

Strengthening Law Enforcement Capabilities to Combat Terrorism

“We always have to be careful that the rights which America stands for are not sacrificed, but we also have to understand that in order for those rights to be enjoyed by citizens, the citizens have to be protected.”

Attorney General John Ashcroft, September 17, 2001

Ten days after the terrorist strikes on New York and Washington, Attorney General John Ashcroft and Federal Bureau of Investigation Director Robert Mueller toured the smoldering rubble where the Twin Towers once had stood. “It’s unspeakable,” the Attorney General kept repeating as he took in the horrible scene. Mueller walked with New York Governor George Pataki. “We’ll get them,” he said.

Mueller’s determination will be needed, as the dimensions of this task are daunting -- both the unraveling of the September 11 network, and the detection and elimination of other terrorist cells and plots that put U.S. interests and citizens at risk. Law enforcement agencies have felt beleaguered as global forces and new technologies erode their ability to maintain public safety. The revolution in information technology is the most salient of these forces, but other aspects of economic and political globalization have similar effects. International travel is fast and easy, allowing criminals and terrorists to move about the globe -- hidden among tens of thousands of immigrants, students, business travelers and tourists. Financial and trade networks have experienced a luxuriant proliferation, allowing money and goods to be transferred easily around the planet. Transnational “just-in-time” manufacturing processes have introduced an urgency in border. Military and advanced civil technologies are readily accessible in the global market place. When exploited in combination and with malevolent purpose, these trends -- as we have so painfully learned -- can endanger America’s safety.

Law enforcement as a counter-terrorism tool faces two major challenges: technological change and globalization. These affect national law enforcement across the board. Making law enforcement more effective in meeting these challenges requires taking advantage of new technologies, with adequate legal safeguards for civil liberties; and using globalization as a positive force to build better international law enforcement, through greater information sharing, coordination and cooperation. For the United States, a crucial part of responding to these two challenges will also be to reconsider the constraints placed on law enforcement and intelligence agencies as a result of the political turmoil of the 1970s. The concerns that prompted these constraints have not disappeared, but some limitations on police authorities and cooperation with intelligence agencies need to be reconsidered to better fit the security environment after September 11.

Technological Change and Increased Interception Capabilities

Communications interception, or wiretapping, has been a powerful tool in the law enforcement arsenal since the early 20th century. In the past, law enforcement could simply tap a fixed line to eavesdrop on communications -- but technological

developments from mobile phones to digital telephony have posed new and difficult challenges. In response, law enforcement has sought, with mixed success, to modify some technologies and restrict others. If we do not allow law enforcement agencies to adopt new technologies and procedures to match the changes in commercial communications, wiretap capabilities will continue to decline at the expense of public safety.

The principle challenge to wiretapping comes from the Internet. The Internet uses different communications technologies and protocols than the telephone system, and as more data and voice traffic migrate to the Internet, communications interception will be significantly reduced if law enforcement does not adopt technologies that allow for interception of Internet communications.

Before September 11, public debate focused on the FBI's Carnivore system, which can be installed at Internet service providers (ISP) to monitor Internet traffic (the system is used mainly with smaller ISPs, as large ISPs have proprietary software to perform the collection task). Once a warrant is obtained, e-mail traffic is examined automatically for messages from a suspect; if a message is found, it is saved for later law enforcement review.

Privacy advocates and some in industry opposed deployment of Carnivore as overly intrusive and are now concerned that the fear and anger generated by the terrorist attack will sweep away opposition to intrusive technologies such as Carnivore. These concerns were unreasonable even before September 11. Greater use of monitoring tools need not be a cause for concern if the appropriate legal safeguards, such as warrant requirements and judicial oversight, remain in place.

New anti-terrorism legislation (named "Uniting and Strengthening America Act by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001"), provides a broad range of new authorities, including an expansion of wiretapping and surveillance authorities. The Act, signed into law by the President on November 25th:

-- Establishes a nationwide order for pen register (recording telephone numbers dialed from a phone) and trap-and-trace (recording the numbers of incoming calls), permitting the interception of communications routed through any jurisdiction in the country. Previously, the law only allowed the placement of interception devices in the jurisdiction where the order is granted, and extends pen register and trap and trace authority to the address information in the headers of e-mails, which will provide some information about content and Web browsing by revealing website names;

-- Allows Internet Service Providers or other network administrators to authorize surveillance of "computer trespassers;"

-- Provides authority to compel disclosure of records in connection with an intelligence investigation;

-- Lets law enforcement authorities conduct wiretaps and secret searches in criminal cases under the standards previously applied to the purpose of collecting foreign intelligence, changes search warrant authorities to allow law enforcement agencies to search homes and offices without immediately notification of the owner and allows sharing information collected in the name of a grand jury with intelligence agencies.

These changes are reasonable adjustments to new technologies if judicial oversight is not diminished. They should probably be continued even after any "sunset clause" in the new law takes effect. Generally, those sections which respond to terrorism and which retain safeguards (especially judicial oversight) will be beneficial. Those sections of the bill which create new authorities for "national security" or which do not require judicial oversight are problematic. Indeed, these sections may actually work against adoption of technological fixes by calling into question whether safeguards are adequate.

Existing Supreme Court guidelines for wiretapping remain the best guide for any new measure. The requesting agency: (1) must show probable cause that a particular offense has been or is about to be committed; (2) must describe specifically the conversations to be intercepted; (3) surveillance must be for a specific, limited period of time; (4) there must be continuing probable cause for surveillance to continue beyond the original end date; (5) surveillance must end once the conversation sought is seized; (6) notice must be given unless there is an adequate showing of exigency; and (7) report back on the warrant so that courts can oversee and limit the use of the intercepted conversations.

An equally broad challenge to privacy will arise if the U.S. government begins to survey and correlate publicly available information. There are enormous volumes of data on American citizens and the activities of organizations and entities. One of the keys to future counterintelligence could be to do detailed mapping of suspect transactions that are identified through extensive data mining and correlation. It is unclear whether existing law governing surveillance applies when law enforcement authorities or intelligence agencies collect and compares such information. It would seem unavoidable, as public sources are rarely limited to foreigners only. Yet, it also would require going beyond current "minimization" rules. Congress and the Courts will need to explore this sensitive issue, and a reasonable solution found.

The lack of adequate privacy protections for Americans may inadvertently contribute to concerns over increased law enforcement capabilities. As technology reduces anonymity and privacy, Americans might be more comfortable if they knew that data from Internet IDs and surveillance devices like sensors and Global Positioning Systems were not being exploited for commercial purposes. Law enforcement must comply with legal constraints and judicial oversight in its use of intrusive technologies. The same constraints, however, do not apply to commercial use of the same technologies. Part of the price for employing more intrusive technologies for public safety might be to limit, through Federal legislation, the use of similar technologies for commercial purposes. This would make trade-offs between privacy and security more palatable.

The September 11 tragedy has rightly led the United States to reconsider the balance between law enforcement and new technologies, but restricting encryption -- technology that renders stored data and communications unreadable -- should not be among the options. Law enforcement officials, already concerned that the Internet and cellular telephony will degrade communications interception capabilities, fear that encryption compounds these challenges. The FBI (and NSA) fought for a decade to limit encryption's use and require that encryption products include a "backdoor" for law enforcement access. These U.S. proposals failed repeatedly because they were expensive and technically difficult to implement and had little public or allied support.

Without multilateral support from a broad range of countries, U.S. restrictions on encryption would not prevent terrorists from obtaining "unbreakable" products from other sources. Moreover, Al Qaeda has shown flexibility in adjusting its operations to avoid technology that has been compromised -- abandoning satellite phones, for example, when it discovered that the United States could listen to messages. We could expect a similar reaction to encryption restrictions, leaving little advantage against the terrorists but real costs for the United States. "Backdoors" and restrictions on the use of encryption will impose large costs for security and the economy, by making computer networks more vulnerable to cyberattacks. The benefit of widespread use of encryption outweighs the cost to law enforcement

Public Surveillance Technologies

Technological changes offer significant increases in the ability of police to monitor public activities. A number of cities already have deployed close circuit cameras and automated face-scanning systems to monitor public places. These systems, however, are relatively primitive, require expensive installations and suffer from an abundance of "false positives" and misidentifications when the system matches an image to a criminal identity in a database.

Improvements in surveillance will come as new technologies enter the market and are combined into new systems. Cheap, small, unobtrusive portable sensors will collect visual or infrared data. Among them will be disposable sensors, or tiny, coin-sized sensors capable of detecting movement or changes in light, and multispectral sensors, such as the infrared sensors now found in some cars for night driving. Wireless connectivity will let these sensors link to the Internet through the cellular telephone system, making them easy to deploy and mobile. Inexpensive Global Positioning System chips will make it easier to pinpoint the location of the sensors and their targets. Connection to the Internet will allow this sensor data to be matched against large, remotely located databases and analyzed automatically by powerful computing resources.

These "networked" recognition technologies already exist in prototype form, but improved wireless capabilities (which depend on the United States resolving bandwidth and radio spectrum allocation issues) and improved recognition software need to be developed before they can be widely deployed. In the interim, we will see the piecemeal use of surveillance systems using increasingly sophisticated sensors in specific locations

like airports or border crossing points. Using face-scanning systems in well-defined situations (as a mandatory part of the airline check-in process, for example) would overcome many of the shortcomings of today's technology. This system could be based on passport and visa photos (perhaps even drivers license photos). The courts have limited the ability of police to use sensors to look into houses, but appear to accept monitoring of public spaces. The basis for this distinction lies in the notion of a "reasonable expectation of privacy, and the 4th Amendment prohibition against "unreasonable search." It is hard to argue that there is a reasonable expectation of privacy in an airport or mall.

The benefits of such a system for airport security are unlikely to be challenged, but arguments will come as systems are deployed further afield and as they are combined with Global Positioning System (GPS) or biometric technologies that allow more precise identification and location of individuals. GPS signal processors will continue to shrink in size and cost. When these chips are built into cars, laptops and cell phones they will allow authorities to pinpoint location. The result will be a world where it is much more difficult to hide or be anonymous or lost.

Biometric technologies will link people's legal and physical identities, by using retinal scans, thumbprints or even voice scans to validate claims to an identity and allow access to systems. Stolen passports would be worthless if they were linked to a retinal scan or digital thumbprint. Multiple identities could be reduced if state and national biometric databases were linked so that part of the application process for a driver's license or passport involved collecting biometric data and checking to see if this data matched a previous application under a different name in a different state or a different country. The United States has already begun to incorporate biometric data into some immigration documents; this could usefully be extended to other forms of legal identification. For biometric technologies to reach their true potential, however, the information they collect must be integrated with the national indices system, the watch lists, and other essential databases. This will require an enormous effort to automate, update and continually evaluate acquired data.

These new technologies offer improved counterterrorist capabilities, but pose difficult legal problems in protecting against misuse. Our legal system has not sorted out the line between private and public for these technologies. The issue lies in defining when law enforcement should collect such data and how that data should be treated (i.e. storage, sharing, application). Congress and the Courts have not dealt with this yet, although the laws governing search and seizure or wiretaps offer some precedent. European models of domestic security, where national identification cards and extensive national police powers are routine, do not fit well with America's Constitution and heritage; still, they reflect a long experience with terrorism. Some elements of the "European" approach to counterterrorism can be accommodated to Constitutional safeguards, but others require careful consideration.

International Cooperation

Localized law enforcement is at a disadvantage in an interconnected world. Law enforcement authorities are limited by jurisdiction – the geographical area to which authorities apply; and by sovereignty – the decision of a group of people to govern themselves, without external interference. No government is willing to let another police its citizens.

This is not an insoluble problem. All law enforcement agencies and all governments face the same challenges created by globalization and technological change. At some level, even political opponents are willing to cooperate on issues of law enforcement and public safety; this willingness has been increased (at least temporarily) by the events of September 11. Building cooperative arrangements among national law enforcement agencies that allow for coordinated activities and information sharing can help ensure the forces of globalization work for us, not against us.

The United States has made considerable strides in the last few years, but overcoming sensitivities over sovereignty issues and differences in national laws (even among the United States and its closest allies) will require compromise and delicate work. Domestic security poses a particular problem. France and the United Kingdom, for example, give their domestic security agencies greater authorities than does the United States, and these agencies face fewer legal restrictions in wiretapping, warrant requirements and in covert operations. This reflects our very different political cultures – the United States limits the power of the sovereign to a far greater degree than European governments. Major European governments have also faced violent domestic terrorism for a much longer period than the United States, and have already made political decisions regarding domestic security that the United States is only beginning to face.

While placing FBI attaches in key countries is an effective tool, much of international law enforcement cooperation is still rooted in the diplomacy of the mid-20th century. Most law enforcement cooperation rests on bilateral Mutual Legal Assistance Treaties. These treaties differ in scope from country to country. They are difficult to negotiate because they raise complex sovereignty issues, like the issue of law enforcement cooperation in general. September 11th's tragedy may offer the United States an opportunity to close some of this distance, both by strengthening existing MLATs and by seeking broader multilateral arrangements.

The most useful venue for multilateral cooperation has been the G-8, the seven leading industrial economies and Russia. Existing G-8 initiatives on counter-terrorism coordination and the Financial Action Task Force for money-laundering (which began in the G-7 but has now extended to two dozen countries) form a solid foundation for expanding cooperation in counterterrorism.¹

¹ FATF is an intergovernmental policy-making task force, created by the G-7 in 1989 in response to growing concern about money laundering. FATF is responsible for examining money laundering techniques and trends, reviewing national and international action and determining new money laundering measures. FATF's membership is two regional organizations -- the European Commission and the Gulf Cooperation Council -- and 29 countries and territories. FATF issued "The Forty Recommendations" in

Enhanced cooperation and information sharing in border control and immigration should complement these efforts. Immigration is among the most serious vulnerabilities revealed by September 11. The Al Qaeda cell responsible for the suicide-hijackings was recruited in the Middle East, organized in Afghanistan, and managed from Germany. Its members entered the United States from Canada and Europe, and did their final planning and deployment from Massachusetts and Virginia, passing undetected through at least three immigration checks. At first glance, this would seem to be a domestic issue, but treating it as a domestic issue will produce inadequate results. Border control is no longer entirely a national problem. The nature of borders has changed extensively in a global economy, and the first point of entry for many into the United States is Canada or Mexico.

Closing our borders is not an option – even the additional checks put in place after September 11 strain the economy. The United States could tighten its visa programs, but we need to recognize that this would contribute relatively little to enhanced security. Potential immigrants have spent years determining the best way to “game” the visa application process, and denying a U.S. visa does little if the option of illegal entry from Mexico or Canada remains open. Few terrorists fly directly to the United States from Afghanistan. Better border security requires both improved immigration procedures in the United States and improved cooperation with other countries in screening entrants.

Improved national immigration procedures have two elements. First, expanded screening at U.S. borders and entry points using information technologies, face scanning against visa and passport databases, biometrics and other detection systems (such as explosive sniffers) should be a priority. This will make future entries by terrorist more difficult (but not impossible). One unfortunate result of the relaxed immigration restrictions adopted by the United States over the last decade is that it is likely that members and supporters of Al Qaeda are legal residents. Solving this poses political questions that go beyond law enforcement. We do not want to restrict the flow of foreign visitors and student to the United States, but greater care is needed in extending the privileges of residency and citizenship to them.

The United States also needs to complement improved border controls with cooperative immigration efforts. Expanded cooperative immigration efforts among the United States and its allies and neighbours could borrow elements of the Schengen arrangement through which European countries share responsibility for screening foreigners entering Europe.² Schengen establishes common entry controls for its members, much the way

1990 to establish a global framework for money-laundering efforts. The Forty Recommendations are the leading international anti-money-laundering standard.

² The Schengen Agreement came into effect in 1995. It replaced the internal borders of the signatory states with a single external border, and created a single set of rules to govern immigration procedures -- as well as common rules on visas, asylum rights and checks at external borders. The goal was to enable the free movement of persons within the Schengen area without compromising law and order. Thus, the abolishing of internal borders was accompanied by so-called “compensatory” measures -- including improved coordination between the police, customs and the judiciary, and enhanced efforts to combat terrorism and

that a foreigner permitted to enter New York can travel to another state without further screening. The Schengen arrangement is not without flaws, but a similar approach to cooperation in screening entrants to the “West” is necessary.

A cooperative approach to entry would involve greater information sharing, but going beyond that to a degree of coordination poses political problems: Countries would have to agree to deny access to foreigners found undesirable by one, but not all. In the past, the United States has rankled Great Britain by allowing entry to IRA members, and Germany has permitted entry to members of terrorist-related groups objectionable to the United States. At a minimum, some sort of restricted entry and notification for individuals on a common control list could address this problem. Further steps would require a willingness to surrender sovereign authorities to some larger consensus.

Law Enforcement and Intelligence Cooperation

An effective response to terrorism will also require a reexamination of the boundary between law enforcement and intelligence. We need to find an approach that allows for effective cooperation between intelligence and law enforcement, but maintains their separate roles and responsibilities. The intelligence community has linguistic and analytical skills needed by national law enforcement agencies, and both intelligence and law enforcement communities have unique information that can benefit the mission of the other.

Designing this cooperation presents challenges for both civil liberties and organizational effectiveness. Law enforcement and intelligence operations are fundamentally different. Successful intelligence agencies routinely violate foreign laws. Effective intelligence operations carefully define and limit cooperation with foreign governments in ways contrary to normal law enforcement practices. Respect for due process is essential for law enforcement but not a part of successful intelligence activities. Information collected by law enforcement is ultimately destined for its public use in a trial, whereas the end use for intelligence information is usually a classified report. The more the intelligence function is like law enforcement, the less effective it will be; the more law enforcement operates like an intelligence agency, the greater the concern and the risk to fundamental civil liberties.

Much of the legal structure governing U.S. national law enforcement activities grew out of Watergate-era concerns that the executive branch was using national intelligence and law enforcement assets for domestic political ends. September 11 has led us to reopen the debate over police authorities in a civil state. The politicization of law enforcement in the last few years complicates this issue. Law enforcement at the national level has become a group with its own objectives and priorities, and a willingness to seek them. In classic bureaucratic fashion, it presses to expand its authorities and prerogatives. While

organized crime. At the heart of this effort is the Schengen Information System, through which member states’ police stations and consular officials can access and exchange data on specific individuals and descriptions of lost or stolen vehicles or objects.

this reflects larger trends in the bureaucratization of American government, where large Departments have developed rationales and political skills to operate with some independence from elected administrations, it also grows in part from the antagonistic nature of the U.S. legal system and a degree of alienation between police forces and the broader public.

The roots of this problem are complex. The system of federal government relies on the fragmentation of power. The Constitution divides authority among the Congress, the President and the Judiciary, and among the federal government and the states. This division is carried over into agency responsibilities. Fragmented authorities prevent the State from overwhelming democratic government. This approach has served the United States well in many instances, but as new technologies and global networks emerge, the cost of fragmented authorities may outweigh the benefit in some specific areas.

While cooperation with the intelligence community has improved dramatically in recent years -- with a jointly staffed Counter-Terrorism Center, the exchange of deputies, personnel assigned to each agency's counterterrorism groups, joint meetings, and joint operational and analytical initiatives -- bureaucratic competition and legal constraints have sometimes prevented crucial terrorism-related information from being shared in a timely and appropriate manner. Law enforcement and intelligence collection techniques are subject to differing legal authorities, which pose problems for information sharing. Distinguishing between collecting and sharing information can resolve some of these problems. For collection, we would want to preserve the distinction between the FBI and the intelligence community's authorities. The FBI should not engage in espionage and the intelligence community should not add criminal investigation to its list of collection priorities.

But while collection should remain separate, the United States should remove the barriers to sharing information that bear on criminal investigations or intelligence activities as they relate to terrorism. (Sharing intelligence that bears on other criminal activities is more a complex problem whose discussion can be separated from counterterrorism). Concern over misuse by the executive branch (or by Congressional leadership) is legitimate, but an artificial distinction for information sharing on international terrorism should be eliminated. In particular, the removal of limitations on sharing of information from guidelines for the Federal wiretap statute (Title III) or grand jury information will be beneficial for coordinated counter-terror efforts.

Yet, information sharing will not automatically spring up with the removal of the legal obstacles. The difficulties that law enforcement and intelligence agencies face in coordinating their operations run deeper than policy and procedure, into the very cores of these organizations. Similarly, the fundamental pattern of secrecy protection *within* the FBI -- a "case file" security approach -- is profoundly counterproductive to developing systematic, analytically based assessments of terrorist network activities. A strategy for promoting effective cooperation -- between agencies and within them -- must provide both the tools for cooperation and the operational conditions for their use.

Part of the new White House Homeland Security Office's task should be to build greater cooperation between intelligence and law enforcement agencies in well-defined circumstances (such as terrorism) and with the appropriate oversight. It should also consider creating a special "anti-terror" agency similar to the Drug Enforcement Agency -- a law enforcement agency with strong support from the intelligence community and military and with extensive international cooperation. While this would raise the same bureaucratic conflict that was engendered when the Drug Enforcement Agency was created, a dedicated agency with operational responsibility for Counterterrorism could be an attractive option.

Going Forward

The September 11 tragedy may shift the terms of the public debate for issues like privacy, Internet surveillance and even the allocation of radio spectrum. Security, law enforcement and homeland defense will be higher priorities than in the past. However, measures that seek to improve law enforcement capabilities by reversing technological change and resisting globalization could involve wrenching changes to the global economy and pose unacceptable risks of economic damage. We have seen "globalization" derailed before, by the First World War and the Great Depression. One of our goals should be denying Al Qaeda a similar outcome.

How then do we map a course for strengthening law enforcement to combat terror? There are concrete measures at the operational level, but the larger question for effective counterterrorism involves our response to technological change and globalization. As we seek to strengthen law enforcement in democratic societies, four questions should guide our review of any proposed measure:

- Is the measure a necessary response to the technological and global changes of the last decade to prevent the erosion of law enforcement capabilities?
- What is its effect on civil society and the economy?
- Can we take advantage of specific new technologies to make law enforcement more effective?
- Are the necessary legal safeguards and oversights in place to protect civil liberties and economic growth?

Law enforcement authorities are neither a panacea nor a substitute for a comprehensive strategy to eliminate terrorism. Increased police powers pose risks to the fabric of American economy and society. If we are cognizant of these risks and take the necessary steps to safeguard against them, greater international law enforcement cooperation, closer cooperation between law enforcement and intelligence in counter-terrorism, and new technologies that restore some law enforcement capabilities can only be beneficial.