5
Law Enforcement

The Function of Law Enforcement: Solution versus Prevention

The purpose of law enforcement is to prevent, interdict, and investigate crimes and to prosecute criminals. There is a certain logic to the order in which these objectives are presented; it goes from the most anticipatory to the most reactive. The closest relationship is between investigation and prosecution, which are by and large the most visible and best known of law enforcement's functions. We will examine these first, then turn to prevention, of which a major component, deterrence, is closely related to the success of investigation and prosecution. Finally we will examine interdiction, which is the area that most often brings law enforcement into conflict with civil liberties.

If asked to name a crime, most people would pick a typical crime: murder or robbery or rape or fraud. Everybody agrees that these are crimes (although there is often disagreement about whether a particular event is an instance of the crime), and they are crimes in which the victims are identifiable. Except (of course) in the case of murder, police generally begin their investigation by questioning the victim to get a description of what has happened and to get "leads."

The investigation of crimes has not changed since the rise of the police in the mid nineteenth century, but the way in which they go about it has changed a great deal.

In the nineteenth century, police work was largely a matter of interpersonal relations. The policeman walking a beat depended as much on

rapport with the people of the neighborhood as on a gun or a nightstick. In the absence of a radio or even a call box, he did not have the option —the first resort of police today—of communicating with the station before taking action of any kind. If he encountered trouble, his choices were to deal with it himself or to turn and go for help. The actions of the police in investigating crimes reflected the same skills and resources they used on patrol. They relied less on forensic evidence, record keeping, and communications and more on talking to people and knowing the community. Police action after a crime would rely heavily on an expertise in community functioning acquired continually as the police developed informants or kept watch on markets known to include stolen goods among their wares.

Since then, the character of policing has changed dramatically, and today the police depend as heavily on technology as on their skill in dealing with people. Nowhere is this more apparent than in detective work. The invasion of technology began around 1900 with the development of fingerprinting[1] and forensics. Forensics, as popularized in the Sherlock Holmes stories, has become a mainstay of detective work, and today crime laboratories maintain vast files of common items (such as paper, automobile paint, and duct tape) that enable them to identify and track these items when they are found at crime scenes (Fisher 1995, pp. 159–193).

When police investigate the scene of a crime today, their first action is to seal off the scene and take numerous samples—fingerprints, cartridge cases, clothing fibers, traces of DNA, and so on. In conjunction with the lab analysis of these samples, they will make extensive use of their records on people (suspects or witnesses) and on cars, guns, jewelry, and other objects that may have been involved.

The act of investigating a crime consists most conspicuously of attempting to discover who committed the crime, but it may also involve determining the nature and extent of the crime and whether there was a crime committed at all. If this process is successful, the next step is prosecution. Once a suspect has been identified, the police must supply the state's attorney with sufficient evidence to prove the suspect's guilt. Sometimes this process is barely distinguishable from investigation. The police may, for example, observe a suspect's movements until they have

a persuasive case that he was in a position to commit the crime and was the only person in such a position. In other cases, particularly in crimes such as burglary or fraud that are likely to be repeated, the process of developing evidence takes on a life of its own and looks quite different. The police may watch someone, whom they suspect of committing a crime but against whom they lack sufficient proof, in hopes that the suspect will grant a repeat performance. They may go so far as to create attractive conditions for the commission of the crime and lie in wait for the suspect to take the bait.

The prevention of criminal activity relies on a combination of security and deterrence. Security measures, ranging from locks and fences to surveillance cameras and patrols, make it more difficult to get away with crimes. Deterrence is in part a result of security and in part a result of the investigation and prosecution of crimes. It persuades a would-be criminal that even success in committing a crime will not mean he has gotten away with it. Security and deterrence are not always easy to distinguish. Police walking beats or patrolling in cars convey the impression that a crime might be observed and stopped outright; they also serve to remind the citizens that the police are present and are likely to find and prosecute the perpetrators of crimes.

The important factor unifying security and deterrence is that neither is aimed at particular individuals. Both are intended to prevent the commission of crimes—to communicate to everyone that criminal efforts are unlikely to succeed and likely to be discovered and punished.

Interdiction of crimes has a different flavor. It is aimed not at everyone, but at particular people who have been detected in the process of planning or preparing to commit criminal acts. Unlike deterrence, it involves concentration of police attention and possibly police action on people who have yet to commit any crime. Any police program of interdiction must, therefore, involve watching people who, at least under US law, are entitled to a presumption of innocence.

A Brief History of the Police

The police as we know them today—an armed force maintained by the state to perform the functions described in the previous section and paid

a salary rather than a share of fines[2]—are a rather recent phenomenon. Police appeared in France as one of the products of the revolution, but police in the United States stem more from the British tradition.

In 1829, Home Secretary Robert Peele established the Metropolitan Police in London. Initially this force was limited to uniformed patrolling, but in 1842 it was expanded to include the Criminal Investigation Division, responsible for detective work. London's salaried force became the organizational model for police throughout Britain and subsequently the United States. Police forces were formed in all major US cities during the latter half of the nineteenth century.

At the time of their founding, the fundamental mandate of the police was a combination of deterrence (through their visible presence on patrol) and investigation. Under earlier British law, there was less provision than there is today for discovering the perpetrators of a crime when their identities were not obvious; it was the responsibility of the injured parties to investigate and "solve" the crime. Over time, however, investigating and solving crimes has evolved into one of the most important functions of the police.

At the time of their founding, the police were viewed not as an outgrowth of the state's ability to make law but as a manifestation of its ability to use violence. As time went by, they gradually became essentially the only body entitled to employ violence in anything other than self-defense and narrowly construed instances of defense of property. They also came to be seen as the lower rungs of a ladder whose upper steps are the prosecutors and the courts.

In the original British conception, police powers of arrest were limited, and police were supposed to have little or no influence in whether cases were brought to trial. Over time, however, the influence of the police over such decisions has increased dramatically,[3] as has their influence over the making of laws.[4]

The Use of Wiretaps in Law Enforcement

Both before and after the development of telecommunication, a central element of police work has been the acquisition of information about

criminals' plans and conversations without their knowledge or cooperation. There are two fundamental ways in which this can take place:

- through conversations in which a criminal is talking to someone who, usually unbeknownst to the criminal, is an undercover police officer or is providing information to the police
- through conversations between criminals being overheard by the police or by their agents.

The development of telecommunication has had an impact on both of these scenarios, but it has affected the latter far more than the former.

Our first scenario occurs widely in traditional police work—for example, when a victim of extortion or blackmail relates the threats he or she has received to the police, or when the police employ a stool pigeon. Telecommunication has left many of these practices unaffected while opening new opportunities for others. Demands by kidnappers and blackmailers are often delivered by phone and may readily be taped at the victim's end for use as evidence or for other investigative purposes. Such taping, legally and practically distinct from a wiretap, is called a *consensual overhear*.

Our second scenario is the home territory of electronic surveillance.

The crimes we have called typical are investigated largely at the interface between the criminal and non-criminal worlds. But neither the typical crimes nor the broader class of acts generally accepted as crimes and having identifiable victims exhaust the criminal repertoire. Many activities that are criminal under law do not have readily identifiable victims. Not coincidentally, the criminal status of such activities—which include such classic activities of organized crime as prostitution, gambling, and drugs—is often controversial.

Under these circumstances, the police cannot proceed from questioning an aggrieved victim to investigating and prosecuting an offender. They must instead attempt to infiltrate the criminal activity—to intrude on the interactions of a group of people who are, by and large, either satisfied purveyors or satisfied customers in the illegal trade.

For many crimes, including conspiracies to fix prices, bribe government officials, or commit terrorist acts, such infiltration is a difficult procedure.

The participants are wary of newcomers, and normal routes of investigation are sealed; it may even be hard to determine what crimes are occurring. It is in such environments that electronic surveillance comes into its own, providing information about the crime being committed and insight into the structure of the criminal organization.

Rarely is it possible to develop or plant an informer high in a syndicate. Information from surveillance enables law enforcement to develop a coherent view of a conspiracy. In the Illwind investigation of corruption in the procurement of weapons for the US military, FBI agents were afraid to run credit checks on suspects for fear of alerting them. Instead they used wiretaps and electronic bugs (which were even more productive) to assemble a picture of the conspiracy. Hundreds of agents were involved in the surveillance (Pasztor 1995, pp. 190–191). Wiretaps can also provide mundane details—the suspect's daily schedule (Weiner et al. 1995, p. 223), or the personal relationship between the suspect and his coconspirators—that can vastly simplify an investigation.

Though equivalent to electronic bugs from a legal viewpoint, wiretaps are generally easier and less dangerous to install. They usually do not provide the same quality of information, however. Criminals are typically considerably less forthcoming over wiretapped telephones than in bugged rooms.[5] Microphone rather than wiretap evidence was responsible for convicting John Gotti, head of the Gambino crime syndicate; information obtained by means of a bug in a Gotti hideaway convinced underboss Sammy Gravano to testify against Gotti.[6] Electronic bugs were also responsible for the conviction of John Stanfa, a Philadelphia crime boss (Anastasia 1994; Hinds 1994).

Even when wiretaps do not directly provide evidence, they can be useful. Wiretaps informed US agents about meetings between the spy Aldrich Ames and his Soviet handlers (Weiner et al. 1995, p. 246).[7] Wiretaps also apprised agents of the fact that Ames's wife had aided him in his illegal activities. Investigators used this knowledge to extract a more detailed confession from Ames in exchange for a reduced sentence for his wife (ibid., pp. 261–262 and 288).

In general, wiretaps appear to be of greater value in gathering intelligence than in developing evidence. They can expose the connections

within an organization, and they may reveal events before they occur. Not to be undervalued is the fact that knowledge of the possibility of wiretapping renders the telephone far less useful to criminals.

Wiretaps and Their Relatives

How Wiretaps Work

Words spoken into a telephone begin their journey at the microphone of the handset, which may be connected to the phone by wire or (in the case of a cordless phone) by radio. From the phone, the signal is passed down a line cord to a wall socket. If the phone is in an office building, its next stop is typically a phone closet where the wires from many phones on the same floor come together. If the phone is in a private home, the signal generally goes directly to a junction box on an outside wall and then by wire to a pole; it is likely to run on poles for only a short distance before it joins wires from other houses in a junction box (similar to the office phone closet) and is routed underground. At this point, the signal takes a fairly long hop and makes its way to the local telephone exchange, where it is received on a frame.

By comparison with the previous elements, the frame plays a more profound role in the call's progress. Up to that point, phone lines were arranged in a basically geographical way, lines coming from nearby houses being routed close together. The frame rearranges the lines to put them in numerical order by phone number. From the frame the lines go into a telephone switch, the formerly mechanical and now electrical equipment that routes calls from one telephone to another. From this point on, no path is permanently bound to any particular phone.

From the viewpoint of security, a phone call is vulnerable to wiretapping at every point along its path. A wiretap may be placed in or close to the phone.[8] It may be placed in a phone closet or in a junction box. It may be placed on the frame or inside the telephone switch. From the viewpoint of an intruder, however, things look entirely different and each of the possible opportunities for wiretapping has serious disadvantages.[9] If he tries to put the tap in the phone, he may get caught in the act of planting the device.[10]

Tapping intermediate junction boxes, whether in phone closets, on poles, or elsewhere, presents both the danger that the installation will be observed and the danger that the tap will later be found by maintenance personnel. Precisely because a junction box serves a number of different clients, it is subject to unpredictable visits by installers and repairmen connecting, disconnecting, or troubleshooting the phones of subscribers other than the target. Any of these maintenance personnel may mistake the tap for a wiring error and disconnect it or take some action that will reveal the tap to its target.

One traditional point for attaching wiretaps was the frame, where an incoming line can readily be connected to an outgoing one in such a way as to make the call accessible at an additional external location. Occasionally this is done for quality-control purposes in the normal course of telephone operations. Like a junction box, however, a frame is tended by numerous people from whom the tappers are trying to keep the tap concealed.

Until the advent of digital telephone switches, the phone, the junction boxes, and the frame were essentially the only points at which a tap targeting an individual line could be placed. It was within the ability of intelligence agencies to target multiplexed flows of traffic further removed from the targets, but only because they had both the budget and the legal mandate to listen to whatever they could find that was of value. Police wiretapping, by comparison, was targeted at individuals and had to be conducted on a limited budget with limited cooperation from the telephone companies.

Digital telephone switches, such as AT&T's ESS series and Northern Telecom's DMS-100, introduce a new (and, from the police viewpoint, far superior) way of wiretapping. The new technique is to make use of the switch's ability to create conference calls. (A tapped call is, after all, simply a conference call with a silent and invisible third party.) Conference calling, however, was not designed with the wiretapper in mind. The technology was intended primarily for creating conference calls in which all connected phones were active and cooperating participants. The new switches had secondary applications to debugging and quality-control monitoring that were closer to the tapper's desires, but a switch's capacity to provide these services was typically limited to a few lines at

a time. Although this was generally sufficient for law-enforcement use in the past, law-enforcement agencies have recently begun pushing for vastly expanded wiretapping facilities.

Pen Register and Trap and Trace

As we noted in the previous chapter, the backbone of a communications intelligence organization is not its ability to read individual messages, valuable as that is, but its ability to keep track of a broad spectrum of communications through traffic analysis. Although this is less true of law-enforcement intercepts, a sort of traffic analysis, generally targeted at individual lines, plays an important role here.

A log of the numbers of all phones called by one particular phone is called a *pen register*.[11] In the United States the ability to record called numbers has been an essential component of billing for a long time and thus has been built into telephone equipment for a long time.[12] Call logging can also be carried out by equipment on a subscriber's premises (Jupp 1989).

The inverse activity—taking note of the numbers of all phones that call a particular phone—is called *trap and trace*. Unlike logging the numbers of outgoing calls, this was very difficult before the changes made during the past two decades in telephone signaling.[13] In the era of electromechanical telephone switching, call tracing took many minutes, during which the caller had to be kept on the line.[14] With digital switching, however, tracing information is almost always available until at least the last switch through which the call passes, and it is often available to the receiving telephone in the form of Caller ID.[15]

As in intelligence work, analysis of the patterns of telephone calls can reveal the structures of organizations and the movements of people. Where billing records preserve such information, it can be employed after the fact, even though the need to do so was not anticipated.[16]

Electronic Surveillance in Context

To be understood correctly, electronic surveillance must be seen in the context of the use of technology by police.

Police have often been at the forefront of the use of new technologies.

Scotland Yard was connected to the district police stations of London by telegraph in 1849, only 5 years after the telegraph was invented. In 1878 the Chicago police introduced telephone boxes along policemen's routes. "Wirephoto," credited with the capture of a criminal as early as 1908, became widespread after World War I.

Some elements of today's police technology are entirely new; others have clearly recognizable roots but have changed so much that they are only barely recognizable in relation to their ancestral forms. The most basic of these are the technologies that shape the operations of a police organization: record keeping and what we will call by the military term "command and control."

Police records serve both a strategic and a tactical function. Strategically, they allow police to decide how to deploy their forces. Tactically, they provide information on persons, property, and events connected with the investigation of individual crimes. Police records were once local to cities or districts, and sharing of information between police was a slow, uncertain process. Today, however, a computerized National Crime Information Center provides information to federal, state, and local police forces throughout the United States. This source of information is augmented by police access to commercial credit databases, national telephone directories, and other online information services.

The utility of records is closely connected to another mainstay of police technology: communications. Today most on-duty officers, whether patrolling in cars or walking beats, are in immediate radio contact with their stations. Police cars in some cities carry data terminals that allow direct access to printed records; in other places, officers on patrol must make voice contact with a dispatcher who has access to databases. Police forces today not only have access to nationwide (and often worldwide) records, but much of that access is directly available to officers in the field.

Radio communication also gives the dispatcher immediate access to officers on patrol. To utilize this effectively, the dispatcher must have information about where the officers are and what they are doing. At regular intervals, officers report their locations and activities, and the information they provide is entered on maps and status boards. In the most advanced setups, tracking systems such as Teletrack automatically

report the location of each patrol car and display it on the dispatcher's map. Coupled with databases of locations developed to support the 911 emergency system,[17] this permits the dispatcher to recognize where a telephone call is coming from and identify the nearest available emergency personnel. Within a patrol car, it may provide automatic directions to the place the car has been told to go.

The same technologies that permit police forces to track their officers permit them to track and watch individuals and goods with unprecedented ease. Many truck, bus, and automobile fleets use tracking systems to monitor the movements of their vehicles. This allows vehicles to be tracked if they are stolen and makes it difficult for the drivers to use them for purposes other than those the employer intended. Surveillance is also facilitated by computerized road tolls, optical character recognition of license plates, and specialized networks for tracking "bumper-bugged" vehicles (Burnham 1996, p. 138).

Police track more than vehicles. It is a rare person in the modern world who can avoid being listed in numerous databases. From a police viewpoint, the process of identification is a process of matching a person with society's records about that person.[18] Until recently, fingerprints were of more use in confirming identity than establishing it. Even long after the availability of computers, the search of a large fingerprint file was a slow process requiring expert human labor.

Even though fingerprint records have been computerized, fingerprints are not an ideal way of tracking the movements of people, and they are rapidly being supplanted or augmented by other technologies.

Video cameras are now ubiquitous. It is popularly believed that such cameras run "tape loops" containing, for example, the last half-hour's view of people entering and leaving a bank. In fact, videotape is cheap, and many cameras record images for much longer periods. After the bombing of the Murrah federal building, the FBI collected videotapes from all over Oklahoma City, synchronized them using the shaking that resulted from the blast, and watched the movements of people before and after the explosion.[19] One developing technology allows automatic identification of people from their videotaped images (Busey 1994). Another new form of technology that allows "surreptitious fingerprinting" is infrared imaging of the veins in the face. Like fingerprints, these are

unique to individuals. Unlike fingerprints, these veins can be detected by hidden infrared cameras installed in airports and other public places.

Today almost every American adult carries a driver's license[20] and other forms of identification that are hard—and illegal—to counterfeit. The near ubiquity of identification cards has given them wide social acceptability. Many communities require hotel registrants to show identification, presumably as an anti-prostitution measure. The 1995 decision by the Federal Aviation Authority that air travelers could be required to show government-issued identification when checking in at airports and more drastic post-9/11 security measures have made anonymity impossible for law-abiding travelers. The Supreme Court ruling that the police cannot require a person to show identification (*Kolender, Chief of Police of San Diego, et al. v. Lawson* 461 US 352 (1983)) has brought no noticeable change in police practice.

Possibly the most important way of tracking individuals is through credit cards. Since credit cards are the easiest way of making most purchases and are essentially required of persons renting cars or checking into hotels, the databases used for billing and credit verification contain good pictures of most people's movements.

Material objects too are tracked; they are also examined. Fear of terrorism initiated the development of a broad range of devices intended to search for guns and bombs. The capabilities of the most recent equipment go far beyond that, however. Some baggage x-ray machines can be programmed to look for sharp things, for guns, for drugs, for precious metals, or for fruits and vegetables. Similar devices can look at an entire truck and detect drugs right through its aluminum skin. There are detectors based on magnetometry, on vapor analysis, on neutron activation analysis, and on nuclear magnetic resonance. Detection of mass concentrations from their gravitational effects is in an experimental stage.

Evaluating the numerous technologies that have appeared over the past 100 years for their law-enforcement potential versus their criminal potential produces a preponderance of cases that favor law enforcement. On the criminal side, chemistry has given us a variety of new drugs that have been condemned by society but enjoy good sales anyway. Improvements in manufacturing and competition in the international arms market have given us "Saturday night specials." Photography has con-

tributed to blackmail. Computers and communications have brought us a new kind of crime—theft of computer and communication services—even while contributing to the operations of both criminals and police. It is hard to see much that microscopy, x-rays, database technology, microbiology, infrared imaging, MRI, or numerous other technologies have contributed to criminal enterprises; they have, however, given the police a host of techniques for tracking, identifying, and monitoring both people and physical objects. On balance, the impact of technology is so weighted on the side of law enforcement as to make it remarkable that crime has survived at all.

Blurring the National Security/Law Enforcement Distinction

In general, "national security" refers to the government's operations outside the borders of the United States and "law enforcement" to its domestic operations. However, at times—most dramatically in the 1960s and the early 1970s—the distinction has been blurred.

In the mid 1970s, the Church Committee, a year-long Senate investigation of US intelligence operations, found evidence of "domestic intelligence activities [that] threaten to undermine our democratic society and fundamentally alter its nature" (USS 94d, p. 1). The Church Committee recommended that the CIA, NSA, the Defense Intelligence Agency, and the armed services be precluded, with narrow and specific exceptions, from conducting intelligence activities within the United States, and that their activities abroad be controlled so as to minimize impact on the rights of Americans (ibid., p. 297). Out of the Church Committee report grew a sharp delineation between laws governing (domestic) law-enforcement investigations and those governing (foreign) national-security ones. National-security investigators were allowed to operate with considerably more latitude outside the borders of the United States than within. This sharp delineation was in line with the 1878 Posse Comitatus Act, post-Civil War legislation that prohibited Army involvement in domestic arrests or searches and seizures.[21]

Within a decade of the Church Committee's recommendation, the line began to blur. In 1981 President Ronald Reagan declared that international drug trafficking posed a threat to national security (McGee 1996c),

and the Military Cooperation with Civilian Law Enforcement Agencies Act sharply increased the Army's role in anti-drug efforts. The military's responsibilities in anti-drug efforts grew. The 1989 Defense Authorization Act put the Department of Defense in charge of applying US command, control, communications, and intelligence assets to monitor illegal drugs.

The National Guard does not face Posse Comitatus restrictions unless it is on federal duty, and it has been given a greater role in drug interdiction. In addition, Army Special Forces and the Marines patrol the Southwest and California for drug smugglers. Military intelligence officers also watch for gang and criminal activity in a number of US cities (McGee 1996b,c). Law enforcement and the military have become closely linked in their anti-drug activities. The scale of military participation is evident in the fact that since 1989 the military has spent over $7 billion on anti-drug operations (McGee 1996b).

Aside from drug trafficking, various international events have been cited as evidence of a need for closer coordination between national security and domestic law enforcement. One such event was the 1991 collapse of the Bank of Credit and Commerce International. According to a 1992 report by Senators John Kerry and Hank Brown, the CIA had discovered the essentials of the bank's criminal activities by 1985 but had never properly conveyed these facts to law-enforcement agencies.[22] Proponents of closer cooperation between intelligence and law-enforcement agencies maintain that globalization and the end of the Cold War make separation between national security and domestic law unrealistic.

A series of laws passed during the 1980s made various acts occurring outside the borders of the United States criminal acts prosecutable within the United States if they involved American citizens. These laws included the Omnibus Diplomatic Security and Antiterrorism Act of 1986 (Public Law 99-399), which established jurisdiction over violent terrorist acts against Americans overseas; the Act for the Prevention and Punishment of Hostage-Taking (18 USC §1203 (1988)); the Aircraft Sabotage Act (Public Law 98-473, 18 USC 63.2, 40 USC App. 1301, 1471 1972, (Supp. v. 1987)); and Public Law 101-519, which established US district court jurisdiction over suits to recover damages in international terrorism cases. The passage of these laws left unclear how they were to be

implemented, and, in particular, what role national security should play in international law enforcement.

The Clinton administration initiated internal discussions on these issues. Then the 1997 Intelligence Authorization Act (§814) stated the following:

> . . . elements of the Intelligence Community may, upon the request of a United States law enforcement agency collect information outside the United States about individuals who are not United States persons. Such elements may collect such information notwithstanding that the law enforcement agency intends to use the information collected for purposes of a law enforcement investigation or counterintelligence investigation.

This wording carefully steers clear of permitting the intelligence community to spy on Americans directly, but opens the way for unprecedented collaboration between the intelligence and law-enforcement communities. Since 9/11, however, the wall between intelligence and law enforcement has been eroded and cooperation between intelligence and law enforcement has been expanded on many fronts. This is discussed further in chapter 11.

It has long been recognized that agents of foreign powers—we used to talk about spies, now we talk about terrorists—may commit crimes in the US but do not behave like ordinary criminals and are not readily controlled by ordinary law-enforcement activities. To start with, they often have the support of foreign intelligence or covert operations services that provide them with equipment, training, or information not available to common criminals. Not only may they be provided with money, expertly forged credentials, and weapons smuggled in in the diplomatic bag, they may be provided with intelligence about the actions of the law enforcement agencies that are pursuing them. More fundamentally, foreign agents are not part of American society and do not care about its censure. They may accept going to prison as a risk of the work or even look forward to prison as a badge of honor. In prison, they may act on training about how to behave as a prisoner, how to escape, how to continue to work for the home country, etc. Their spirits may be buoyed by the knowledge that they may be traded for American agents captured by their own side.

These considerations are considered adequate justification for special

laws dealing with agents of foreign powers and special agencies for carrying out those laws. In the United States the Foreign Intelligence Surveillance Act, the Classified Information Procedures Act, and more recently the USA PATRIOT Act have been passed with this in mind. Such laws diminish the presumption-of-innocence-based protection that the Constitution guarantees to ordinary citizens suspected of crimes and allow the government to act "more expediently," most particularly, in secret.

Unfortunately, there is an opposite side of this coin that generally faces down and goes unobserved. If the Constitution's guarantees of due process, presumption of innocence, and the right to be confronted by one's accusers are to be upheld, laws aimed at agents of foreign powers must be circumscribed so that they cannot be broadly applied. Unfortunately, this is not done as often as it should be and prosecutors dealing with ordinary criminal activities are quick to make use of the new "tools" to improve their conviction rates.