• 30 •

Civil Liberties and Effective Investigation

Coleen M. Rowley

The balance between individuals' civil liberties and the need for effective investigation is hard to maintain even during so-called normal times, let alone times of increased terrorist threat or war. It is, admittedly, a difficult balancing act.

—Coleen M. Rowley, *New York Times*, March 6, 2003

Civil libertarians warn that privacy and liberty are at risk in America, that a combination of lightning-fast technological innovation and the erosion of privacy protections threatens to transform George Orwell's Big Brother into a very real part of American life, turning the nation into a "Surveillance Society."

At the same time, law enforcement and other government authorities tell us that they need additional powers and new technological tools to effectively investigate in order to bring criminals to justice and prevent acts of terrorism.

What is the truth? The debate has been monopolized by the people who are the most passionate on the issue—the partisans on both extremes. Many have observed and complained about the unwise, needless, and in some cases bizarre restrictions placed on law enforcement at the expense of victims and the public. But a review of old FBI files from the communist "Red Scare" era and the protests and civil disobedience of the 1960s and 1970s shows how real or perceived threats can easily result in overreaction by authorities that threaten citizens' rights. (FBI Director Robert Mueller III has himself chronicled the various abuses that have occurred in the United States during times of crisis: the "Palmer Raids" of 1919, the Japanese internment during World War II, and the FBI's COINTELPRO program of the 1960s and 1970s.)

Accordingly, in this chapter I want to eliminate some of the misinformation and hyperbole in the debate on civil liberties and effective investigation since September 11 and the Patriot Act. I want to highlight valid points on both sides of the issue in order to achieve a better understanding of the problems facing America today.

The debate needs to proceed in an informed but dispassionate way. Only by debating the true problems facing law enforcement and national security, and the true costs of law enforcement action, can we dispel public paranoia, obtain public cooperation, and thereby maximize Americans' security without too high a price on personal freedoms.

THE PATRIOT ACT

The Patriot Act is 342 pages long and contains about 160 provisions. Very few people are conversant with every change made by the legislation. It is safe to say, however, that at least some of the provisions in the Act are noncontroversial. For instance, Section 102 of the Act contains the "sense of Congress" condemning discrimination against Arab and Muslim Americans. In addition, many provisions were on the drawing boards long before September 11—for example, to remedy gaps in the law as it dealt with emerging computer technology and electronic communications.

Other provisions were added specifically in response to September 11 because of the new threat of terrorism. The most controversial provisions of the Act are those which have been repeatedly cited in news articles and discussed on civil-libertarian websites. These provisions include requests for business records, use of "sneak and peek" search warrants, provisions for e-mail surveillance, permission to share intelligence-driven information with criminal investigations and prosecutors, and definitions of terrorism that raise questions about the First Amendment right to dissent. Consider the following provisions.

REQUESTS FOR BUSINESS RECORDS

Section 215 of the Patriot Act allows the FBI to request Foreign Intelligence Surveillance Act (FISA) orders for business records and other "tangible things." The main criticisms of this provision by civil libertarians are that the FBI need not show probable cause or even reasonable suspicion; persons served with such orders are prohibited from disclosing the fact to anyone else; and there is no notification to the person whose records are obtained.

These criticisms can easily be countered. Criminal subpoenas and court orders for business records and other materials held by third parties have never required any showing of probable cause or even reasonable suspicion—because they are not "searches." They are not considered searches because, in the legal sense, one does not have a reasonable expectation of privacy in matters that one has openly entrusted to someone else. For example, the bank records of someone suspected of committing bank fraud are usu-

ally obtained by the FBI through a subpoena requiring only relevance, not any level of suspicion (in fact, there is a federal privacy protection law that *prohibits* search warrants from being used to obtain records from certain third-party holders of records, those intending to publish; in those cases, the law specifies that subpoenas *must* be used). It can be argued, and government officials have done so successfully, that it should not be harder to investigate terrorist suspects than ordinary criminal suspects.

This section of the Act does not allow for investigation of Americans *solely* based on exercise of First Amendment rights. For example, the FBI would *not* be able to seek records about someone who merely wrote a letter to the editor criticizing government policy. However, this First Amendment protection only extends to citizens and permanent residents. Many if not most criminal subpoenas and court orders contain provisions prohibiting the third party from notifying the subject and, with only a few exceptions, law enforcement need not inform criminal subjects that their records have been obtained. Court orders for nondisclosure are usually available to delay any required notice until the conclusion of the investigative phase. (Otherwise, preliminary investigative steps would tip off the subject.) It is true that a criminal subject, if and when charged, will eventually learn of the evidence that the government has obtained, including any records. But if a terrorist is charged criminally, he or she would also probably learn of the fact that the federal government had obtained his or her records from a third party through the FISA method.

There is much concern over the potential for infringement of First Amendment protection by use of Section 215 authority with libraries and bookstores to ascertain the books a person has read or purchased. This concern has even resulted in internal policies or local resolutions being adopted to mandate noncompliance with relevant provisions of the Act. However well-intentioned such concern may be, it is misplaced. As a practical matter, it is easier to obtain an ordinary grand jury subpoena than to obtain a FISA court order under Section 215 to seek library or bookstore records. It also should be recognized that such limited use of subpoenas has on occasion been justified. For example, when the Unabomber's "manifesto" cited four obscure books, the FBI promptly served subpoenas on certain libraries to ascertain who had checked out those books.

We know that the September 11 hijackers relied on public-access computers, including those available in libraries and stores like Kinko's, to communicate with each other via the Internet. There is a legitimate need for speedy access to records of such computer usage. (This would, of course, not include the content of any stored communications in computers, which must normally be obtained through a criminal or FISA search warrant demonstrating probable cause.) In fact, since September 11, FBI contact with libraries has been minimal and sporadic. In 2003, the attorney general announced that, thus far, no Section 215 order had been served upon any library. In any case, long before the Act, access to computer usage and other library records was possible via the subpoena route, requiring nothing more than a showing of relevance.

Thus, although this section of the Act creates an additional avenue through the FISA court to potentially obtain records, it does nothing to widen the government's power to acquire them and thus poses no additional risk to First Amendment protection in this area.

On the other hand, a little-noticed section of the Act, Section 505, allows FBI special agents to issue national-security letters to obtain three common types of records: an individual's telephone and Internet service provider toll and transaction records, bank records, and credit records. This delegation of authority down to special agents-in-charge has greatly streamlined and speeded up the process of issuing national security letters. The Department of Justice also expanded the authority to issue national security letters in preliminary investigations. It is also only fair to note that long-term secrecy accompanies the use of national security letters and the information obtained by the FBI. A further provision, tucked inside an intelligence-spending bill which was signed into law in 2003, expands the ability of the FBI to obtain a host of third-party records from a wide range of entities such as casinos, realtors, and the U.S. Post Office. (This legislative expansion was, however, far from a cakewalk. More than one third of the House, including fifteen conservative Republicans, voted against what some dubbed "Patriot Act II," stating that "expanding the use of administrative subpoenas [national security letters] and threatening our system of checks and balances is a step in the wrong direction.")

USE OF "SNEAK AND PEEK" SEARCH WARRANTS

Section 213 of the Act creates a uniform standard for courts to authorize delayed notice in execution of certain search warrants, as long as no items are actually seized.

So-called "sneak and peek" search warrants predate the Act. Section 213 merely made existing court practices uniform. Despite the temporary secrecy associated with this authority, there is strict judicial review of the justifications given and the length of delayed notice necessary (the standard is "reasonable cause," which is defined to include endangering the life or physical safety of an individual, flight from prosecution, evidence tampering, witness intimidation, or otherwise jeopardizing an investigation). Along with a subject's right to pursue appropriate remedies after the fact, this judicial review should provide sufficient protection against abuse.

In 2003, the House of Representatives voted to prohibit the use of "sneak and peek" warrants. However, even if this measure were to pass the Senate and be enacted into law, it is not clear what effect it would have because many courts had previously found inherent judicial authority to order such delayed notice in appropriate cases.

PROVISIONS FOR E-MAIL SURVEILLANCE

Section 216 of the Act deals with "pen/trap" information. On a telephone, "pen/trap" data are the numbers dialed into or from a target number. No search warrant establishing probable cause is necessary because courts and Congress have long determined that one does not have an expectation of privacy in the numbers alone. This type of information can therefore be obtained with a pen register court order approved by a magistrate judge.

Section 216 broadens coverage to Internet communications. The Internet communications equivalent to "pen/trap" data consists of the "to" and "from" headers of e-mail letters. It only makes sense that a pen register–type court order be available to obtain the limited to/from information in the e-mail context. The subject line is, however, considered to be content and can only be obtained with a search warrant.

The American Civil Liberties Union (ACLU) objects to the nationwide aspect of such orders. The issue here is that a judge cannot monitor the extent to which his or her order is being used. This objection, too, misses the mark. No such monitoring really ever occurred for regular telephone "pen/trap" orders. Before the availability of nationwide effectiveness, court orders had to list every conceivable communication carrier, which became more and more difficult with constant additions and changes in telecommunication carriers.

PERMISSION TO SHARE INTELLIGENCE-DRIVEN INFORMATION WITH CRIMINAL INVESTIGATORS AND PROSECUTORS

Section 218 of the Act allows law enforcement to conduct surveillance or searches under the FISA if a "significant purpose" is foreign intelligence. Debates on this part of the Act center on the phrase "significant purpose."

A criminal search warrant requires probable cause that a crime has occurred and that evidence of the crime is likely to be found at a particular place. However, searches on possible attempts by foreign countries to spy on the United States don't always have criminal searches as their objectives. A foreign intelligence officer—a spy—operating in the United States may not be breaking any criminal laws. In addition, American authorities may wish to neutralize such an officer's activities without prosecuting him.

For these reasons, a separate avenue to conducting foreign intelligence surveillance and searches was created in 1978 through FISA. In order to get authority to search or monitor wire or electronic communications under FISA, FBI agents must show probable cause that the target is a foreign power or is acting on behalf of a foreign power. Over time, in my opinion, it had become harder and harder, in a practical

sense, to obtain a FISA warrant. Practically speaking, there is no litmus test to scientifically quantify any given legal standard. So meeting any of the given standards will always be somewhat subjective.

Then international terrorism hit the United States. An international terrorist group is a "foreign power" under FISA. The FBI therefore was free to obtain orders to search and conduct surveillance of suspected terrorists under FISA authority. But terrorist acts are inherently almost always criminal as well. This reality caused problems because there was supposed to be a "wall" between the criminal and the intelligence investigation of specific terrorists.

As a result, both criminal and intelligence cases would be opened. But the FBI intelligence agent could not share any information with the FBI criminal agent working on the same matter—for fear that it would be seen as an end run around the criminal process. The criminal standard appeared to be stricter and harder to satisfy than the secret intelligence process. Consequently, the FISA Court demanded strict database checking, reporting, and other procedures to ensure that the primary purpose of any FISA order was for intelligence gathering and not for evidence gathering that could be used to prosecute the terrorist criminally.

For the most part, this regimen had worked fine when dealing with foreign country–sponsored spying. So few questioned how absolutely insane the "wall" was when applied to international terrorism. That is, no one questioned it until after September 11. Then there were plenty of questions—including those raised by the dramatic testimony of an FBI agent in the New York office. Prior to the attacks, he had been thwarted from launching a criminal fugitive investigation of two of the September 11 hijackers for exactly this reason.

After September 11, then, there was plenty of reason for the Department of Justice to seek to bring the wall down. This was accomplished in the Act—with the change of essentially one word. Instead of intelligence having to be "the" purpose of a FISA order, Section 218 said it only need be a "significant" purpose. The wall was brought down, allowing sharing of intelligence-derived information with criminal investigators and criminal prosecutors.

This practice was subsequently approved in a 2002 decision by the FISA court of review. The decision opened the door to conducting both types of investigations, criminal and intelligence, on the same terrorist subjects. An investigator can select the type of criminal or intelligence method that may be the most effective. Then the information can be shared fully with every federal investigator or intelligence officer having an interest. This ability to combine the best of the criminal and intelligence worlds has become perhaps the main rationale for the current argument by the FBI that it ought not to be split up, or have its intelligence function severed, as some legislators have proposed.

But with the throttle now set at full-speed ahead when it comes to FISA initiatives in the war on terrorism, we must ask about the potential for their abuse. The

judges appointed to the FISA court are the first line of defense to prevent abuse of the process. But subjectivity is inherent in this judicial process. It may be that FISA judges are even more susceptible to subjectivity than regular federal district judges because of the cloak of secrecy that surrounds their decisions and the fact that there is no appeal except in the event of any decision that adversely affects the government. (There has only been one appeal ever taken in the history of the FISA court.)

Above all, the FISA process should not become an end run around the normal criminal process. Foresight and oversight must be exercised so this doesn't happen—now or somewhere down the road. It can even be argued that the perception of an "end run" occurring is enough reason to consider instituting an independent oversight review process.

DEFINITIONS OF TERRORISM AND THE RIGHT TO DISSENT

The Patriot Act defines domestic terrorism as "acts dangerous to human life that are a violation of the criminal laws of the United States or of any state" and that "appear to be intended . . . to influence the policy of a government by intimidation or coercion" (see Section 802). Civil libertarians believe this "overbroad definition" creates a new crime, which may be used against activists exercising their rights to assemble and to dissent. However, the phrase "acts dangerous to human life" consists of strongly limiting language. This limiting language should exclude all lawful activism. For someone to be defined as a domestic terrorist, he or she must first commit a crime that is an act dangerous to human life. Property damage, even damage of great magnitude, is not enough.

On the other hand, some types of severe property damage, such as the setting of arson fires or the spraying of gunfire into what may be believed to be an unoccupied building (as, for example, occurs repeatedly at Planned Parenthood clinics around the country) could be seen as so reckless in endangering human life as to fall under this definition. The rights of all American citizens to engage in lawful protest by speaking, writing, marching, and other nonviolent acts must, however, be protected.

Close attention also should be paid to the use of large-scale interviewing initiatives; police monitoring of public events, including marches and other lawful protest events; the use of tipsters and other informants; and other privacy-defeating database mining initiatives. Such initiatives must not limit the exercise of our First Amendment rights.

Unfortunately, there are indications that the FBI failed to pay close attention when, in anticipation of large protests in Washington, D.C., and San Francisco against the war in Iraq, it issued an intelligence bulletin in 2003 to law enforcement officers around the country that seemingly blurred the distinction between First

Amendment–protected speech and acts of terrorism. The bulletin has since been posted on the FBI's website. The purpose of the bulletin is to "provide law enforcement with current, relevant terrorism information developed from counterterrorism investigation and analysis." The bulletin discusses how protestors sometimes have used training camps to rehearse for demonstrations, the Internet to raise money, and gas masks to defend against tear gas.

Whether due to overzealousness or simple carelessness, this bulletin blended lawful protest activities, civil disobedience, and terrorism together, providing little in the way of constructive guidance and perhaps unnecessarily confusing the nation's law enforcement officers who are responsible for policing such events. For example, shortly after the bulletin was issued, Miami police are reported to have unjustifiably fired rubber bullets and used batons, pepper spray, tear gas canisters, and concussion grenades on people demonstrating against Free Trade Area of the Americas meetings in Miami.

However, when certain lines are crossed, like commission of acts dangerous to human life, then First Amendment rights should not be used to shield perpetrators. For instance, because Kathleen Soliah (who later named herself Sara Jane Olson) spoke at protest rallies in the early 1970s, her exercise of First Amendment rights should not serve to obscure what else she did or to protect her from being brought to justice for her participation in a Symbionese Liberation Army pipe-bomb murder attempt, bank robbery, and other crimes.

Unfortunately, there are always a few persons who, at some point, lose patience with nonviolent, lawful methods of advocating on behalf of their cause or are otherwise driven to cross the line to domestic terrorism. Sometimes such persons seek to employ their First Amendment and other civil rights as covers for their behind-the-scenes criminal acts. This does make it more difficult, but not impossible, for law enforcement to protect the public.

THE INCREASE IN SURVEILLANCE

Let me turn now from specific sections of the Patriot Act to related policies and problems, including the increase in surveillance, mass-detention initiatives, and the need for the Freedom of Information Act.

The Dangers of an Orwellian Future

Department of Justice interrogations of large numbers of young Arab men fitting certain criteria have received harsh criticism from civil-liberties organizations. So have the announced-but-never-implemented Operation TIPS (Terrorist Information and

Prevention System) and the Pentagon-proposed Total Information Awareness project (recently renamed the "Terrorist Information Awareness" program). The loosening of guidelines allowing FBI agents to enter public places (including churches and mosques) and to surf the Internet have also met with criticism from civil libertarians.

In *1984*, George Orwell wrote, "How often, or on what system, the Thought Police plugged in any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate, they could plug in your wire whenever they wanted to."

In terms of heightened surveillance potential and consequent loss of privacy, the dangers of a *1984* future for America cannot be overstated. One does not need to be an alarmist to agree with Steven Aftergood, director of the Project on Government Secrecy at the Federation of American Scientists, that "there is an enormous temptation to expand surveillance and information gathering. And unless there is an effective system of checks and balances, sooner or later this kind of surveillance is going to get out of control."

The Dangers of Corporate Surveillance

The ACLU is right in pointing out that the increase in surveillance is as much due to the private sector as it is due to the government. The danger stems not from a single government program but from a number of parallel developments in the worlds of technology, law, and politics.

Let me relate some of my own experience. Despite having an unlisted telephone number, not registering my driver's license and cars to my home address, and attempting to remove my name from a major commercial database, the national news reporters were on my doorstep within an hour of my May 21, 2002, letter to FBI Director Robert Mueller, published May 28, 2002, in *Time* magazine. I joked that they seemed more effective in tracking persons down than the FBI. They told me it only took a couple of keystrokes on the computer to find me.

During a LexisNexis training session a few months later, I had the instructor input my name, and despite my earlier attempts to be unlisted, my name, address, telephone number, and children's names popped up immediately—along with how much we had paid for our house.

So an enormous amount of information has been gathered on almost every American by private businesses as well as government entities. It is now just a question of mining the information to exploit its value. The cameras that capture one's presence in all types of public venues are not usually those of any law enforcement or government officer but of security-conscious private entities. For example, Minneapolis police have installed many "crime-fighting surveillance cameras" downtown, with $250,000 of the cost paid by the Target Corporation.

The Exercise of Discretion

Consequently, fear exists that such cameras, if misused by public officials, could chill public protest activity protected by the First Amendment or otherwise invade persons' privacy. But the key to whether these initiatives ultimately will be a good or bad thing lies in discreet use of the stored data. For example, it turned out to be a good thing recently that a Californian had a surveillance camera fixed on his neighbor's property. The camera recorded a portion of the kidnapping of his neighbor's child. It also proved beneficial that a surveillance camera apparently recorded a bit of Timothy McVeigh's vehicle during his bombing of the Alfred P. Murrah Federal Building in Oklahoma City. In addition, the banking industry and the FBI have long and good experience in the use of footage from bank surveillance cameras to identify bank robbers.

Exercise of discretion similarly should be required in terms of follow-up to all information obtained from citizen tipsters. Even without a formal program of registering citizens who furnish tips, the (at times panic-struck) public has been more than willing to call in information and tips to the FBI and other law-enforcement agencies. In calling for greater vigilance, citizens and noncitizens alike have been repeatedly encouraged to report what they see or know. Only a small percentage of this information may turn out to be valuable in actually uncovering a terrorist or terrorist plot. But even that small percentage may justify law enforcement's continued encouragement of citizen reporting and a certain amount of time invested by law enforcement in tracking down such tips. Discretion must be exercised by law enforcement not only in determining which tips or leads to follow up but also in deciding the amount of documentation to retain.

Some in the FBI have criticized the Bureau for not showing sufficient discretion—because all leads are being followed. The *U.S. News & World Report* quotes unnamed supervisors saying, "You used to look at threats; you knew what had validity; you'd get to them after you got all these other things out of the way. Now no matter how bizarre or how routine, you go after them." Similarly, FBI spokesman Bill Carter was quoted as saying, "At one time, when information came to us, a lot of times based on experience, the investigator would say, 'Nah, this is not something we will follow through on,' but after the September 11 attacks, the director has stated that no counterterrorism lead will go uncovered."

This strategy, however, ignores the mounting number of documented instances of federal agents, facing intense pressure to avoid another terrorist attack, who have acted on information from tipsters with questionable backgrounds and motives, touching off needless scares and upending the lives of innocent suspects. Federal officials defend their strategy of running most such terrorist tips to ground, calling it critical to thwarting another attack. But we must be careful that we do not abdicate our responsibilities in evaluating citizen tips and informant information before acting in a way that negatively impacts innocent persons.

Coupled with this broad no-tip-will-go-uncovered policy was the Department of Justice's announcement in 2003 of new national security guidelines that allow the FBI to conduct a threat assessment of potential terrorists or terrorist activity without initial evidence of a crime or national security threat. Although this policy is justified by Department of Justice officials as necessary to prevent acts of terrorism before they occur, the ACLU and others have criticized "the notion that the government can put your life under a microscope without any evidence that you're doing anything wrong." A study released in 2002 by Syracuse University, using Justice Department statistics, appears to confirm the position of the ACLU. Of the thousands of people referred by the FBI and other federal investigators to prosecutors in connection with terrorism since September 11, 2001, only a handful have been convicted and sentenced to long prison terms.

DETENTION AND DEPORTATION

In the same vein, new initiatives undertaken by law-enforcement agencies must be closely scrutinized to ensure they truly serve the needs of public safety. An example of such an initiative that should be scrutinized consists of the "special registration" rules for immigrants that, according to news reports, have required nationals from twenty-two countries to sign up with immigration authorities. As a result, there are reports that more than 13,000 Arab and Muslim immigrants are in deportation proceedings, mostly for routine immigration violations, like not registering a change of address.

At the same time, Supreme Court decisions have recognized that a "right to not be talked to" has never existed in our country and that "it is an act of responsible citizenship for individuals to give whatever information they may have to aid in law enforcement" (see the *Washington v. Glucksberg*, *Miranda v. Arizona*, and *Chavez v. Martinez* decisions cited in the bibliography).

Mass-detention initiatives are of great concern. As I noted in my February 26, 2003, letter to FBI Director Mueller, "The vast majority of the one thousand-plus persons detained in the wake of September 11 did not turn out to be terrorists. They were mostly illegal aliens. We have every right, of course, to deport those identified as illegal aliens during the course of any investigation. But after September 11, headquarters encouraged more and more detentions for what seem to be essentially public-relations purposes. Field offices were required to report daily the number of detentions in order to supply grist for statements on our progress in fighting terrorism . . . from what I have observed, particular vigilance may be required to head off undue pressure (including subtle encouragement) to detain round up suspects—particularly those of Arabic origin." (My figure of "one thousand–plus" detainees was based on the FBI's

daily press statements issued after September 11. The Department of Justice's Office of Inspector General report, cited in the bibliography, actually counted 762 illegal aliens detained after September 11.)

The temptation exists to fall into an "us-versus-them" attitude, reserving the most aggressive initiatives for Middle Eastern males. The most common citizen tip received by the FBI sounds something like: "I don't want you to think I'm prejudiced because I'm not, but I just have to report this because one never knows. I'm worried and I thought the FBI should check it out." The tipster then provides general information about an Arab or Middle Eastern man who is a neighbor or coworker. Typically, the information includes nothing specific to potential terrorism. Should such a tip be followed up? Or is it little more than racial profiling? These are perhaps the most important questions today and in the future.

The Department of Justice has exempted its anti–racial profiling policy from application to the "war on terrorism." This is a troublesome decision. On right-wing talk shows, we hear people say, "All Muslims aren't terrorists, but all the terrorists were Muslims." The Justice argument here is that we must do everything in our power to learn of the next attack before it happens—and then prevent it. This means many false leads must be pursued.

However, before September 11, the single most dangerous terrorist groups in the United States consisted of radical Christians, the kind of groups with which Timothy McVeigh had ties. Not all Christians were terrorists, but all the terrorists were Christians. Did we post FBI agents at every Sunday church service? Of course not. The FBI targeted the radical factions that perverted Christianity for their own evil purposes.

Today, then, we need to concentrate law-enforcement efforts on the extremist groups and violent individuals who are suspect based on specific, reasonable evidence. We need to follow this process for suspects who are radical Muslims, radical Christians, radical animal/environmental rights believers, or whomever the evidence suggests should be investigated.

THE PENDULUM HAS SWUNG TOO FAR

It was clear to some experts ahead of time, and to almost all experts and nonexperts alike in hindsight, that our country was complacent in a variety of ways prior to September 11. Very few people believed that foreign terrorists would strike on American soil to the extent they did. This mindset made most "emergency" law enforcement actions and court orders for national security almost nonexistent. Prior to September 11 and other terrorist-type incidents (including the anthrax letters and the D.C.-area sniper shootings), we would probably not have tolerated the myriad intrusions and restrictions on our personal lives and affronts to our dignity that we

now all seem quite willing to put up with (including airport inspections of removed shoes and use of scanners to examine one's body cavities).

What's happened since September 11? The pendulum has really swung, at least with respect to terrorism. Without adequate oversight, the pendulum risks swinging too far, violating the rights of citizens and immigrants without appreciable gains in security.

What are we actually talking about in terms of possibly giving up "civil liberties"? All people may be created equal, but it's pretty obvious that our rights to "life, liberty and the pursuit of happiness" are not equal. Life is a lot more important than liberty, which in turn is more important than one's pursuit of happiness. The oft-recited quote that "the Constitution is not a suicide pact" reflects this ordering. Because our right to life, and thus to security, is itself a liberty, and the most precious and important one at that, the weighing of civil liberties versus security is, in essence, a false debate.

Despite Patrick Henry's lofty words "Give me liberty or give me death" which urged Americans to war against the British, it turns out that few incarcerated individuals who have lost their civil liberties and personal freedoms commit suicide. In fact, it turns out that most people who have been placed in concentration camp–type existences even worse than prison, and who have lost every shred of their humanity, still seem to want to cling to life.

Of course, most people who are not in prison and who commit suicide are unhappy—and we can debate endlessly about which rights are paramount. But if the reader agrees with me that life is very high on the list, then consideration of the tradeoffs between life and the other liberties often is necessary when it comes to practical ways of preventing acts of terrorism. These tradeoffs can only be avoided by improving the ability of law enforcement to "home in" on the real criminals and terrorists. But law enforcement does not presently have the ability to divine criminal intent by reading minds. So our ability to accurately identify the real culprits is always limited by fixed factors—most importantly by the state of forensic science and by the amount of existing inside information furnished by informants and confidential sources. In an ideal world, this means there would be efficient methods for narrowing a given pool of suspects without having to interview them, surveil them, ask others about their activities, and in some cases subject them or their possessions to interception, seizure, or forensic testing. Unfortunately, the ideal world does not presently exist and identifying criminals and terrorists still requires use of these methods.

How these investigative actions are undertaken is of great importance. For example, given the present reality that homing in still requires the use of many of these standard law-enforcement activities (like citizen tips, physical surveillance, electronic surveillance, searches, seizures, and forensic testing), the intrusion can be greatly alleviated and minimized if done in a professional, respectful manner (and after September 11, FBI agents were afforded training in just this area). In some instances, how

an investigative action is undertaken may actually prevent a potential risk to civil liberties from being realized. Even the impact of true liberty deprivations such as detaining or arresting individuals can be greatly alleviated by professional conduct appropriate to the circumstances. Efforts by the FBI director and other management to reach out to the most affected groups in the Muslim community have gone a long way toward improving how such law enforcement actions are perceived.

By contrast, it has been demonstrated, for example in Northern Ireland, that draconian restriction of civil liberties in combating terrorism has led to more terrorism.

THE FREEDOM OF INFORMATION ACT AND PROTECTION FOR WHISTLEBLOWERS

Issues of national security require considerable secrecy. But terrorist threats uninvolved with foreign-country sponsorship may not require as much secrecy because they are more like criminal than traditional intelligence matters. Sufficient generic data can be provided to key congressional oversight committee members—information like the number of times each particular investigative technique is used, within a set of agreed-upon categories.

The Freedom of Information Act (FOIA) fulfills a necessary watchdog function. The act often is viewed as a nuisance, or worse, by law enforcement and intelligence officials charged with protecting national security. But litigation involving FOIA requests usually is decided by a small cadre of experienced judges who are adept at balancing the watchdog function of the act with the government's need for secrecy.

Better legal protection for government whistleblowers should be enacted. At present, federal laws are either inapplicable or ineffective for many government employees such as FBI agents. As I said in a recent letter to selected senators in support of proposed legislation designed to remedy this problem: "Prior to my personal involvement last year in a specific matter, I did not fully appreciate the strong disincentives that sometimes keep government employees from exposing waste, fraud, abuse, or other failures they witness on the job. Nor did I appreciate the strong incentives that do exist for government agencies to avoid institutional embarrassment. . . . Unfortunately, the cloak of secrecy which is necessary for the effective operation of government agencies involved with national security and criminal investigations fosters an environment where the incentives to avoid embarrassment and the disincentives to step forward combine. When this happens, the public loses. We need laws that strike a better balance, that are able to protect effective government operation without sacrificing the agencies' accountability to the public."

THE IMPORTANCE OF INTEGRITY

The generally accepted goal of preventing acts of terrorism is accompanied by the potential for intrusions into the lives of ordinary, innocent American citizens and especially into the lives of immigrants and travelers in America. I emphasize the word "potential" to describe the intrusions. Care must be taken so the potential is not realized. Successful future terrorist attacks on American soil will greatly magnify the likelihood of intrusions and abuses.

To avoid this outcome, we need more than mere lip service and assurances from on high; we need concrete proposals for employing additional safeguards. To address the difficult questions, we need free, open, and informed debate with an eye to enhancing, rather than eroding, mutual trust. In 2002, I testified before the Senate Judiciary Committee about problems I saw with the FBI's bureaucracy and intelligence gathering. I concluded then, as now, on the importance of integrity.

The final reason I can think of for the FBI to adhere to the highest standards of integrity is another self-serving one. Since joining the FBI, I can't tell you how many debates, both public and private, I've engaged in about where the line should be drawn between the needs of effective criminal investigation and preserving the rights of innocent citizens. The trick is to be as surgical as possible in identifying the criminals and those dangerous to our country's security without needlessly interfering with everyone else's rights. From what I've seen in recent years, I can safely assure you that the FBI usually does a pretty darn good job of this. Although such debates always begin with addressing specific provisions of the policy or law in question, they almost always boil down, in the final analysis, to one thing: Trust. It's hard to win the debate if the person on the other side simply refuses to trust what you're saying about how the law or policy is applied in practice. In fighting the current war on terrorism, the federal government has already asked for and received further investigative powers. Although it can be argued that many of the new powers are simply measures to apply prior law to new computer technology or things that any private citizen can do, some members of the public remain apprehensive that the FBI will go too far and will end up violating the rights of innocent citizens. It may be necessary to ask for certain other revisions of policy, or even law. The only way the public's distrust can be alleviated, to enable us to do our job, is for the FBI, from the highest levels on down, to adhere to the highest standards of integrity.

BIBLIOGRAPHY

American Civil Liberties Union report, "Federal Court in Detroit Hears Arguments Today in ACLU Challenge to Patriot Act," December 3, 2003.

Bill Carter, quoted by Michael Moss, "False Terrorism Tips to F.B.I. Uproot the Lives of Suspects" *New York Times*, June 19, 2003.

Chavez v. Martinez, 2003 U.S. LEXIS 4274.

Department of Justice, Office of the 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" (Detainee Report), June 2, 2003.

Amy Driscoll, "Judge: I Saw Police Commit Felonies," *Miami Herald*, December 20, 2003.

Miranda v. Arizona, 384 U.S. 436 at 477-478 (1966).

Michael Moss, "False Terrorism Tips to F.B.I. Uproot the Lives of Suspects" *New York Times*, June 19, 2003.

Robert Mueller III, speech to American Civil Liberties Union, June 12, 2003.

———, speech to Stanford Law School, October 18, 2002.

George Orwell, *1984* (New York: Random House, 1992).

"Protecting the Nation: The FBI in War and Peace," Transactional Records Access Clearinghouse study, 2002. http://trac.syr.edu/tracfbi/findings/aboutFBI/keyFindings.html.

Solana Pyne, "Making Enemies," *Village Voice*, July 9-15, 2003. http://www.villagevoice.com.

Coleen Rowley, February 26, 2003 memo to Federal Bureau of Investigation Director Robert Mueller III, published in the *New York Times,* March 6, 2003.

———, statement to Senate Committee on the Judiciary, oversight hearing on counterterrorism, June 6, 2002.

———, memo to Federal Bureau of Investigation Director Robert Mueller III, dated May 21, 2002; *Time* magazine, May 28, 2002. http://www.time.com/time/covers/1101020603/memo.html.

Celia Rumann and Michael P. O'Connor, "Into the Fire: How to Avoid Getting Burned by the Same Mistakes Made Fighting Terrorism in Northern Ireland," *Cardozo Law Review*, Vol. 24, No. 4, April, 2003.

Jay Stanley and Barry Steinhardt, *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society*, American Civil Liberties Union Technology and Liberty Program, January, 2003.

Rachel L. Swarns, "More Than 13,000 May Face Deportation," *New York Times*, June 7, 2003.

Nancy Talanian, "Guide to Provisions of the USA Patriot Act and Federal Executive Orders That Threaten Civil Liberties," Bill of Rights Defense Committee. http://www.bordc.org/index.html.

U.S. News & World Report, "Special Report: Inside the FBI," May 26, 2003.

Washington v. Glucksberg, 521 U.S. 702 at 721 (1997).

Shaun Waterman, "Figures Show 'Hype' of Terror War," United Press International, December 8, 2003.