

B425. "Better Safe Than Sorry" The Weekly Standard (July 21, 2003, p.9).

The Bush administration is incessantly criticized, and not only from the left, for a variety of safety measures it introduced in the wake of the 2001 terrorist attacks. Senator Patrick Leahy, for example, said in November 2001, "We don't protect ourselves by bending or even shredding our Constitution." And a New York Times editorial the same month claimed that the president "is eroding the very values and principles he seeks to protect, including the rule of law." Almost daily, someone bemoans the "death of privacy" or the rise of the "surveillance society."

The administration has chosen not to respond to most of these allegations, and when it has responded, it has tended to be tone deaf. And whatever one thinks about mining private data banks to identify suspicious patterns of activity, calling a program designed to do this Total Information Awareness (TIA) only played into the critics' hands.

A careful examination of the new homeland-protection policies finds that they are not all cut from one constitutional, legal, or ethical cloth. Many were overdue when they were finally enacted in the wake of 9/11; several others are also quite reasonable; a few raise troubling questions; and at least one useful innovation the administration has yet to adopt.

Before any Cook's tour of the major new measures can begin, a few general points are in order. The key question is often framed as: How far should we be willing to sacrifice our individual rights in order to enhance our safety? But it's a mistake to think of homeland security as a zero sum game, where 100 percent of the turf belongs to rights, and every new safety measure amounts to an intrusion to be justified. To realize how prejudicial this approach is, ask the opposite, equally loaded, question: How far should we be willing to sacrifice our security in order to enhance our rights?

At the heart of the matter is the observation that under the Constitution, no right is absolute. Indeed, protecting the public interest--especially the public safety--is as legitimate as protecting individual rights. Thus, the Fourth Amendment states, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated...." That is, the Fourth Amendment recognizes that some searches are reasonable--those deemed to serve a compelling public interest. They do not violate anyone's rights, because the Constitution never gave anyone an absolute right not to be searched.

There is a considerable legal literature about what is "reasonable," with many differences of opinion. By and large, it comes down to an admittedly vague notion: what a reasonable person would consider reasonable. One thing, however, is not in doubt: Much of what was unreasonable before 9/11 ceased to be so that morning.

MEASURES THAT WERE OVERDUE

Many of the new safety measures simply bring the law into line with technological developments. These should have been introduced years ago. The most important of these changes involve the Foreign Intelligence Surveillance Act (FISA), enacted in the faraway days of 1978. FISA provides guidelines under which a federal agent can obtain authorization to conduct surveillance for "foreign intelligence purposes." These purposes include protecting Americans from acts of foreign powers, occurring within the United States, or their agents (such as terrorists), whether foreign or American. A major tool of surveillance is the wiretap.

Historically, a wiretap was authorized for a given phone, usually the phone in the suspect's home or office. In recent decades, people have acquired multiple phones, cell phones, and e-mail, but federal officials conducting surveillance under FISA could not follow a suspect as he moved from one instrument to another--not without a separate court order for each communication device. The USA Patriot Act, enacted in October 2001, amended FISA to allow "roving surveillance authority," making it legal for agents to follow the suspect whatever instrument he uses.

Unless you believe that terrorists are entitled to benefit from new technologies but law enforcement must not catch up, this measure is entirely reasonable. Moreover, the critics' claim that surveillance orders are promiscuously granted simply doesn't stand up. Nearly 40 million foreigners visit the United States each year, according to the Commerce Department, yet the FISA court issued little more than 1,000 surveillance orders in 2002--after 9/11--Attorney General Ashcroft reported to the Senate Judiciary Committee in March 2003.

Believe it or not, before 9/11 the regulations that allowed public authorities to record or trace e-mail were interpreted by Department of Justice lawyers as requiring a court order from every jurisdiction through which an e-mail message traveled. This was a holdover from the days when phone lines were local; warrants for phone taps were granted by local authorities and had only a local reach. But today, e-mail messages zoom around by a variety of routes. Now, thanks to the Patriot Act, nationwide tracing and recording orders are permitted under FISA. That is, law enforcement authorities may finally catch up with the technological features of e-mail. Anybody who sees a civil rights violation here should have his vision checked.

Few changes in the laws and regulations after 9/11 have raised more ire than new Department of Justice guidelines permitting the FBI to conduct surveillance of political and religious organizations. The new guidelines, introduced in May 2002, state, "For the purpose of detecting or preventing terrorist activities, the FBI is authorized to visit any place and attend any event that is open to the public, on the same terms and conditions as members of the public generally." Civil libertarians are still fixated on the fact that more than a generation ago the FBI infiltrated some fringe groups (such as the Ku Klux Klan and the Black Panthers) and tapped the phones of civil rights leaders like Martin Luther King Jr. But that was a different FBI, one run by J. Edgar Hoover, accountable to no one, feared by presidents and legislators because of files Hoover kept on their personal lives and because he succeeded in building a public cult around himself. The reforms of the mid-1970s barred FBI agents from so much as attending a public event or entering a public space to observe the goings-on there unless they were investigating a specific crime.

The absurd result was that agents charged with protecting a community were unable to inform themselves firsthand about inflammatory elements in its midst. In particular, terrorists could meet and recruit in places of worship without any fear of being overheard by public authorities. As it turned out, the danger was far from theoretical. A score of people were recruited at mosques in Britain to fight with the Taliban, and some of the 9/11 hijackers were recruited at a mosque in Hamburg, according to German security sources. Since 9/11 several American mosques have been investigated for links to terrorism, including two in the Seattle area and one near St. Louis.

Before 9/11 a Chinese wall separated intelligence agencies, such as the CIA and National Security Agency, from law enforcement, above all the FBI. As Attorney General Ashcroft put it in his July 2002 testimony before the Senate, "A criminal investigator examining a terrorist attack could not coordinate with an intelligence officer investigating the same suspected terrorists." The barriers between agencies, Ashcroft said, prevented cooperation and

coordination. Michael Hayden, the director of the NSA, told a recent meeting of the Council on Foreign Relations in Washington that his staff were repeatedly drilled in not sharing "raw information" (which included names and addresses and other identifying marks) with anybody.

Since 9/11 the walls dividing the intelligence collection and law enforcement agencies have been largely removed. A major factor was a 2002 ruling by the FISA court that permitted information-sharing between intelligence agents and criminal investigators under FISA. And a new culture is being fostered, one that puts a premium on the very collaboration that once was avoided. Turf battles have not disappeared, but there is a growing appreciation that the enemy is not the other agency, but bin Laden and his followers. Attorney General Ashcroft is rhapsodic about the new culture, describing it as "capable of adaptation, secured by accountability, nurtured by cooperation, built on coordination, and rooted in our Constitutional liberties." Even without such Hollywood music in the background, it is good to know that now, as a rule, the left hand is allowed to know what the right hand has found out.

MEASURES THAT ARE REASONABLE AFTER 9/11

A few measures that arguably were not needed before 9/11 are now slowly, woefully slowly, being introduced. Prominent among them is a tracking system for foreigners who come to the United States to study. Before 9/11 the United States did not check whether those who came to the country for a defined period of time, say on a student visa, left at the end of the period. Many did not leave, but there was no way of knowing who they were or what they were up to. Actually, a partial tracking system with a mouthful of a name, the Student and Exchange Visitor Information System (SEVIS), was mandated by Congress as far back as 1996, but widespread opposition from colleges and civil libertarians prevented its implementation. No funds were appropriated until the passage of the Patriot Act. The new Internet-based student tracking system requires colleges to verify whether the students they are expecting actually show up. The system is plagued with technical difficulties (when many colleges sign on, the computer system slows to a crawl), procedural delays (to participate, a college must be certified by the INS), and political opposition (several deans of students complain that they are being made to spy for the government). And colleges fear scaring off foreign students, who often pay full fare.

Given that several of the hijackers came to the United States on the pretext that their purpose was to study, and given the large number of students from the terrorists' countries of origin, the tracking system is fully justified. Once debugged, SEVIS should entail minimal bureaucratic burdens; the scrutiny, moreover, falls upon people who are not Americans and who have come here of their own free will, knowing in advance that they would be tracked. Indeed, some kind of tracking system is in place in many democracies. In several E.U. countries, for instance, aliens who relocate are required to register with the local police within 30 days. In the age of international terrorism, some tracking capability is needed so security forces can do their job.

The most important change in law enforcement since 9/11 is that the FBI has shifted its focus from prosecution to prevention. This policy shift comes from the White House. It reorients the agency from collecting information after a crime has been committed to stopping terrorist attacks before they take place. The reason the shift is portentous is that, while prosecution deals with suspects, prevention often entails stirring the pot in the belief that something in it needs to be disturbed. In such cases, a considerable number of people who are not themselves suspected of any wrongdoing may be put through some kind of wringer in order to try to upset a plot that authorities have reason to believe is being hatched.

Thus, in late 2001, on instructions from the Department of Justice, U.S. attorney's offices throughout the nation sent letters to some 5,000 men who had come from countries where al Qaeda is present or active and who had entered the United States on nonimmigrant (work, tourist, or student) visas, requesting that they present themselves to be interviewed. The purpose of the interviews was to solicit information the government might use in thwarting attacks. Also, it was assumed that there were probably some bad dudes among these men, and that interviews might help ferret them out or scare them into leaving the country. In March 2002, Attorney General Ashcroft reported that the interviews had been productive, saying they "provided us with a number of leads which we think to be very important, and helped us establish relationships with individuals in a number of communities in this country that can be helpful to us in terms of information." Hence, a similar dragnet was cast in early 2003, when, according to the Justice Department, the FBI interviewed nearly 10,000 Iraqis in the United States. These interviews, the FBI revealed, "resulted in 250 reports that provided information on possible weapons production, storage and underground facilities."

Some may wonder what the guardians of civil liberties are upset about: Why shouldn't the government interview people? The answer is that these investigations are an intrusion on thousands of people, suspected of nothing, who would rather not spend their afternoon being interrogated in an FBI office. Moreover, a Department of Justice official explained privately that anyone who declines to be interviewed or simply to show up becomes a suspect and may well be brought in for interrogation.

These are steps the United States would not take in normal times. They are a price we must pay--and not a trivial one--to minimize the likelihood of terrorist attacks in our midst.

MEASURES THAT REMAIN TROUBLING

Still other new measures raise difficult questions. Some of these policies have already been modified. Others have been abandoned. Still others, appropriate to our new security environment, should be retained but with enhanced provisions for accountability.

Military Tribunals. There is a clear need to avoid disclosing our intelligence sources and methods in open court--so much so that in several instances, an American charged with espionage has been allowed to bargain down the sentence to avoid his pleading not guilty, which would necessitate a public trial. Terrorists should not be allowed to benefit from a right to demand a public trial. Nevertheless, there did appear to be cause for concern when the White House announced in November 2001 that under some circumstances, civilians might be tried before military tribunals. The procedures to be used were left vague; the implication seemed to be that the death penalty could be imposed by a mere majority of the tribunal and that there would be no opportunity for appeal. In March 2002, however, the Pentagon clarified the matter, announcing that a unanimous verdict will be required for the death penalty, that most proceedings would be open to the press, that defendants would be eligible for military lawyers at government expense, and that suspects would be presumed innocent until proven guilty. The rules also provide for appeals through the military, specifically review by the military Court of Criminal Appeals, the Court of Appeals for Armed Forces, and the Supreme Court. These are welcome clarifications. Still, military tribunals should be used as sparingly as possible. Up to this point, their use has been avoided.

Eyes and Ears. Operation TIPS (the Terrorist Information and Prevention System) was proposed as part of Citizen Corps, the voluntary service the Bush administration introduced following the president's 2002 State of the Union address and through which Americans can help protect the homeland. TIPS, as conceived by the White House, was to serve as "a nationwide mechanism for reporting suspicious terrorist activity." Americans would report

questionable activities they encountered by calling a hotline. To many, it sounded as if people were being asked to snoop on one another, as if every mailman, meter reader, and UPS driver might be peeping into one's living room and reporting whatever he deemed odd. If such a program had been implemented, it would have fueled enormous mistrust among Americans. It also would have been truly unreasonable, generating millions of false reports that would have overloaded authorities already afraid of being blamed for missing some genuine warnings of terrorist preparations.

Fortunately, TIPS, with its overtones of invasion of privacy, was killed in a little-known provision of the Homeland Security Act. It should be noted, however, that other programs continue to invite people to report suspicious activity they observe in public places. In the spring of 2003, for instance, New York City introduced the slogan "If You See Something, Say Something" to encourage people riding the subway to keep their eyes open. And New York State maintains a hotline introduced in September 2002. Such measures should be evaluated by an independent analyst to determine whether they yield sufficient leads to justify them.

New Powers: New Accountability? In addition, the government has acquired a whole slew of other new powers since the first attack on the World Trade Center in 1993. None of these is small potatoes; together they amount to a considerable shift in the balance between security and individual rights. Public debate often focuses on whether these new powers are needed. I take it for granted that they are called for, given the new level of threat; the issue is whether their application is being adequately supervised.

One of these new powers, enacted in 1994 and extended in 1996, is the ability to charge someone with the crime of providing "material support" to terrorists. "Material support" is a broad category that includes money, training, expert advice or assistance, and false documents or identification. Making a donation to the Holy Land Foundation of Richardson, Texas (which claims to support charitable work but actually provides support to Palestinian terrorist groups), for instance, can land a person in jail--whether or not he knew the true purposes of the foundation.

Also, since 9/11, new "sneak and peek" legislation contained in the Patriot Act allows authorities, with a court order of course, to search a home in connection with a terrorism investigation without notifying the homeowner, as required by a normal search warrant. Under the Patriot Act (Section 215), business records and computer hard drives, including those of libraries, can also be searched, with a court order, in connection with a terrorism investigation. Furthermore, an American citizen can be declared an "enemy combatant," depriving him of many of his constitutional protections. This has happened in precisely two cases. President Bush declared Jose Padilla, suspected of planning a "dirty bomb" attack with al Qaeda, an enemy combatant. Yaser Hamdi, who was born in the United States, but spent most of his life in Saudi Arabia, was captured on the battlefield in Afghanistan.

Critics view these new powers as threatening our democracy. As I see it, these powers are neither dangerous nor reasonable per se, but dangerous if employed without close scrutiny, and reasonable if properly supervised.

Some oversight is built into the structure of federal agencies, including law enforcement: Supervisors are supposed to watch what their subordinates do, and Congress is meant to provide another layer of oversight. Then there are the courts. It is encouraging that those new security measures that have been reviewed by appeals courts have, by and large, been upheld. Another source of accountability is the inspector general of the Justice Department. Indeed, last month he issued a report that criticized the ways the FBI dealt with some of

those detained on immigration offenses in the months after the terrorist attack. Nevertheless, even this multilayered set of safeguards is by no means foolproof--as we were reminded by the FBI scandals in Boston, where agents protected mob informants in the 1990s and warned a mob boss that he was about to be arrested; he is still on the lam.

The good news is that some new measures of accountability have been put in place alongside the new powers. Thus, the Homeland Security Act of 2002 provides for an officer whose job it is to protect privacy and another whose job is to promote civil rights and liberties. It is too soon to tell how effective these officers will be. Either way, I believe Americans would welcome heightened scrutiny of the way these powers are exercised.

Further, accountability might take the form of review by a panel of judges similar to the FISA court. Such a panel could regularly examine the cases of Americans charged under the new powers. It could meet in closed session and release its findings to the public in summary form. For instance, it might report that, say, suspects were held appropriately in 80 percent of the cases under review; in another 15 percent of cases, more information was needed (bureaucratese for "We have doubts about some aspect of these cases"); and in the remaining 5 percent, the detainee must be released forthwith. I focus on Americans because noncitizens have fewer rights than members of our national community. Which rights noncitizens are entitled to and how those rights are to be safeguarded requires a separate examination.

PROBLEMS NOT YET ADDRESSED

Many provisions of the Patriot Act expire in 2005. Some of them the Justice Department and Congress are seeking to extend one at a time. For instance, in May, the Senate passed what is called the "Moussaoui-fix" bill, which would allow law enforcement to conduct surveillance of "lone wolf" terrorist suspects. (Currently, association with a known terrorist organization must be documented.)

Another safety measure deserves the attention of Congress: more reliable means of personal identification. The usefulness of watch lists, airline passenger profiles, student tracking systems, and dossiers on suspects is greatly impaired as long as people can readily obtain false identification (typically driver's licenses) or steal someone else's identity.

This is no small matter. Driver's licenses are a de facto national ID card. Although they are issued by states, each state honors all the others'. People are regularly required to present their license (or some other document, such as a green card) when they fly, drive, or enter numerous public buildings and quite a few private ones. Whatever loss of anonymity and privacy is involved, law-abiding Americans have already suffered it. But as long as terrorists and other criminals can readily obtain false or fraudulent driver's licenses, many new security measures are undermined. Hence, we need to make driver's licenses meet a basic standard of reliability, as the American Association of Motor Vehicle Administrators has recommended. Bipartisan bills to this effect were introduced in the 107th Congress--one by representatives James Moran and Tom Davis; the other by senators Dick Durbin and John McCain--but garnered little support. The administration should back the effort to make driver's licenses tamperproof and uniform across the 50 states.

The world had changed, and we cannot afford to pretend that any recalibration of our rights in view of our new need to defend the United States at home amounts to an attack on the Constitution. This is not to say that we should mindlessly consent to any innovation introduced in the name of safety. Societies have no precise control mechanisms; they tend to oversteer. Hence, significant corrections in the delicate balance between public safety and individual rights typically require their own corrections. After 9/11, there were good reasons

to rush through legislation expanding government authority, given the fear of imminent follow-up attacks by sleeper cells. Now is the time to revise and fine-tune these measures.

When all is said and done, most of the measures that the Bush administration has launched since 9/11 are reasonable and necessary. Others may well be necessary, but call for close supervision by Congress to ensure that the government does not yield to new temptations. Regrettably, there still are some pressing security needs, above all in our ability to reliably identify people, and in that area the government needs more, not less, authority.

Amitai Etzioni, University Professor at George Washington University, is the author of *The Limits of Privacy* and the recently published memoir, *My Brother's Keeper*.