</sup> The attorney general's letter-report is posted at [www.fas.org/irp/agency/doj/fisa/2002rept.html](http://www.fas.org/irp/agency/doj/fisa/2002rept.html).

<sup>18</sup> This account derives from *Interim Report on FBI Oversight in the 107th Congress by the Senate Judiciary Committee: FISA Implementation Failures*, (February 2003), p.14ff, posted at [www.fas.org/irp/congress/2003\\_rpt/fisa.html](http://www.fas.org/irp/congress/2003_rpt/fisa.html).

<sup>19</sup> 50 U.S.C. Section 1805 and Section 1824, and 50 U.S.C. App. Section 1801 (b).

<sup>20</sup> A sanitized version of the letter was released to the Senate Judiciary Committee by the Justice Department on June 6, 2002. The quote is from pp. 7-8, fn.7.

<sup>21</sup> See his Additional Views, cited above, p. 36.

<sup>22</sup> Ibid., p. 37.

<sup>23</sup> Shelby, Additional Views, cited above, p. 37.

<sup>24</sup> See Stephen J. Schulhofer, *The Enemy Within: Intelligence Gathering, Law Enforcement and Civil Liberties in the Wake of September 11*, (New York: The Century Foundation, 2002), p. 46.

<sup>25</sup> Ibid. provides a very good, readable discussion of many of these categories.

<sup>26</sup> Department of Justice Inspector General, "The September 11 Detainees: A Review of the Treatment of Aliens Held on Immigration Charges in Connection with the Investigation of the September 11 Attacks, April 2003, available at [www.usdoc.gov/oig/special/0603/full.pdf](http://www.usdoc.gov/oig/special/0603/full.pdf).

<sup>27</sup> See Charles Lane, "Showdown on Terrorism Case: Administration Seeks Fast Track for High Court Appeal," *Washington Post*, January 8, 2004; Page A02, available at [www.washingtonpost.com/wp-dyn/articles/A63262-2004Jan7.html](http://www.washingtonpost.com/wp-dyn/articles/A63262-2004Jan7.html).

<sup>28</sup> See *Creating a Trusted Network for Homeland Security, Second Report of the Markle Foundation Task Force*, December 2003, available at <http://www.markletaskforce.org>, (last visited December 5, 2003).

<sup>29</sup> *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* ( hereafter referred to as Patriot Act ) , Pub. L. No. 107-56, 115 Stat. 272 (2001).

<sup>30</sup> 50 U.S.C., section 1804 (a) (7) (b), emphasis added.

<sup>31</sup> Ibid., as amended by Patriot Act, section 218, emphasis added.

<sup>32</sup> See, Dan Eggen and Robert O'Harrow Jr., "U.S. Steps Up Secret Surveillance," *Washington Post*, March 23, 2003, at [www.washingtonpost.com/wp-dyn/articles/A16287-2003Mar23.html](http://www.washingtonpost.com/wp-dyn/articles/A16287-2003Mar23.html).

<sup>33</sup> 12 U.S.C., section 3414(a)(1)(C); 3414(a)(5)(A) (2001)

<sup>34</sup> 18 U.S.C., section 2709 (b) (2001), as amended by Patriot Act, section 505 (a) (2001).

<sup>35</sup> 20 U.S.C., section 11232g (j) (1)&(2) (2001) ), as amended by Patriot Act, section 507 (2001).

<sup>36</sup> Officially, the "Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations" (May 30, 2002). A sanitized version of the partly-classified "Attorney General's Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations" is available at [www.usdoj.gov/ag/readin-groom/terrorismintel12.pdf](http://www.usdoj.gov/ag/readin-groom/terrorismintel12.pdf)

<sup>37</sup> For background, see "FBI Pairs Criminal and Intelligence Cases," *CNN.com*, December 13, 2003, available at <http://www.cnn.com/2003/LAW/12/13/fbi.terrorism.ap/index.html>, (last visited December 23, 2003).

<sup>38</sup> See Shane Harris, "Total Information Awareness Official Responds to Criticism," *Government Executive*, Daily Briefing, January 31, 2003, <http://goveexec.com/daily/fed/0103/013103h.1.htm>

<sup>39</sup> For a summary of the privacy issues involved by TIA, see Gina Marie Stevens, *Privacy: Total Information Awareness Programs and Related Information Access, Collection and Protection Laws*, (Washington: Congressional Research Service, March 21, 2003).

<sup>40</sup> Eric Lichtblau and William Glaberson, "Millions Raised for Qaeda in Brooklyn, U.S. Says", *New York Times*, March 5, 2003, [www.nytimes.com/2003/03/05/international/europe/05TERR.html?ex=1047](http://www.nytimes.com/2003/03/05/international/europe/05TERR.html?ex=1047)

<sup>41</sup> See for example, "The System That Doesn't Safeguard Travel," *Business Week Online*, at <http://uk.biz.yahoo.com/030417/244/dxz9z.html>.

<sup>42</sup> General Accounting Office, Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing, GAO-03-322, (Washington: April 15, 2003). <http://www.nytimes.com/2003/04/30/international/worldspecial/30TERR.html>

<sup>43</sup> *Annunzio-Wylie Act of 1992*, P.L. 91-508, 32 U.S.C., section 531 (g); 31C.F.R, section 103.18(a)(2) and 108.19(a) (2) (ii).

<sup>44</sup> Of the Transportation Security Administration's \$7.1 billion budget for 2003, \$6.1 billion went for aviation security. See E. Marla Felcher, "Aviation Security," in *The Department of Homeland Security's First Year: A Report Card*, (New York: The Century Foundation, 2004).

<sup>45</sup> As quoted in Thomas Frank, "Push Is on to Overhaul FBI," *Newsday*, December 29, 2002.

<sup>46</sup> See the *Final Report*, cited above, Recommendations.

<sup>47</sup> Mark Rice-Oxley, "Plans to Fight Organized Crime with a 'British FBI,'" *Christian Scientist Monitor*, February 12, 2004, available at [www.csmonitor.com/2004/0212/p05s01-woeu.html](http://www.csmonitor.com/2004/0212/p05s01-woeu.html), (last visited March 8, 2004).

<sup>48</sup> Extrapolating from the Israeli experience in the first years of this century, an "Israel-sized" terrorist threat to the United States would imply about 10,000 deaths and 100,000 casualties per year.

<sup>49</sup> For an argument for such a capability, along with the formidable obstacles to creating it, see my "Intelligence, Law Enforcement and Homeland Security," Twentieth Century Fund, August 2002, at [www.homelandsec.org](http://www.homelandsec.org). For my more recent assessment, see my "Intelligence," in *The Department of Homeland Security's First Year: A Report Card*, cited above.