VOLUME 63

NUMBER 3

## THE TYRRELL WILLIAMS MEMORIAL LECTURE

The Tyrrell Williams Memorial Lecture was established in 1948 by the family and friends of Tyrrell Williams, a distinguished member of the faculty of the Washington University School of Law from 1913 to 1946. Since its inception, the Lectureship has provided a forum for the discussion of significant and often controversial issues currently before the legal community. Former Tyrrell Williams Lecturers include some of the nation's foremost legal scholars, judges, public servants and practicing attorneys.

The Honorable William H. Webster, distinguished jurist, public servant and attorney, delivered the 1985 Tyrrell Williams Memorial Lecture on the Campus of Washington University in St. Louis, Missouri, on March 14, 1985.

## SOPHISTICATED SURVEILLANCE— INTOLERABLE INTRUSION OR PRUDENT PROTECTION?

## WILLIAM H. WEBSTER\*

A few days ago someone gave me the lapel button I hold in my hand. It reads: "My job is so secret even I don't know what I'm doing."

1985

<sup>\*</sup> Director of the Federal Bureau of Investigation, Washington, D.C. Numerous times in his career, Judge Webster has left private practice to serve the public interest. He served as United States Attorney for the Eastern District of Missouri from 1960 until 1961. He was appointed a Judge of the United States District Court for the Eastern District of Missouri in 1970, and elevated in 1973 to the United States Court of Appeals for the Eighth Circuit. He resigned the Bench in 1978 to become Director of the FBI. Judge Webster is a graduate of Amherst College and the Washington University School of Law.

There may be some rough correlation between that statement and how we feel about secrecy. Secrecy conjures up images of Orwellian intrusion by government, of clandestine activities that put at risk our most cherished individual liberties, and of mistakes and blunders concealed within documents classified "Secret" or "Eyes Only."

There is, of course, historical basis for all of these concerns, but that is not my real purpose in speaking to you today. Rather, I propose to talk about some of the measures we legitimately can employ in a free society to protect ourselves from the ravages of crime, of terrorism, of betrayal of the public trust.

Our basic liberties are identified and enshrined in our Constitution. There must be no retreat from that. An awareness of and respect for the law's demands is fundamental to all who are sworn to uphold the law. But it is no defense of ordered liberty to deny to those whom we commission to enforce the laws the lawful tools that modern science and professional advancement have made possible. There is a balancing process which each of us must share. We call it "justice" and it continues to be the great interest of man on earth.<sup>1</sup>

When the FBI announces arrests in a major case such as a round-up of outlaw motorcycle gang members, charges brought against the leaders of organized crime, interdiction of a terrorist plot, the break-up of a huge drug distribution network, or the revelation of major frauds against the government or corruption in public office, there is usually a substantial cheer from around the country that we have been able to serve and protect our fellow citizens. These investigations are frequently conducted in secret over sustained periods of time, utilizing sophisticated and, at times, intrusive techniques. It is my experience that these techniques generally have been accepted as necessary and their use largely has been supported. The key to acceptance lies in preestablished rules of conduct and ultimate public accountability for the faithful adherence to such rules.

When these factors are absent, what we do may be seen as intolerable intrusion. When they are present, our work is most likely to be viewed as it was intended to be—prudent protection for our fellow citizens.

Through the years a healthy public skepticism has helped to keep those of us in law enforcement mindful of the ultimate source of our

<sup>1.</sup> Daniel Webster quoted in 2 LIFE AND LETTERS OF JOSEPH STORY 624 (WILLIAM W. STORY, ed., 1851).

authority. Trust is something to be earned by performance and maintained by periodic public accountability.

Thus far, I have painted with a broad brush some thoughts in which I sincerely believe. I will now refine the strokes a bit and focus on some critical areas where these principles find application in modern, sophisticated law enforcement.

I propose now to discuss some sensitive investigative techniques that we use currently—the informant, electronic surveillance and the undercover agent.

These techniques help us to reach beyond the individual street criminal to the upper echelons of criminal enterprises, to those who are calling the signals, making the profits and who are really responsible for the heavy impact of crime in our society. These tools help us obtain information that traditional investigative techniques—the interview, the physical surveillance and the crime scene inspection—simply will not produce.

The use of informants, electronic surveillance and undercover agents has become very sophisticated. Some say their use is merely prudent protection for society. Others argue that it is an intolerable intrusion into our private lives. But maintaining law and order in society often requires a certain amount of intrusion. In a typical investigation, our agents will talk to people, look into records and examine forensic evidence. These activities are, to a lesser degree, intrusive.

Most of us willingly accept some degree of intrusion to ensure public safety. For example, some years ago while sitting on the Eighth Circuit, I wrote an opinion touching upon the use of inspection points for passengers boarding aircraft. It was my opinion then that the additional measure of safety provided to passengers in flight more than offset the minimal intrusion involved in that situation.<sup>2</sup> Experience has reinforced that view and, as I said then, I believe the public would be outraged if these checks suddenly were removed from airport terminals.

But the use of sensitive techniques in federal investigations has raised some important issues—particularly questions about fairness. I remember reading an article that appeared a number of years ago in the *Ameri*can Bar Association Journal entitled "Lincoln and the Law" by the noted legal scholar Arthur L. Goodhart, who delivered the Tyrrell Williams Lecture in 1964. Dr. Goodhart made an important observation about

<sup>2.</sup> United States v. Flum, 518 F.2d 39, 45 (8th Cir. 1975).

Lincoln's legal philosophy. He said, "[T]o Lincoln the most important idea that the law represented was the idea of fairness. Justice carries a pair of scales that are evenly balanced."<sup>3</sup> Maintaining that sense of fairness is as important today as it was in Lincoln's time. So, I shall tell you how we manage these sensitive techniques to keep the scales in balance.

The informant is the single most important tool in law enforcement. Every police officer knows that if a bank robbery is not solved within forty-eight hours, it is not going to be solved, in all likelihood, until an informant is located who has some information about the robbery and is willing to share it. After all the forensic evidence is in, after all the eyewitnesses have been interviewed, if the police cannot find or identify the bank robber, it is going to depend on someone who has information either before or after the fact. This is true in most investigations, but is especially true of the more elusive, insulated and often consensual criminal activity that is associated with organized crime and white-collar crime.

There are many kinds of informants. On one end of the spectrum is the professional criminal informant who is paid for information, promised confidentiality, and not required to testify. He is simply giving us information that helps build prosecutable cases. At the other end of the spectrum is the good citizen who gives us information out of a laudable sense of duty. He may want his identity kept confidential. If he agrees to play a more important role in the investigation, we call him a cooperating witness because he ultimately may testify in court. In ongoing investigations his immediate role may be to feign collusion with the criminal element, to observe and gather evidence, or to introduce our undercover agents to those running the criminal enterprise.

An informant may be someone deeply involved in crime, such as Jimmy Fratianno. Fratianno was a vicious criminal and an admitted mob hit man. He had become a very important organized crime figure. But he was in serious trouble: someone had put out a contract on him. So he came to us. Because of his long-time criminal ties, Fratianno revealed some very valuable information on the structure, interrelationships and activities of organized crime groups. His testimony resulted in the convictions of the entire ruling hierarchy of the Los Angeles organized crime family.

A cooperating witness may be someone with an unblemished reputa-

<sup>3.</sup> Goodhart, Lincoln and the Law, 50 A.B.A. J. 422, 441 (May 1964).

tion for honesty and fairness such as Judge Brockton Lockwood. Judge Lockwood, an associate judge from southern Illinois, was serving as a visiting judge in Cook County. He came to the FBI after he became aware of the long-known but unproved corruption in the Cook County court system. I met with him and he eventually agreed to pose as a dishonest judge, hiding a tape recorder in his cowboy boots. Cultivating an image as an "ignorant hillbilly," Judge Lockwood gathered information that has been crucial in our GREYLORD investigation. In a newspaper interview, Judge Lockwood explained why he decided to report the judicial corruption: "I tried to avoid it. But my conscience just wouldn't let me."<sup>4</sup> I wish more people shared that sense of responsibility.

Jimmy Fratianno and Brockton Lockwood are at different ends of the informant spectrum. Yet they both provided important information on criminal activity. Our main concern in selecting informants is not their lovability, but their reliability.

At the same time, once an ongoing relationship with an informant has been established, fairness to the public as a whole requires us to do an increasingly better job of managing the informant. Criminal informants are capable of working both sides of the street. They need supervision. That is why we keep extensive records on our dealings with them. I have thought for a long time that the so-called "hip-pocket informant," an informant on whom the police officer keeps no record, is an occasion for mischief. We require that absolutely meticulous records be kept on our informants. Their confidentiality is protected, but we know, and our files reflect, what they have done, what they have been instructed to do, what they have been paid and what they have produced. Those records are carefully safeguarded, but they exist to discharge our responsibility to account for the activities of a particular informant.

In assessing the suitability of an informant, we are interested in such things as his productiveness, his personal involvement in crime, the likelihood of his engaging in violent behavior, the reasons he is willing to cooperate with us and, most importantly, his willingness to follow instructions. We must be sure that our informant is not taking advantage of his relationship with us to engage in frolics of his own, or worse, to become an agent provocateur. With careful supervision we can direct him in paths most likely to lead to a successful investigation that will withstand the closest judicial scrutiny.

<sup>4. &#</sup>x27;Hillbilly' Judge Stars in Chicago Courtroom Sting, The L.A. Times, Aug. 12, 1983 at 1.

We function under Attorney General guidelines and FBI regulations that spell out specific responsibilities for use of informants, a vitally important tool. The agent controlling an informant is required to report to his supervisor any criminal activity of the informant that comes to his attention. Some minor illegal activity may be allowed to continue in the interest of getting information that will permit us to reach a much more significant and perhaps more dangerous criminal. This exception, however, does not extend to violence. We will not permit our informants to participate in violent crime. If such plans come to our attention, the informant will be instructed to dissuade the conspirators. If this fails, we will take steps to circumvent the violence. The informant understands that if he violates these instructions, he will be prosecuted.

We have learned that when confronted by overwhelming evidence of defendants engaged in wrongdoing, an increasingly popular defense strategy is to attack the means by which the evidence was acquired, to denigrate the government agents personally, and to play on jurors' innate sense of fairness. Unless the government witness has been prepared for such an assault, the slightest hesitancy or confusion can be made to suggest deviousness of purpose. The focus then shifts away from the defendant's own acts of wrongdoing. When, for example, an undercover agent participates in a scenario such as a contrived business dealing with criminals, the agent on cross-examination may be pressed to admit that he "lied" about his work. While deception is a legally sanctioned tool in law enforcement,<sup>5</sup> in skillful legal hands it may be inaccurately characterized as, if not entrapment, then somehow "unfair."

It therefore is the task of the prosecution to demonstrate both the necessity and the fairness of the procedures the government has employed.

Perhaps nowhere does this fairness factor come to the surface in a jury trial more visibly and more critically than when the government asks the jury to accept the testimony of a cooperating witness with a tainted record over the word of a defendant who has no record of prior convictions. Juries rightfully demand corroboration of the testimony of such a witness whom they have no reason to trust. Our natural aversion to "snitches," to criminals trying to buy their own way out of trouble with their testimony against others, requires a higher level of persuasion before such witnesses will be believed.

<sup>5.</sup> Lewis v. United States, 385 U.S. 206, 208-09 (1966); Sorrells v. United States, 287 U.S. 435, 441-42 (1932).

The lessons we have learned from the fairness factor at trial are these: (1) use the tainted witness as sparingly as possible in an undercover investigation and move him into the background as soon as he has vouched for our undercover special agents; (2) employ the electronic and video coverage to obtain confirmation from the defendant himself of what the cooperating witness will eventually say from the witness stand; and (3) rely more upon our own special agents to make the case at trial. The tainted witness' pretrial conduct must be able to withstand the most searching cross-examination, and their testimony must be so forthright that no jury can read into it any form of dissembling or equivocation. Under such circumstances juries will convict and their subliminal need for fairness will have been satisfied.

Where feasible, we use informants and our other traditional techniques to obtain the evidence we need on criminal activities. But sometimes these less intrusive methods will not do the job. Then when, we have probable cause to believe that criminal conversations can be intercepted in this manner, we may turn to electronic surveillance. The Title III provisions of the Omnibus Safe Streets and Crime Act of 1968 authorize and regulate this vitally important investigative tool, referred to as the Title III wiretap. These wiretaps are particularly effective in dealing with members of organized criminal enterprises who are often too wary to meet, but who must communicate in order to be effective.

In every instance when we use a Title III wiretap, a federal judge has authorized it upon a showing of probable cause. We distinguish Title III wiretaps from consensual monitoring wiretaps, which we use to listen to a conversation between a criminal and someone working for us. Although we are listening to that conversation, the courts have held there is no expectation of privacy because the person with whom the criminal is talking has consented that we overhear. But even then we listen pursuant to certain approved rules, so that it is not a promiscuous operation.<sup>6</sup>

One example will show our level of concern about keeping our agents advised of what they can and cannot do with respect to electronic surveillance. Shortly after I became director of the FBI, there was a Sixth Circuit opinion holding that notwithstanding the Title III wiretap statute

<sup>6.</sup> The same rules apply whether the device used to overhear conversations is a telephone or a microphone. Whatever the device, the key factor in distinguishing a consensual monitoring interception from a Title III interception is the consent of one person privy to the intercepted conversation.

authorizing us to install a microphone in a given place upon a showing of probable cause, courts do not have the authority to permit us to make a surreptitious entry to put the microphone in place.<sup>7</sup> That left us in the position of ringing the doorbell and saying, "Sir, may we put a microphone in your living room?" Obviously, we believed that opinion was clearly and seriously wrong. But the first thing we did was send a teletype to all of our field offices within the Sixth Circuit advising them of the opinion and instructing them to immediately discontinue any microphone wiretaps installed by surreptitious entry.

Not long after that, the Ninth Circuit came down with a parallel ruling,<sup>8</sup> and we immediately did the same thing in the Ninth Circuit. Fortunately for us, a similar case was working its way up through the Third Circuit. The Supreme Court heard that case and held that inherent in the authority to put a microphone in place is the authorization to make a surreptitious entry to do so. The Court said it was not even necessary for the authorizing court to spell that out in its order.<sup>9</sup>

But again, out of an abundance of caution and concern for fairness, I instructed the field that we would advise the court of every instance in which we intended to make a surreptitious entry and ask the court to include the authority to do so in the order. In that way, the judge would know beyond question what he was approving. Occasionally, we have a judge say, "Why do you require this? The Supreme Court doesn't demand that." We require it because we want to be sure that the judge knows exactly what we propose to do.

A court order for a wiretap will not be granted just because we ask for it. We must convince a federal judge that there is probable cause to believe a particular crime is being committed or is about to be committed, that a particular individual is involved in criminal activity, that a certain phone or house will be used and that certain conversations will likely occur on a particular phone. We have to tell the federal judge how many times we have tapped a phone so he can decide if we are on a fishing expedition and should be barred from further intruding on that person's privacy.

But even before the application for a Title III wiretap goes to the reviewing judge, it comes to FBI headquarters where my special assistants

<sup>7.</sup> United States v. Finazzo, 583 F.2d 837 (6th Cir. 1978), vacated, 441 U.S. 929 (1979).

<sup>8.</sup> United States v. Santora, 583 F.2d 452 (9th Cir. 1978), vacated, 441 U.S. 939 (1979).

<sup>9.</sup> Dalia v. United States, 441 U.S. 238 (1979), aff'g, United States v. Dalia, 575 F.2d 1344 (3d Cir. 1978).

and I scrutinize it carefully. These special assistants are selected for outstanding law school and clerking performance. They serve in an advisory capacity for two years before going on to promising legal careers. I have found they bring a fresh new dimension to our deliberations. If they find the application in order, and I concur, then I will approve it. Finally, the application goes to the attorney general or his designee for review.

An important element of the application is the description of the minimization procedures we will use to prevent our accumulating non-criminal and privileged information. These procedures include turning off the wiretap when there is a conversation taking place that is unrelated to the crime or where attorney-client privilege might be involved. When we are tapping a public phone booth, we make every effort to watch the booth so that we intercept conversations only when the suspect is using the phone. This precaution protects the public from indiscriminate listening and ensures fairness.

While we have directed most of our court-ordered electronic surveillance at organized crime and narcotics trafficking, we are also using this technique to investigate terrorist groups and espionage activities.

In our Chicago investigation of the FALN, a Puerto Rican terrorist group, we used closed-circuit television cameras to effectively gather information on the terrorists' bomb making. We watched them assemble the ammunition and make the bombs. This group was responsible for a number of serious bombings and armed robberies and our investigation revealed they were planning even more violence. Based on our TV monitoring and other evidence, we arrested four terrorists. During the pretrial phase of this case, the district court suppressed the videotapes on the ground that there was no statutory or other basis for the judge's granting an order pursuant to Title III for the use of closed-circuit TV cameras.<sup>10</sup>

Proposals for electronic surveillance under FISA receive a thorough review beginning with an FBI Headquarters supervisor. We want to be sure that our use of this technique is absolutely necessary.

<sup>10.</sup> While Title III does not expressly authorize the use of closed-circuit television surveillance, the Foreign Intelligence Surveillance Act of 1978 does. This act, known as FISA, created the Foreign Intelligence Surveillance Court, composed of seven federal district judges who must approve electronic surveillances that monitor conversations of people suspected of espionage or terrorism in the United States. The Act covers four categories of electronic surveillance: (1) wiretaps; (2) radio intercepts; (3) monitoring devices, such as microphones, closed-circuit television, transmitters that track vehicle movement, and other techniques; and (4) watch listing—acquiring wire or radio communications of a particular individual. Senate Select Committee on Intelligence, The Foreign Intelligence Surveillance Act of 1978: The First Five Years, S. Doc. No. 660, 98th Cong., 2d Sess. 3 (1984).

The Department of Justice appealed that ruling and, just recently, the Seventh Circuit reversed it. Judge Richard Posner distilled the law down to this one crisp conclusion: "There is no right to be let alone while assembling bombs in safe houses."<sup>11</sup>

The third of these very sensitive techniques is the undercover agent. He has been glamorized or criticized, depending upon one's perspective, primarily as a result of the enormous publicity accompanying the AB-SCAM cases.<sup>12</sup> But the undercover agent is not a panacea for law enforcement. He is a valuable weapon, especially effective in investigations involving consensual crime when we do not have a willing witness. This is true in prostitution, gambling, drugs and bribery, where there are willing participants on each side. The transactions are not taking place in the middle of Main Street so there are no witnesses. Courts have fully sanctioned, and congressional reports have encouraged, properly managed use of undercover agents.

To attack major criminal enterprises, we need staying power. We had long used informants to provide leads and occasionally function as cooperating witnesses acting out a predesigned scenario. But we found that

One important purpose served by all of these steps is to ensure that we do not direct electronic surveillance against people because of lawful political activities protected by the Constitution. We want to be confident that when we approve a FISA application, as well as any proposal for use of electronic surveillance techniques, we are using these tools in not only a *legal*, but an *appropriate* manner.

11. United States v. Torres, 751 F.2d 875, 883 (7th Cir. 1984).

12. United States v. Jannotti, 729 F.2d 213 (3d Cir.), cert. denied, 105 S. Ct. 243 (1984); United States v. Jenrette, 744 F.2d 817 (D.C. Cir. 1984); petition for cert. filed, 53 U.S.L.W. 1171 (U.S. Jan. 19, 1985) (No. 84-1171); United States v. Thompson, 710 F.2d 915 (2d Cir.), cert. denied, 461 U.S. 961 (1983); United States v. Williams, 705 F.2d 603 (2d Cir.), cert. denied, 464 U.S. 1007 (1983); United States v. Weisz, 718 F.2d 413 (D.C. Cir. 1983), cert. denied, 104 S. Ct. 1285 (1984); United States v. Silvestri, 719 F.2d 577 (2d Cir. 1983); United States v. Kelly, 707 F.2d 1460 (D.C. Cir.), cert. denied, 464 U.S. 908 (1983); United States v. Alexandro, 675 F.2d 34 (2d Cir.), cert. denied, 459 U.S. 835 (1982); United States v. Carpentier, 689 F.2d 21 (2d Cir. 1982), cert. denied, 459 U.S. 1108 (1983); United States v. Jannotti, 673 F.2d 578 (3d Cir.), cert. denied, 457 U.S. 1106 (1982); United States v. Myers, 692 F.2d 823 (2d Cir. 1982), cert. denied, 461 U.S. 961 (1983); Hughes v. United States, 701 F.2d 56 (7th Cir.), aff'g. 534 F. Supp. 352 (N.D. Ill. 1982); United States v. Criden, 633 F.2d 346 (3d Cir. 1980), cert. denied, 449 U.S. 1113 (1981); United States v. Murphy, 642 F.2d 699 (2d Cir. 1980); United States v. Myers, 635 F.2d 932 (2d Cir.), cert. denied, 449 U.S. 956 (1980); United States v. Jenrette, 594 F. Supp. 769 (D.D.C. 1983), aff'd, 744 F.2d 817 (D.C. Cir. 1984); Hughes v. United States, 534 F. Supp. 352 (N.D. Ill.), aff'd, 701 F.2d 56 (7th Cir. 1982); United States v. Jannotti, 501 F. Supp. 1182 (E.D. Pa. 1980), rev'd, 673 F.2d 578 (3d Cir.), cert. denied, 457 U.S. 1106 (1982).

Again, my special assistants and I evaluate the proposal. Once I approve it, I send it to the Justice Department for approval by the Attorney General. Finally, the application is reviewed by the FISA court.

the informant, often with a criminal background, was sometimes not sufficiently disciplined or trustworthy to carry out the demanding responsibilities required by an investigation. Often they had to be entrusted with large sums of money. In addition, there was the problem of establishing, for a jury, the credibility of someone who had made a deal with the government in return for his cooperation and testimony.

On the other hand, we believe our special agents are more trustworthy, more disciplined, and more sensitive to individual rights. We train them to understand and respect the law's requirements. The bottom line for successful undercover work is control, discipline and staying power—the ability to remain in the operation until all the evidence has been developed. We use the informant or cooperating witness to vouch for the undercover agent and give us an entry. But as soon as possible, we ease the cooperating witness out of the picture, using him less and less and our agent more and more.

Although we currently budget less than one percent of our field resources to undercover work and use undercover agents only when traditional methods have been unsuccessful, they are extraordinarily costeffective. During fiscal year 1984, investigations using this technique produced nearly 1,200 arrests, almost 1,000 convictions, more than \$100 million in recoveries and fines of almost \$3 million.

A recent Miami case is a good example of how these undercover operations frequently develop. In that case, a cooperating witness came to us after some people interested in overthrowing the Honduran government approached him to hire a hit man to assassinate President Roberto Suazo. We arranged for the cooperating witness to introduce an undercover agent to the group. The plotters struck a deal with our agent and agreed to pay him \$300,000 for the assassination.

During our investigation, we found out that some members of the group were also involved in drug trafficking and they invited our undercover agent into a previously arranged drug deal. We brought down the operation by arresting eight of the plotters. We have requested extradition of the ninth conspirator, a general assigned to the Honduran embassy in Santiago, Chile. In addition to preventing the assassination of President Suazo, we seized a twin-engine airplane, two small jet airplanes, a 158-foot freighter converted to carry marijuana, and 345 kilos of cocaine valued at more than 10 million dollars.

The length, complexity and sensitive nature of undercover projects call for very careful planning and control. The review process originates in the field when we try different ways of getting at a crime problem. We know the problem is there, but sometimes we can not develop sufficient admissible evidence. Our field office managers develop a scenario to use an undercover agent. The special agent in charge of the field office and the local United States Attorney's office review and approve the scenario. The proposal is then submitted to headquarters where it is reviewed by what we call the "substantive desk," the particular program management area for that specific crime.

If the proposal fails to survive this scrutiny, it goes back for reform or is rejected outright. If it passes the substantive desk, it is reviewed by our Undercover and Special Operations Unit, which is concerned with the payment of money, the utilization of equipment and other things unique to undercover work. And then it goes on to our most important institutional group, which I established in late 1978, the Criminal Undercover Operations Review Committee. This committee consists of representatives of key divisions within headquarters-again, those who have to pay the money, develop the sensitive technical equipment and bear personal responsibility for the investigations. The committee also includes representatives from the Legal Counsel Division, one of my special assistants and four representatives from the Department of Justice. This group reviews the proposal in terms of its legality, practicality and appropriateness. I review the minutes of the committee's deliberations to monitor their actions. If the committee approves of the proposal, they make a recommendation to the head of our Criminal Investigative Division, or in particularly sensitive circumstances, to me. No operation is approved for more than six months and extensions are granted only after committee review.13

Legal issues are very carefully considered. The issue of entrapment comes up in every undercover case. It will be a defense argued at the beginning; it will be a defense argued at trial; it will be a defense argued

<sup>13.</sup> Occasionally, the committee will reject a proposal or require the submitting field office to redesign it because of some flaw. For example, a field office recently made a proposal to investigate "chop shops"—auto wrecking yards handling stolen auto parts. The proposal involved an undercover operation in which our agents would set up a chop shop and then contact thieves to obtain the parts requested by body shops.

When the committee reviewed this proposal, we found some significant problems. Our first concern was the risk of civil liability and loss to an innocent party if our request for parts resulted in the theft of someone's vehicle. Our second worry was that personal property left in a stolen vehicle would be kept or sold by the thieves. Finally, we were concerned that someone would be injured or perhaps killed during an auto theft. Because of these concerns, the committee would not approve the proposal in this form.

on appeal. I can think of only one case in my seven years when such a defense may have prevailed.

We have an equal concern for possible harm to third parties. Sometimes, in spite of our best efforts to avoid it, third parties have sustained losses. We are working with the Department of Justice on some legislative proposals that will provide financial protection for innocent people who may have been harmed unintentionally by our undercover operations. But that legislation will not mean relaxed vigilance on our part. We will continue to weed out those proposals that run excessive risk of injuring innocent parties.

Once in place, we monitor undercover operations closely to ensure compliance with the Attorney General's legal requirements and guidelines. For example, federal prosecutors in New York and Justice Department attorneys in Washington reviewed the ABSCAM case on a daily basis and made recommendations on numerous investigative steps. Prosecutors personally monitored, on closed-circuit television, many of the transactions as they took place. One purpose for this on-line monitoring was to guard against conduct amounting to entrapment. The attorneys could pick up a telephone and call into the meeting room. The undercover agent would answer as if he was receiving a business call and obtain instructions necessary to ensure that we were following all legal requirements.<sup>14</sup> The procedures worked well, as we were successful in every appeal taken in the ABSCAM cases.

We cannot anticipate and avoid every conceivable problem in a scenario in which only some of the players have the script, but we make every effort to do so and to build upon our past experience. That is the purpose of the Review Committee: to build institutional awareness.

Supreme Court Justice Robert Jackson once observed that the Consti-

<sup>14.</sup> The conclusion of an undercover operation signals the beginning of the final phase of fairness evaluation. This retrospective assessment starts in the courts, where judges or juries must ultimately rule on the defense of entrapment or denial of due process. We are keen observers of this evaluation phase, for it is here that we find out how successful we have been in trying to ensure fairness. If the court finds that our agents induced an otherwise innocent individual to commit a crime, we will carefully reexamine the case to find where our controls broke down. And in future investigations involving similar scenarios, we will take additional steps to guarantee the standard of fairness. This retrospective assessment does not stop with the trial courts or even with the appellate courts. It may include a review of our entire undercover program by congressional committees and subcommittees. For example, the ABSCAM cases resulted in considerable congressional review. We welcome these reexaminations by Congress because we know that ultimately we must answer to the American people.

tutional Bill of Rights of the United States was not a suicide pact.<sup>15</sup> The protections it includes and affords to us must be rationally applied if we are to prevail against those in our midst who daily frustrate through violence and lawlessness the liberties our Constitution was designed to secure. To this degree the police power of the state is allowed to function through lawful, if occasionally intrusive, techniques; through statutes, guidelines, rules and regulations appropriately adopted; through law enforcement officers trained to know and respect these requirements; through executive, legislative and judicial oversight of the process; and through ultimate public accountability. To this degree our modern investigative weapons can protect us from the power and viciousness of otherwise unchecked criminality. Unless the technique is illegal per se or so contrary to public policy as to be unworthy of use, we should rely upon appropriate management of the technique to serve the ends of justice rather than lose its great value for fear of its possible abuse.

In the FBI, these safeguards are in place. We realize that the law enforcement officer is the port of entry to the criminal justice system. If we fail in our duty to be both effective and fair, no prosecutor or judge can save the case, so we must not fail. We must preserve both the appearance and reality of fairness that Lincoln thought was the most important aspect of our legal system.

This is what the American people expect of us; this is what the Constitution demands of us.

<sup>15.</sup> Terminiello v. Chicago, 337 U.S. 1, 37 (1949).