21. Terrorism

Congress *should*

- repeal the Antiterrorism and Effective Death Penally Act of 1996,
- resist efforts to expand wiretapping,
- remove all export controls on encryption, and
- enact appropriations bills forbidding any executive branch official from spending money to promote the Clipper Chip.

From the Alien and Sedition Acts of 1798 to the Palmer Raids of 1919 to the McCarthy era to the present, proponents of restrictions on civil liberties have made exaggerated claims about various threats posed by American political dissidents and the necessity of a federal "crackdown." Indeed, proponents of a crackdown have often claimed that anyone who is skeptical of their exaggerated assertions must be sympathetic to the enemies of America.

Any violent crime is terrible, but terrorism is extremely rare in the United States. The risk that any given American will be killed by a terrorist is about the same as the chance that a randomly selected high school football player will one day be a starting quarterback in the Super Bowl. One's chance of being killed in a terrorist attack is many times less than one's chance of drowning in a bathtub or being killed by a fall from scaffolding or a ladder. We would not adopt the "if it saves one life" theory to justify a ban on bathtubs, even though hundreds of lives would be saved each year. Accordingly, America should reject terrorism legislation that will probably not save any lives and that demands that Americans give up things far more important than bathtubs.

Terrorists cannot destroy a free society, but they can scare a free society into destroying itself. In 1974 Irish Republican Army terrorists bombed pubs in Birmingham, England, killing 21 people. Home Secretary Roy

Jenkins introduced the Prevention of Terrorism (Temporary Provisions) Bill. Approved without objection in Parliament, the bill was supposed to expire in one year, but it has been renewed every year.

Under the Prevention of Terrorism Act, and subsequent British terrorism legislation, the police may stop and search without warrant any person suspected of terrorism. They may arrest any person they "reasonably suspect" "supports an illegal organization." An arrested person may be detained without court approval for up to a week. It is illegal even to organize a private or public meeting addressed by a member of a proscribed organization, or to wear clothes indicating support of such an organization.

In Britain wiretapping does not need judicial approval. If committed pursuant to an order from a secretary of state, acts such as theft, damage to property, arson, procuring information for blackmail, and leaving planted evidence are not crimes.

A suspect's decision to remain silent during interrogation may now be used against him in court. Although terrorism in Northern Ireland was the stated reason for the change, the change also applies in England and Wales. No one who has seen what is happening in Great Britain can feel confident that repressive measures introduced solely to counter terrorism will not eventually creep into the ordinary criminal justice system.

The Birmingham bombings that led to the Prevention of Terrorism Act resulted in the conviction of a group of defendants called the Birmingham Six, whose confessions were extracted under torture and who were convicted on what was later admitted to be the perjured testimony of a government forensic scientist. Eventually, they were freed, although if Britain had a death penalty, they would have been executed.

To state the obvious, all the repressive legislation has hardly immunized Britain from terrorism. To the contrary, British citizens are as vulnerable to an IRA car bomb as they were in 1974, and they are at much greater risk of being terrorized by the state itself. For centuries, "the rights of Englishmen" were proudly held up in contrast to the absolutism of the Continent. Far from being an exemplar to the world, the modern "anti-terrorist' ' United Kingdom has been found guilty of human rights violations under the European Convention on Human Rights more often than any other member of the Council of European States. As Britain's recent history illustrates, no matter how great a country's tradition of freedom, freedom can be lost in less than a generation if public officials, and the public, allow terrorism to destroy their traditional way of life.

To study the terrorism agenda being pushed in the United States these days is to study a series of assaults on the Bill of Rights. Despite the First

Amendment, some members of Congress have announced their dismay that explosives recipes (usually incomplete or otherwise erroneous) and other instructions for making products that are illegal without a special license can be found on the Internet. First of all, it is legal in the United States, and always has been, to publish information about how to make firearms, or explosives, or other weapons.

The fact that some such information is being distributed electronically, by phone lines, rather than in printed form by mail order, hardly changes its secure status within the protection of the First Amendment, any more than did the fact that *The Anarchist Cookbook* in the 1960s was printed with a high-speed modern printing press rather than a Franklin press. The government may not punish people for possessing knowledge or for reading about breaking the law. Indeed, a rule that outlaws speech because a criminal could learn something from it puts one on the way to banning crime novels and police training manuals, which, after all, contain detailed examples of how to commit various crimes.

Taggants

The main terrorism legislation threat to the Second Amendment is the Clinton administration's "taggants" proposal, under which literally millions of Americans would be classified as felons. A taggant is a chemical marker that can be placed in explosives. Even after the explosive is detonated, the taggant can identify the factory the explosive came from and perhaps the batch.

Whatever the possible value of taggants for commercial high explosives, taggants can be of no use for crimes involving black powder and smokeless powder. Those consumer products are sold in one- or five-pound bags. Smokeless powder and black powder are used in the home manufacture of ammunition (hand loading) by literally millions of families in the United States. Since one batch of factory powder may eventually be sold to tens of thousands of consumers, there is no realistic possibility that a taggant could lead to the solution of a crime. Instead, taggants legislation would create millions of crimes, since the Clinton proposal would criminalize the possession of black powder or smokeless powder without taggants, making the existing supplies of the millions of hand loaders a federal felony.

Taggants for gunpowder would have forensic value only if all powder purchases were registered and if each individual one-pound box of powder had its own individual taggant, a very expensive proposition. Even then, a person could obtain untagged powder by purchasing ammunition, disas-

sembling it, and removing the powder. Thus all ammunition purchases would have to be registered.

A study from the Office of Technology Assessment suggests that taggants could destabilize smokeless powder and black powder. Although Switzerland is frequently cited as a model for the use of taggants, that country does not require taggants in smokeless powder and black powder.

Finally, according to the Office of Technology Assessment, taggants are easy to remove from gunpowder by sifting, or by viewing the powder under black light and picking the taggants out with tweezers. Other taggants can be removed with a magnet. In short, taggants in gunpowder are a stalking-horse for ammunition registration, with no real crime-fighting value.

Wiretapping

The Fourth Amendment has also come under severe attack, as the Federal Bureau of Investigation and other federal agencies have used terrorism as a vehicle to push existing plans for significantly expanded electronic surveillance. For example, the original Clinton and Dole terrorism bills defined almost all violent and property crime (down to petty offenses below misdemeanors) as "terrorism" and then allowed wiretaps for "terrorism" investigations. (Those provisions did not become law.)

Terrorists are, of course, already subject to being wiretapped. Yet, as federal wiretaps set record highs every year, wiretaps are used overwhelmingly for gambling and drugs. From 1983 to 1993, of the 8,800 applications for eavesdropping, only 16 were for arson, explosives, or firearms.

Wiretaps are currently authorized for the interception of particular speakers on particular phone lines. If the interception target keeps switching telephones (for example, by using a variety of pay phones), the government may ask the court for a "roving wiretap," authorizing interception of any phone line the target is using. Although roving wiretaps are currently available when the government shows the court a need, there is a campaign to allow roving wiretaps *without* court approval. In other words, the FBI would be on the honor system for conducting wiretaps according to the Constitution. The Fourth Amendment, however, mandates that an essential part of the system of checks and balances is that intrusive surveillance of Americans citizens must not take place without prior judicial authorization. Moreover, the FBI's recent record of lawlessness—from Ruby Ridge to Waco to Travelgate to Filegate, and all of the associated coverups—hardly

inspires confidence that independent supervision of the bureau should be curtailed.

The final terrorism bill, while deleting provisions for warrantless roving wiretaps, did significantly expand wiretapping authority. The Electronic Communications Privacy Act outlaws wiretapping by the government or by private parties, with certain exceptions (such as when a warrant is obtained). The terrorism bill narrowed the type of communication interceptions that are considered to be wiretapping and thereby greatly expanded the scope of communications that can legally be intercepted by private actors, as well as by government officials who lack both probable cause and a search warrant. Wireless transmission of computer data is now subject to search without a warrant.

Encryption

If a person writes a letter to another person, she can write the letter in a secret code. If the government intercepts the letter, and cannot figure out the secret code, the government is out of luck. That basic First and Fourth Amendment principle has never been questioned. But, if instead of being written with pen on paper, the letter is written electronically, and sent over a computer network rather man by postal mail, do privacy interests suddenly vanish? According to FBI director Louis Freeh, the answer is yes.

Testifying before the Senate Judiciary Committee, Freeh complained that people can communicate over the Internet "in encrypted conversations for which we have no available means to read and understand unless that encryption problem is dealt with immediately." The supposed encryption problem (i.e., people being able to communicate privately) could only be solved by outlawing high-quality encryption software like Pretty Good Privacy.

First of all, shareware versions of Pretty Good Privacy are ubiquitous throughout American computer networks. The cat cannot be put back in the bag. More fundamentally, the potential that a criminal, including a terrorist, might misuse private communications is no reason to abolish all private communication.

Although Freeh apparently wants to outlaw encryption entirely, the Clinton administration has been proposing the Clipper Chip as a first step. However, the Clipper Chip provides a low level of privacy protection against casual snoopers, and some computer scientists have already announced that the chip can be defeated. Moreover, the "key"—which

allows private phone conversations, computer files, or electronic mail to be opened by unauthorized third parties—will be held by the federal government or a third party approved by the government. The federal government promises that it will keep the keys carefully guarded and use them only to snoop when absolutely necessary.

Proposals for the federal government's acquisition of a key to everyone's electronic data, which the government promises never to misuse, might be compared to the federal government's proposing to acquire a key to everyone's home. Currently, people can buy door locks and other security devices that are of such high quality that covert entry by the government is impossible; the government might be able to break the door down, but the government would not be able to enter quietly, place an electronic surveillance device, and then leave. Thus, high-quality locks can defeat a lawful government attempt to bug a home, just as high-quality encryption can defeat a lawful government attempt to read a person's electronic correspondence or data.

While wiretaps or government surveillance of computer communications may be legal, there should be no obligation for individuals or businesses to make wiretapping easy. Simply put, Americans should not be required to live their lives so that the government can spy on them.

Thus, although proposals to outlaw or emasculate computer privacy are sometimes defended as maintaining the status quo (easy government wiretaps), the true status quo in America is that manufacturers have never been required to make products that are custom designed to facilitate government snooping. The point is no less valid for electronic keys than it is for front-door keys.

Efforts to limit electronic privacy will harm, not just the First and Fourth Amendments, but also American commerce. Genuinely secure public-key encryption gives users the safety and convenience of electronic files plus the security features of paper envelopes and signatures. A good encryption program can authenticate the creator of a particular electronic document—just as a written signature authenticates (more or less) the creator of a particular paper document. Public-key encryption can greatly reduce the need for paper. With secure public-key encryption, businesses could distribute catalogs, take orders, pay with digital cash, and enforce contracts with verifiable signatures—all without paper.

Conversely, the Clinton administration's weak privacy protection (giving the federal government the ability to spy everywhere) means that confidential business secrets will be easily stolen by business competitors

who can bribe local or federal law enforcement officials to divulge the "secret" codes for breaking into private conversations and files or who can hack the Clipper Chip.

Aliens

Although the United States has suffered exactly one alien terrorist attack in the last 11 years, special, harsh rules for aliens were at the top of the Clinton terrorism agenda. The new Clinton-Dole terrorism law allows secret evidence in alien deportation cases in which the government asserts that secrecy is necessary to national security. Georgetown University law professor David Cole calls the secret court the new "Star Chamber," because its powers resemble those of the inquisitorial court that the British monarchy, in violation of the common law, used to terrorize dissident subjects.

Modern Star Chamber proceedings are to be before a special court (one of five select federal district judges), after an ex parte, in camera showing that normal procedures would "pose a risk to the national security of the United States." After further ex parte, in camera motions, evidence that the government does not wish to disclose may be withheld from the defendant, who will instead be provided a general summary of what the evidence purports to prove. In other words, secret evidence may be used. Of course any of the "showings" that the government makes in camera and ex parte may be based on the unreviewable claims of a secret informant. No evidence may be excluded because it was illegally obtained, no matter how flagrantly the law was broken.

Legal aliens do not, of course, have the full scope of constitutional rights guaranteed to American citizens; for example, they cannot exercise rights associated with citizenship, such as voting or serving on a jury. But the Fifth Amendment's guarantee of due process protects "all persons," not "all citizens."

The argument for allowing secret evidence in deportation proceedings is that otherwise the identity or operational mode of a confidential informant might be jeopardized. First of all, the very purpose of the Sixth Amendment's confrontation clause is to prevent people's lives from being destroyed by secret accusations. Moreover, the argument against endangering the secrecy of confidential accusers in deportation cases proves too much. The very same argument applies in every other type of case in which informants are heavily used, including tax evasion, drug sales or possession, and gun laws. Obeying the confrontation clause may impede

the short-term interests of law enforcement, but the Constitution makes it clear that a criminal justice system without a right of confrontation poses a far greater long-term risk to public safety than does requiring the government to disclose the reason why it wants to imprison, execute, or deport someone.

Some persons may accept the Star Chamber for legal resident aliens under the presumption that such procedures would never be used against American citizens. Yet if there is anything the experience of Great Britain proves, it is that special, "emergency" measures implemented in a limited jurisdiction soon spread throughout the nation. Cancers always start small. If one international terrorist incident in 11 years is sufficient to justify a Star Chamber for aliens, then it is hard to resist the logic that crimes that actually are widespread (such as homicide, rape, or sales of controlled substances) should be entitled to their own Star Chamber.

Everything that terrorists do is already illegal. Current laws already provide ample authority for investigations of potential terrorists, including persons who have done nothing more than talk big. The Oklahoma City and World Trade Center bombings were both solved under existing laws. While the 1995 terrorism bill, one of the most repressive measures ever enacted by the U.S. Congress, was promoted as a response to the Oklahoma City bombing, not a single item in the entire bill would have prevented that heinous crime or assisted in its solution. The tiny but sensational threat of terrorism should not be used as a pretext for stripping fundamental freedoms from the American people. As the Founders of the American Republic understood, public safety in the long run is best protected by vigorous enforcement of the Constitution, not by giving more power to federal agencies that abuse the powers they already have.

Suggested Readings

Kopel, David B., and Joseph Olson. "Preventing a Reign of Terror: Civil Liberties Implications of Terrorism Legislation." *Oklahoma City Law Review* 21, forthcoming.

Office of Technology Assessment. *Taggants in Explosives.* Washington: Government Printing Office, 1988.

—Prepared by David B. Kopel